EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ANNUAL ACTIVITY REPORT




2019

ISSN 2314-9434

CONTACT

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

LEGAL NOTICE

This publication presents the annual activity report of ENISA for 2019. The report is based on the 2019 work programme as approved by the Management Board of ENISA in **Decision No MB/2018/20.**
The *ENISA Programming Document 2019–2021* was adopted as set out in Annex 1 to that decision. After the draft Cybersecurity Act was adopted, the Management Board amended the 2019 work programme in **Decision No MB/2019/3**.
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

© The European Union Agency for Cybersecurity, 2020
Reproduction is authorised provided the source is acknowledged.
Copyright for images on the cover and internal pages: © Shutterstock.
For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

Print	ISBN 978-92-9204-349-0	ISSN 1830-981X	doi:10.2824/303633	TPAB-20-001-EN-C
PDF	ISBN 978-92-9204-348-3	ISSN 2314-9434	doi:10.2824/653387	TPAB-20-001-EN-N

ANNUAL ACTIVITY REPORT 2019

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TABLE OF CONTENTS

A MESSAGE FROM THE EXECUTIVE DIRECTOR

It is a great honour for me to present the annual activity report of 2019.

A turning point in the history of the European Union Agency for Cybersecurity (ENISA), 2019 set the agency's future in motion. My esteemed predecessor, Prof. Dr Udo Helmbrecht, brought to a conclusion 10 years of successful management, paving the way for the most significant of the year's achievements: the Cybersecurity Act (CSA), which came into force in June 2019, providing the agency with a permanent mandate and significantly extending the scope of its activities.

In addition to expanding the existing activities of the agency, the CSA gives ENISA an operational role and mandates it to implement the cybersecurity certification framework, a new challenge that the agency already started to address in 2019. The provisions of the CSA enhance the capacity of the agency to act as a centre of expertise for the EU, its Member States and the private and public sectors.

The CSA also establishes the new Advisory Group. Formerly known as the Permanent Stakeholder Group, its purpose is to take on board the opinions of key stakeholders such as industry, academia and relevant EU agencies and bodies as well as consumer protection specialists.

The act also requires us to look to the future in order to ensure that the technological developments that are about to change our society are properly secure. Today's information security must integrate the various concepts used to develop the emerging technologies of tomorrow, an idea that is reflected in the new name given to ENISA by the CSA: the European Union Agency for Cybersecurity.

These being significant changes, the introduction of the CSA necessarily had an impact on the planning of activities. Working closely with its Management Board, ENISA identified a series of amendments to be made to its work programme to reflect the key changes. I am happy to report that the revised work programme was successfully implemented during the course of 2019, the details of which are provided in this report.

As part of this work, the agency continued to reach out to stakeholders through major events, including the European Cyber Security Challenge (ECSC) (which concluded in Romania), the European Cyber Security Month (ECSM) and the fifth eHealth Security Conference organised in partnership with the Centre de Seguretat de la Informació de Catalunya (Centre for Information Security of Catalonia) (CESICAT). Such events demonstrate ENISA's ability to draw communities together and further enhance collaboration across Member States.

As in previous years, the agency delivered a series of publications on important areas in cybersecurity. These included texts covering a wide range of topics, providing recommendations and information on securing modern technologies (e.g. how to implement security by design for the internet of things (IoT) and the threat landscape of 5G networks), along with a substantial number of reports on more traditional subjects (e.g. good practices for the security of healthcare services and good practices for maritime security (port cybersecurity)).

The agency delivered a wide range of training sessions such as those offered during the sixth Summer School on Network and Information Security (NIS). The topics covered ranged from quantum computing and cryptography to cyberthreat analysis and cyberthreat intelligence (CTI). The event was successfully co-organised with the Foundation for Research and Technology – Hellas (FORTH) based in Heraklion, Crete.

The agency would not have achieved the successful results presented in this report without the precious support of all our stakeholders and of the communities, European institutions and bodies and Member States engaged with us in the challenge of keeping Europe secure. Cybersecurity is a shared responsibility. I am especially grateful for the level of commitment evidenced by the achievements of 2019.

Finally, it is time for me to congratulate those passionate professionals at the heart of ENISA, namely the staff, for their unfailing motivation and engagement. They are the ones creating the synergies behind the success of the European Union Agency for Cybersecurity.

Juhan Lepassaar

Executive Director, ENISA

THE EUROPEAN UNION AGENCY FOR CYBERSECURITY IN BRIEF

A new legal basis in 2019

ENISA was established in 2004[1]. The first 4-year mandate of the former European Network and Information Security Agency was extended without interruption in 2009, 2011 and 2013.

The CSA, signed on 17 April 2019, came into force on 27 June of the same year. Under this new act, ENISA's tasks are reinforced and extended with the new activities under the cybersecurity certification framework. ENISA's areas of action are the following:

- **expertise**
- **policy**
- **capacity**
- **cooperation**
- **certification**
- **enabling.**

The CSA also gives the agency a new name – 'The European Union Agency for Cybersecurity' – and, for the first time in its history, a permanent mandate.

1 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15, available at: http://data.europa.eu/eli/reg/2019/881/oj

Mission

ENISA's mission is to contribute to securing Europe's information society. This is achieved by raising awareness of cybersecurity and by developing and promoting a culture of NIS in society for the benefit of citizens, consumers and public and private organisations in the EU.

The role of ENISA is therefore to ensure a high level of NIS within the EU. Acting as a centre of expertise, ENISA supports European institutions and bodies and Member States to that end.

ENISA's tasks are the following:

- **development and implementation of EU policy and law,**
- **capacity building,**
- **operational cooperation at EU level,**
- **market cybersecurity certification and standardisation,**
- **knowledge and information sharing,**
- **awareness raising and education,**
- **research and innovation,**
- **international cooperation.**

In line with the objectives defined in the act, the agency carries out its operations in accordance with the 2019–2021 annual and multiannual work programme containing all of its planned activities, drawn up by the executive director of ENISA and adopted by the Management Board of ENISA.

Objectives

In order to implement the provisions of the CSA and achieve its mission, ENISA has defined the following objectives.

EXPERTISE

Objective 1. Improving expertise related to NIS.
Objective 2. NIS threat landscape and analysis.
Objective 3. Research, development and innovation.

POLICY

Objective 1. Supporting EU policy development.
Objective 2. Supporting EU policy implementation.

CAPACITY

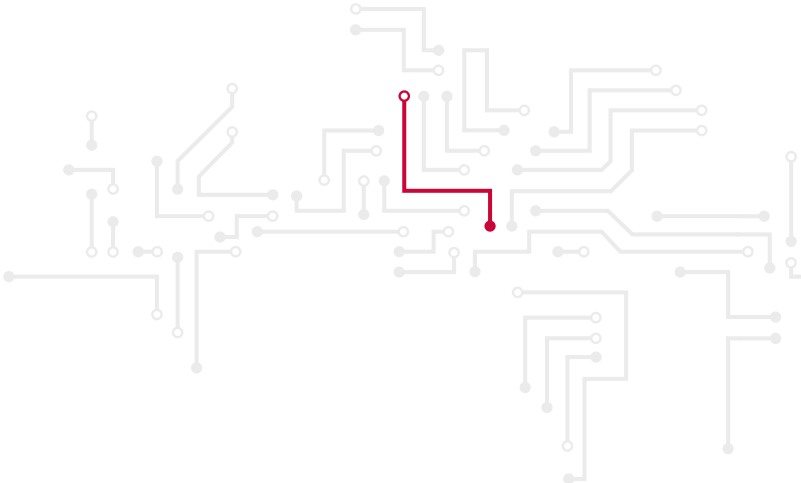
Objective 1. Assisting Member States in capacity building.
Objective 2. Supporting EU institutions in capacity building.
Objective 3. Assisting in improving private sector capacity building and general awareness.

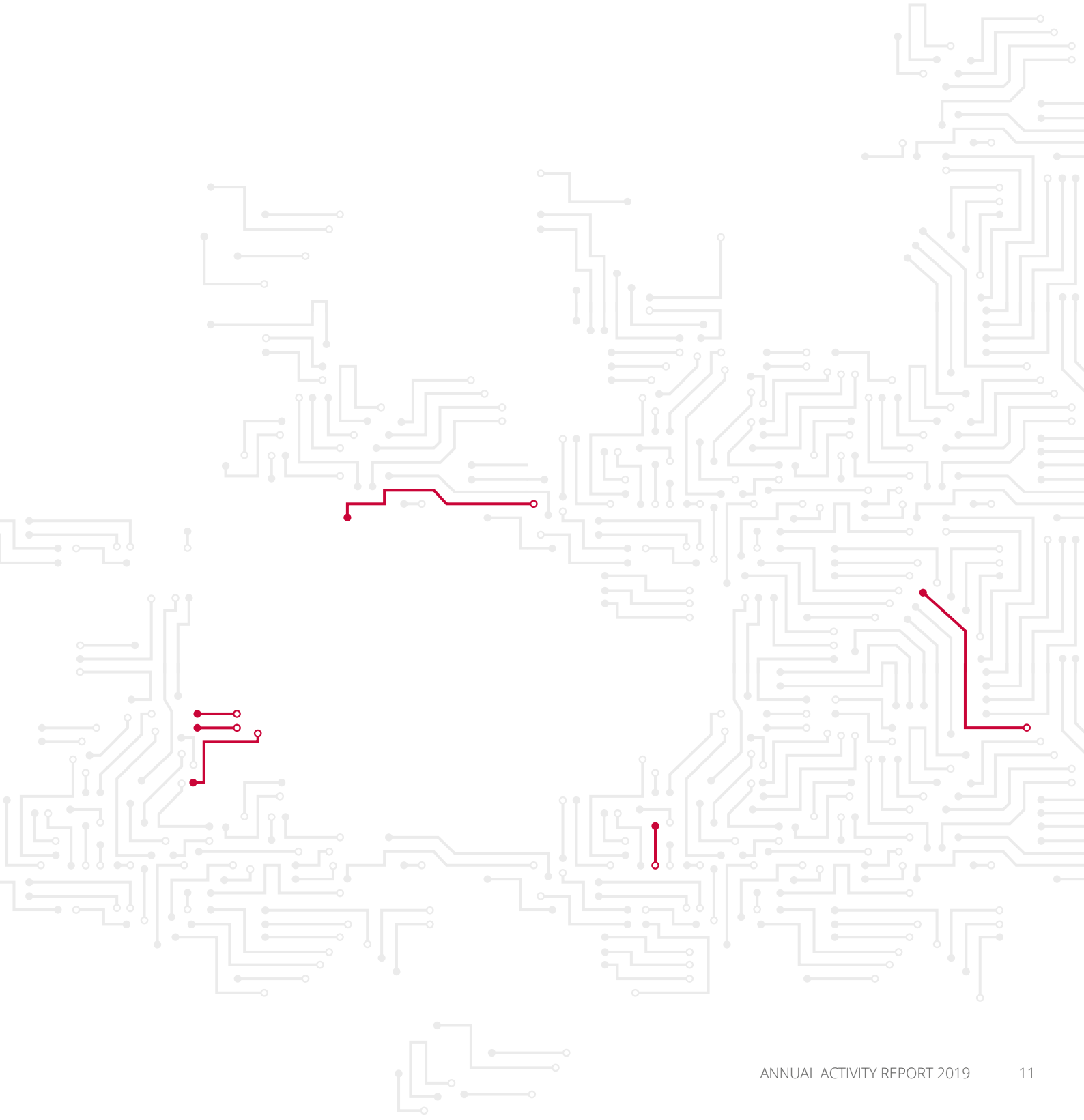
COMMUNITY

Objective 1. Cyber-crisis cooperation.
Objective 2. Computer security incident response teams (CSIRTs) and other NIS community building.

ENABLING

Objective 1. Management and compliance.
Objective 2. Engagement with stakeholders and international activities.





ENISA MANAGEMENT BOARD ASSESSMENT

The analyses and assessment by the Management Board of ENISA of the consolidated annual activity report for the year 2019 of the authorising officer of ENISA

The Management Board takes note of the Annual Activity Report (AAR) for the financial year 2019, submitted by the Executive Director of the European Union Agency for Network and Information Security (ENISA) in accordance with Article 48 of the Financial Regulation applicable to ENISA.

The Executive Board received a copy of the 2019 AAR produced by the Executive Director of ENISA in his quality of Authorising Officer for the implementation of the annual budget on 26 May 2020 and the Management Board received a copy of the 2019 AAR on 11 June 2020.

In analysing and assessing the AAR 2019, the Management Board has concluded the following:

- The AAR presents key results of the implementation of the ENISA Work programme 2019 and leads to conclusion that the Agency completed all deliverables agreed with the Management Board in the Work Programme 2019.
- Despite challenging circumstances associated with the transition to the responsibilities of the new mandate following the entry into force of the Cybersecurity Act, the Agency was able to meet the objectives set in the work programme 2019 as shown by the results presented in this report.
- ENISA produced 55 reports on a variety of subjects pertaining to the current cybersecurity environment. These reports provided guidance in 'traditional areas' of cybersecurity, such as critical systems and incident handling, but also in evolving areas such as SMART technologies and the Internet of Things (IoT). Impact indicators show that the Agency's results exceeded the targets established in the Work Programme 2019, against the framework of the ENISA Strategy 2016-2020.
- In addition to delivering on its core work programme, ENISA also supported the European Commission and the Member States in responding to priorities that arose during the course of the year – notably the need to secure the elections for the European Parliament and the support for the Commission's 5G Action Plan.
- Overall, the AAR is in line with the ENISA Work Programme 2019 and ENISA's work is well aligned with the overall European Union priorities for digital single market. A coherent link is provided between activities planned in the Work Programme 2019 and the actual achievements reached in the reporting period.
- The AAR also describes ENISA's management of resources and the budget execution of the

EU subsidy. The changes in the legal mandate also impacted the allocation of the budgetary resources. An increase from EUR 11,0 million to EUR 16,3 million could only be inscribed and made available to the Agency following the amendment approved by the Management Board on 31/05/2019. ENISA was able to implement a budgetary increase. In 2019, ENISA executed 15 771 525 euros in commitment appropriations representing 97% of the total budget of the year.

- The AAR also provides a follow up of the 2017 Discharge and control results. This section also notes the main categories of deviation that led to exceptions reported. In 2019 the agency recorded 38 exceptions. 33 of these are under the relevant materiality level (less than EUR 15.000) and are of minor administrative nature with no financial impact. The remaining 5 exceptions were linked to a posteriori commitments.

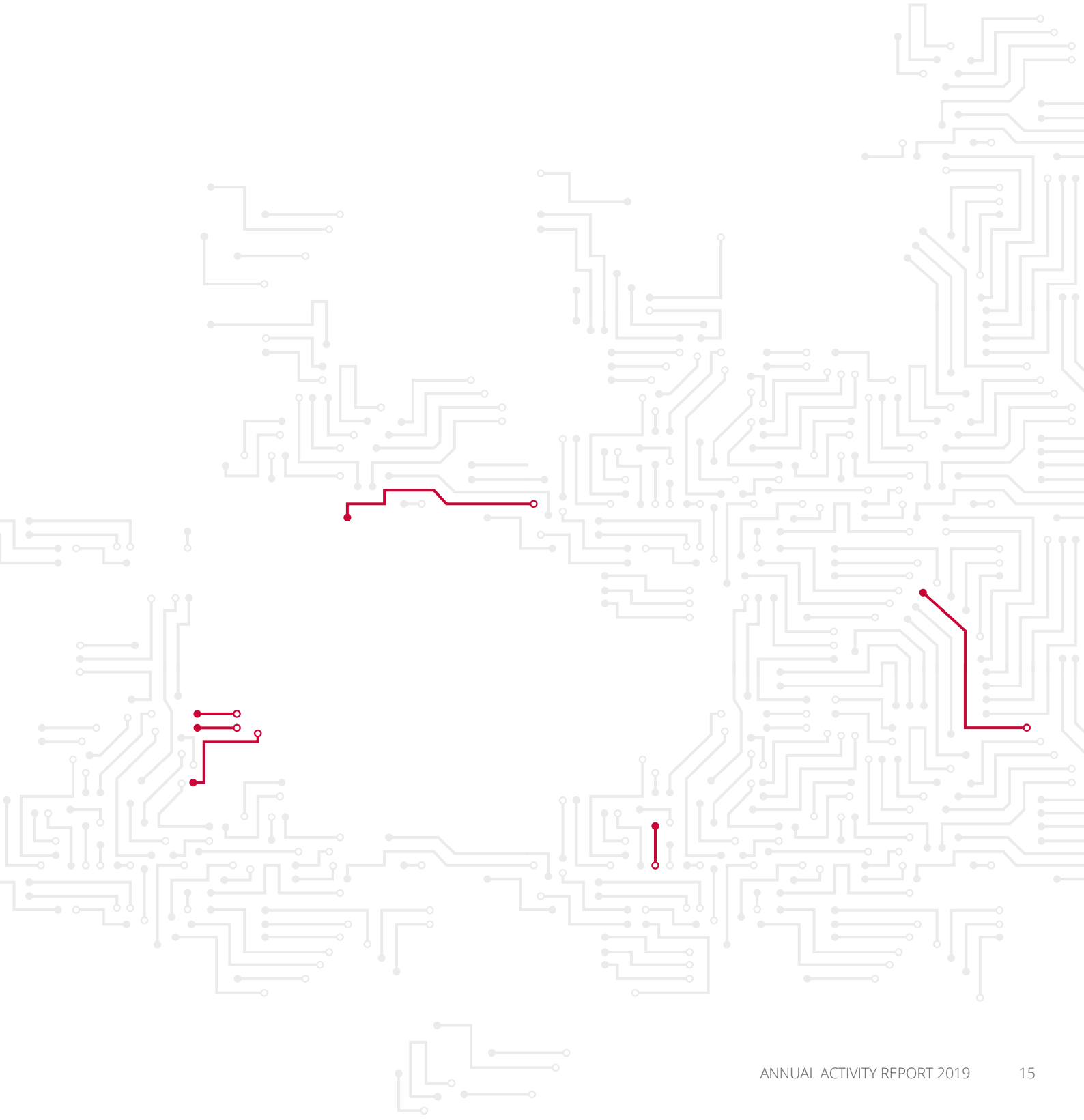
- The AAR leads to conclusions that the adequate management of risks, high level of transparency, data protection, business continuity, as well as efforts were undertaken to improve overall efficiency in all activities.

- 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 achievements of ENISA in 2019. The Management Board notes with satisfaction that ENISA could deliver work programme 2019 despite the Cybersecurity Act entering into force on 27 June 2019. The Management Board expresses its appreciation to the Executive Director and his staff for their commitment and achievements throughout the year.

The Management Board notes that the Executive Director has no critical issues to report which would affect the presentation of the annual accounts for the financial year 2019 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 YEAR IN CONTEXT

There were two major events in 2019 that are of significance for this report.

The signing of the CSA in June resulted in the need to amend the work programme to reflect the most important changes. These changes also impacted the allocation of the budgetary resources.

In October, ENISA welcomed a new executive director: Dr Prof. Udo Helmbrecht handed his role over to Juhan Lepassaar.

KEY PERFORMANCE INDICATORS

ENISA's key performance indicators (KPIs) provide the metrics with which to measure the performance, results and impact of the agency's outcomes and output. KPIs are defined and outlined in this report according to the type of output for each activity.

Three types of output are identified: publication (P), event (E) and support (S).

The major KPIs are the following:

- number of reports, news items, dissemination materials, etc. published;
- number of Member States, stakeholders and communities engaged in discussions or workshops, or total number of individual participants;
- variety of representatives involved in the preparation of recommendations;
- quantity of training materials developed or updated;
- number of tests and exercises performed;
- number of Member States using tools and/or platforms developed.

ACHIEVEMENT OF STRATEGIC PRIORITIES AND OBJECTIVES

The CSA signed in April impacted the strategic priorities of the agency initially defined for 2019. As a result, ENISA, together with its Management Board, identified and agreed on a number of minor amendments to be performed to align its activities accordingly.

From an operational perspective, the highlights of the year were as follows.

- ENISA produced 55 reports on a variety of subjects pertaining to the current cybersecurity environment. These reports provided guidance in 'traditional' areas of cybersecurity, such as critical systems and incident handling, but also in evolving areas such as self-monitoring analysis and reporting technology (smart) technologies and the IoT.
- As in previous years, the agency was also active in various awareness-raising activities. The ECSM and the ECSC are key examples.
- ENISA supported the effort to ensure the security of the European Parliament elections. As part of this effort, the agency supported an exercise to ensure that the EU institutions and Member States were prepared for potential attacks.
- Following the high-priority request from the Commission to engage in activities related to the cybersecurity of 5G networks, ENISA worked together with the Commission and the Member States to produce a consolidated risk assessment for 5G and an associated threat landscape. The agency also contributed significantly to the development of the 5G toolbox. This work was carried out in addition to the work programme activities; the only consequence was a delay in the publication of the ENISA threat landscape (ETL) report.
- Despite the challenging circumstances associated with the transition to the responsibilities of its new mandate, the agency was able to meet the objectives set in the single programming document, as shown by the results presented in this report.

ORGANISATION, BUDGET AND INTERNAL CONTROL

The structure of the organisation had to be slightly adapted to integrate ENISA's new activities under the cybersecurity certification framework, its increased coordination of crisis management and its extended responsibilities derived from the NIS directive (NISD).

Budget management was extremely challenging as the budget associated with the entry into force of the CSA (constituting an increase from EUR 11 million to EUR 16.3 million) could only be encoded in the financial system and made available to the agency following the amendment approved by the Management Board on 31 May 2019. This late transition affected recruitment planning and also resulted in the need to revise and update the agency's information technology (IT) infrastructure to meet the new requirements under the CSA.

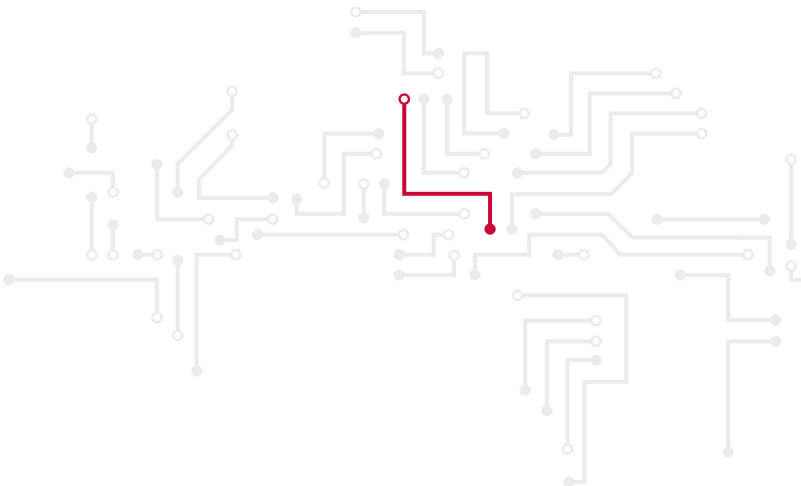
Between 1 January and 31 December 2019, ENISA executed EUR 15 771 525 in commitment appropriations, representing 97 % of the total budget for the year.

Although our ambitious financial goal of committing 99 % of the budget was not achieved, the commitment rate of 95 % set by the Commission for the year was exceeded for 2019. Compared to 2018, there was a slight decrease in commitment execution (99 %) but ENISA was able to implement a budgetary increase of almost 50 % following the adoption of the CSA.

The payment execution rate of 70 % is a result of:

- the late entry into force of the CSA;
- delays in the recruitment execution, caused by the late entry into force of the CSA;
- late commitment of significant IT infrastructure investments (in the last quarter of 2019) required to meet the new challenges associated with ENISA's new mandate.

The agency takes the measures necessary to comply with any observations or recommendations issued by the Internal Audit Service (IAS) of the European Commission and the European Court of Auditors (ECA). The management team continuously uses all these elements to assess the risk associated with each area and to further develop controls and procedures.



KEY CONCLUSIONS

The agency successfully carried out its work programme throughout 2019 and managed the transition to the new mandate in a smooth fashion. In addition to delivering on its core work programme, ENISA also supported the Commission and the Member States in responding to priorities that arose during the course of the year – notably the need to ensure the security of the European Parliament elections and the support for the Commission's 5G action plan.

In conclusion, management has reasonable assurance that the objective to increase assurance of reliability of performance, legality and regularity based on our legal and financial framework is realised and working as intended. Internal risks are identified and appropriately monitored. Mitigation measures are implemented wherever deemed appropriate.

PART I
ACHIEVEMENTS OF THE YEAR

1 ACTIVITY 1: EXPERTISE

Anticipate and support Europe in facing emerging NIS challenges

1.1 Key results in the implementation of Activity 1: EXPERTISE

1.1.1 Objective 1: Improving expertise related to NIS – outputs

O.1.1.1. Good practices for the IoT

Main achievements:

- guidelines on the IoT;
- online tool visually representing IoT security measures;
- workshop in Brussels for the validation of the report findings[2];
- third ENISA–European Union Agency for Law Enforcement Cooperation (Europol) IoT Security Conference in Athens.

ENISA issued guidelines identifying and analysing good practices for developing applications in a secure manner, making use of secure software development life cycle ([3]) principles. Several IoT security challenges can be addressed in this way, such as checking for security vulnerabilities, secure deployment, ensuring continuity of secure development in the case of integrators, continuous delivery and more.

Existing frameworks, guidelines and initiatives were considered while collaborating with the ENISA IoT SECurity (IoTSEC)[4] Experts Group and the ENISA Industry 4.0 Cyber Security Experts Group (EICS)[5] Furthermore, targeted IoT case studies were developed in order to identify risks and vulnerabilities. This was achieved by setting out appropriate attack scenarios and providing relevant recommendations and good practices. ENISA also developed an online tool that visually represents IoT security measures, in order to further support stakeholders.

On 8 October 2019, ENISA organised a workshop in Brussels in order to validate the findings of the report. The workshop brought together 28 IoT stakeholders. They all actively contributed to the study. Overall, the study involved 37 IoT stakeholders from 9 EU Member States, a European Economic Area (EEA) country, Israel and the United States.

On 24 and 25 October 2019, the third ENISA–Europol IoT Security Conference took place in Athens, Greece. Organised by ENISA in cooperation with Europol, the event brought together about 180 IoT stakeholders.

2 https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1
3 Typically referring to the activities of planning, implementation, testing, documentation, deployment and maintenance.
4 https://resilience.enisa.europa.eu/iot-security-experts-group-1
5 https://resilience.enisa.europa.eu/eics-experts-group

The main topics of the conference included IoT security and the emerging topic of artificial intelligence (AI) security.

O.1.1.2. Good practices for the security of smart cars

Main achievements:

- report on good practices for the security of smart cars;
- workshop in Brussels to validate the findings of the report;
- supporting related activities of the European Commission.

On 25 November 2019, ENISA issued a report on good practices for the security of smart cars, namely connected and (semi-)autonomous vehicles and their added-value features designed to enhance car users' experience and improve car safety.

This report can be used as a reference point since it takes all existing standardisation, legislative and policy initiatives into consideration. It helps promote the cybersecurity of smart cars across Europe and raises awareness of relevant threats and risks with a focus on cybersecurity for safety.

On 7 October 2019, ENISA organised a workshop in Brussels in order to validate the findings of the report. The workshop brought together stakeholders from the EU automotive sector. Overall, the study involved over 20 automotive stakeholders from 7 EU Member States.

ENISA also actively supported the Commission in several activities, including the cooperative, connected, automated and autonomous mobility single platform[6].

O.1.1.3. Encrypted traffic analysis: use cases and security challenges

Main achievement:

- Report on encrypted traffic analysis.

In 2019, ENISA focused on the disrupting impact encryption has on network security. According to recent studies, more than 80 % of internet traffic is protected by Hypertext Transfer Protocol Secure[7] and applications increasingly use encryption by default for their communications.

However, encryption is not always used in legitimate ways. Encryption can also be used in ransomware and sophisticated malicious software operating with off-the-shelf or homemade encryption to evade detection and prevention. This reduces the efficacy of traditional network detection and protection tools, since these require access to unencrypted traffic. Organisations relying on such controls lose valuable insight and end up relying on an infrastructure hiding compromising blind spots.

An obvious solution to this problem is to prohibit or to undo the encryption to allow inspection of traffic. However, this can only be enforced on legitimate users and it negates the principle of end-to-end encryption, potentially exposing data and reducing user privacy.

A lesser-known alternative leverages machine learning and AI techniques to make inferences directly from the encrypted traffic. These techniques work by analysing traffic metadata, without having to access the unencrypted payload.

ENISA's study entitled *Encrypted Traffic Analysis – Use cases & security challenges* looks at these techniques and their use cases, such as encrypted malware and traffic detection. For each use case, the study identifies mainstream methods, denoting capabilities and limitations. The impact of misuse of encryption on the privacy of end users is also addressed. In addition, the report presents simple but efficient countermeasures to correct common bad Transport Layer Security practices.

The objective of the report is threefold; its aim is to:

(a) advise decision-makers, security practitioners and administrators on new network security tools and techniques;

(b) discourage improper Transport Layer Security practices;

(c) alert policymakers to limitations of encryption posed by machine learning and AI, especially with respect to user privacy.

6 The cooperative, connected, automated and autonomous mobility platform is a joint initiative by DG Mobility and Transport, DG Communications Networks, Content and Technology, DG Internal Market, Industry, Entrepreneurship and SMEs and DG Research and Innovation (see https://connectedautomateddriving.eu/mediaroom/european-commission-launches-ccam-single-platform/).

7 Estimates place the percentage of web pages loaded by Firefox using Hypertext Transfer Protocol Secure at + 80 %. Source: https://letsencrypt.org/stats/

O.1.1.4. Good practices for the security of healthcare services

Main achievements:

- report on procurement guidelines for cybersecurity in hospitals;
- fifth eHealth Security Conference organised with CESICAT in Barcelona;
- participation in the Medical Device Coordination Group – New Technologies Task Force on Cybersecurity facilitated by DG Internal Market, Industry, Entrepreneurship and SMEs;
- participation in the European Cybersecurity Health Group set up by the eHealth Network (run by DG Health and Food Safety);
- creation of the NIS Cooperation Group (NIS CG) work stream dedicated to the healthcare sector.

ENISA issued a set of guidelines for ensuring cybersecurity in procurement for hospitals. The guidelines are aimed at IT professionals and procurement officers in hospitals and healthcare organisations. They are of specific interest to the professionals in charge who need to make informed decisions when procuring services, products or infrastructure for their organisation. All good practices presented are linked to the types of procurement for which they are relevant and to threats that they can mitigate, providing an easy-to-filter set of practices for hospitals who want to focus on particular aspects. ENISA collected input from 15 healthcare professionals, covering 8 Member States and the private sector, namely medical device manufacturers. The report was officially published in February 2020.

On 30 October 2019, ENISA held the fifth eHealth Security Conference in cooperation with CESICAT in Barcelona, during the Barcelona Cybersecurity Congress.

The conference brought together high-level speakers who spoke on cybersecurity to an audience of 100 participants from both the public and the private sector, from about 17 Member States and European Free Trade Association (EFTA) countries.

ENISA also actively supported the European Commission and the community through several actions.

ENISA participated in the Medical Device Coordination Group – New Technologies Task Force on Cybersecurity facilitated by DG Internal Market, Industry, Entrepreneurship and SMEs. The group published guidelines to help manufacturers meet all the relevant safety and performance requirements of the medical device regulation in regard to cybersecurity ('MDCG 2019–16 – Guidance on cybersecurity for medical devices').

ENISA also engaged in the European Cybersecurity Health Group established by the eHealth Network (run by DG Health and Food Safety). The group is meant to identify technical measures to enhance cybersecurity in healthcare organisations by raising

awareness and building capabilities in the area. Through their national healthcare authorities, 12 Member States participated in the group.

Finally, ENISA supported the community and relevant authorities in the creation of the NIS CG work stream dedicated to the healthcare sector. The work stream supported the implementation of the directive by operators of essential healthcare services. Activities are meant to start in 2020.

O.1.1.5. Good practices for maritime security

Main achievements:

- report on good practices for chief information security officers (CISOs) and chief information officers of port authorities and terminal operators;
- workshop in Lisbon to strengthen the cybersecurity of EU ports hosted by the European Maritime Safety Agency (EMSA);
- activities in support of DG Mobility and Transport and EMSA.

ENISA conducted a study to produce a comprehensive set of good practices for CISOs and chief information officers of operators involved in the port ecosystem, especially port authorities and terminal operators.

Cybersecurity in ports is addressed in a holistic manner for the first time in the report. It provides detailed mapping of the relevant stakeholders, interfaces and key services. It also introduces an extensive taxonomy of port assets covering both IT and Operational Technology. It proposes a detailed threat taxonomy. It also defines four key scenarios of potential attacks on ports.

The report concludes with a list of policy, organisational and technical security measures, to be implemented for protection against cyberattacks. The report was developed in cooperation with a number of EU ports and has been widely referenced.

On 26 November, ENISA organised a workshop in Lisbon with the objective of strengthening the cybersecurity of EU ports. The workshop was hosted by EMSA and brought together over 60 stakeholders from the EU maritime sector. A significant part of the workshop was dedicated to a discussion on ENISA's report *Port Cybersecurity – Good practices for cybersecurity in the maritime sector*. The afternoon session focused on the concept of 'information sharing and analysis centres' (ISACs), including presentations on good practices and lessons learnt from similar initiatives in other sectors.

A total of 75 stakeholders from 18 Member States actively contributed to these activities by providing input on the drafting of the report and/or by participating in the workshop.

ENISA also actively supported the Commission and EMSA in several activities, including:

- the organisation by DG Mobility and Transport of a maritime cybersecurity workshop in Brussels;
- the organisation of a tabletop cybersecurity exercise by EMSA in Lisbon;
- EMSA's SafeSeaNet project.

1.1.2 Objective 2: NIS threat landscape and analysis – outputs

O.1.2.1. Annual ENISA threat landscape

Main achievements:

- 5G threat landscape mapping;
- risk assessment work in support of the 5G toolbox;
- organisation of CTI training (cyberthreat analysis, CTI and practical cryptography) delivered during the 2019 Summer School;
- preparation of CTI-EU event[8] of 30th and 31st January 2020.

The ETL is an annual compilation of the cyberthreats that have been encountered throughout the year. The ETL summarises the top 15 cyberthreats, based on the number of occurrences, as reported in open-source resources, such as various reports, articles, incident analyses and expert opinions. The ETL report provides strategic intelligence on the cyberthreats assessed, including points of interest, statistics, mitigation measures, main incidents, information about threat actors and their motives, attack vectors deployed, mitigation measures and authoritative resources.

In 2019, the Commission requested that ENISA be involved in the work on the cybersecurity of 5G networks[9]. Considered high priority, the extra work this endeavour represented did not allow ENISA to issue the ETL that it usually delivers on a yearly basis. The 2019 ETL was therefore postponed to 2020. The ETL report for 2019 will be based on data collected

8 https://www.enisa.europa.eu/events/2019-cti-eu/2019-cti-eu-bonding-eu-cyber-threat-intelligence

9 Commission recommendation of 26 March 2019 – Cybersecurity of 5G networks, C(2019) 2335 final, available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58154

during both 2019 and the first half of 2020. The ETL is expected to be released in mid 2020.

Further to the Commission's request in relation to 5G, ENISA delivered mapping of the 5G threat landscape.

The 5G threat landscape was developed thanks to existing work of ENISA in the area (of software-defined networking / 5G threat landscapes). It was created with the support of relevant stakeholders, and was supported by the NIS CG.

The content of the 5G threat landscape was communicated to other relevant bodies, such as the Body of European Regulators for Electronic Communications (BEREC) working group on 5G.

In support of the Member States, the Commission and relevant stakeholders, ENISA consolidated national risk assessments performed by Member States into a single document.

For this task, ENISA engaged in close cooperation with DG Communications Networks, Content and Technology by means of common efforts towards the consolidation of the national risk assessments received.

The NIS CG reviewed the material in a continuous manner.

This consolidated risk assessment and the 5G threat landscape were merged into a joint review of the EU-wide risk exposure of 5G networks and formed the basis for the development of the 5G toolbox[10].

ENISA continued to engage with its CTI Expert Group in 2019. The group supported ENISA in streamlining various tasks in the area of CTI. It provided advice for the key ENISA CTI stakeholder event 'CTI-EU'. It also provided support for the organisation of the CTI training during the 2019 ENISA Summer School and contributed to information collection.

ENISA also delivered training sessions on cyberthreat analysis, CTI and practical cryptography during the ENISA–FORTH NIS Summer School.

The objective of such training sessions is to promote cyberthreat analysis by ensuring knowledge transfer on CTI matters between cybersecurity practitioners. The feedback received from participants has revealed the interest of the community in cyberthreat analysis.

O.1.2.2. Restricted and public info notes on NIS

Main achievements:

ENISA provides guidance on important NIS events and developments through info notes.

The work on info notes was suspended in 2019 further to the emergence of activities to be performed in relation to 5G.

Resources allocated to this task were transferred to the 5G threat landscape and the consolidation of 5G national risk assessments.

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

Main achievements:

- Article 13a[11] Expert Group meetings and Border Gateway Protocol (BGP) security paper;
- Article 19[12] meetings and 2-day cryptography seminar;
- update of the telecoms and trust services breach-reporting templates;
- report on breach-reporting synergies.

Throughout the year, ENISA continued to engage in the cooperation with ENISA's expert group set up to carry out the provisions of Article 13a of the Telecom Framework Directive.

Every year the group of experts from European national telecoms security authorities sees its number of members and meeting attendance increase.

The group is chaired by the Dutch telecoms authority. Formed of 28 countries (from the EU/EFTA/EEA), the group validated the EU-wide annual telecoms security incidents report.

About 45 experts from telecoms security authorities joined the meetings related to the provisions of Article 13a of the Telecom Framework Directive in Stockholm, Ljubljana and Belgrade.

The Article 13a in-depth technical publication focused on BGP security (*7 Steps to Shore up BGP*) was drafted and delivered in close cooperation with industry experts.

10 https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123

11 https://resilience.enisa.europa.eu/article-13/
12 https://resilience.enisa.europa.eu/article-19

ENISA continued to engage in strengthening its cooperation with supervisory bodies and with FESA[13], supporting ENISA's expert group set up to carry out the provisions of Article 19 of the eIDAS regulation.

Chaired by the Austrian supervisory body, the group, now involving 29 countries (from the EU/EFTA/EEA), validated the EU-wide annual trust services security incidents report. A total of 40 experts from trust service supervisory bodies joined the meetings related to the provisions of Article 19 of the eIDAS regulation in Tirana and Paris.

ENISA also hosted and delivered a 2-day cryptography seminar (theoretical and practical) for experts from the supervisory bodies (to support the Article 19 Expert Group).

ENISA maintained its cooperation with the EU Member States on EU-wide breach reporting. This cooperation operates along two lines:

- the support given by ENISA to the NIS CG work stream 3 (NISD breach reporting) building on the telecoms breach-reporting experience;
- the work of adapting the telecoms and trust service breach-reporting templates, for better alignment with the NISD.

The new tool is designed to support telecoms, trust services and the NISD, and uses the NIS CG taxonomy.

ENISA also delivered a new map of breach-reporting processes: the breach-reporting synergies paper.

The breach-reporting synergies paper, delivered by ENISA, was validated by the group, 12 countries and 20 experts from the NIS CG work stream 3.

The paper was delivered to the work stream by the deadline in the work stream 3 work plan (end of 2019).

O.1.2.4. Regular technical reports on the state of cybersecurity

Main achievement:

- report on software vulnerabilities.

For this particular output, ENISA produced a report on the state of software vulnerabilities for 2018/2019. The report analyses the actual figures and generates intuitive statistics on the root causes of the most critical vulnerabilities. In order to produce this deliverable, ENISA engaged with experts in the related fields from the CTI and the CSIRT community.

1.1.3 Objective 3: Research, development and innovation – outputs

O.1.3.1. Supporting cybersecurity public–private partnership in establishing priorities for EU research and development

Main achievements:

- publication of an information and communications technology (ICT) consultation paper on digital sovereignty;
- report on research and innovation directions for EU digital sovereignty.

To help shape the research and innovation landscape, ENISA produced a report on the most important cybersecurity research priorities, following an open consultation.

In 2018 the focus was on improving the EU's cyber safety[14]. A new report was necessary to identify the research and innovation directions for EU digital sovereignty.

To that end, ENISA studied recent relevant cybersecurity research roadmaps proposed and defined by several groups in the EU including recent Networks of Excellence, the European Cyber Security Organisation (ECSO) and several national initiatives.

To select the most relevant research directions, ENISA created a survey and invited a wide community of stakeholders to express their opinions.

About 100 stakeholders responded to the survey and ENISA drafted its conclusions to be discussed in an open validation, in which an ECSO representative and members of ECSO Working Group 6 were invited to participate.

A final presentation of the results was given to the ECSO Working Group 6 community in February 2020.

In addition, ENISA provided secretariat support to the National Public Administration Committee. Two meetings were scheduled by ECSO in 2019, one in February and the other in May.

13 Forum of European supervisory authorities for trust services providers: http://www.fesa.eu/

14 https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity

1.2 Outputs and performance indicators for Activity 1: EXPERTISE

Summary of outputs from Activity 1: EXPERTISE – Anticipate and support Europe in facing emerging NIS challenges		
Outputs	**Performance indicator**	**Results achieved**
Objective 1.1. Improving expertise related to NIS		
Output O.1.1.1. Good practices for security of the IoT	Engagement of 5 industries using the IoT and 5 IoT stakeholders from 5 EU Member States in the preparation of the study (P) and/or validation workshop (E).	37 industries using the IoT were involved in the preparation of the study (P) and/or validation workshop (E). 37 IoT stakeholders from 9 EU Member States, 1 EEA country, Israel and the United States were involved in the preparation of the study (P) and/or validation workshop (E).
Output O.1.1.2. Good practices for the security of smart cars	Engagement of 5 automotive manufacturers and 5 automotive stakeholders from 5 EU Member States in the preparation of the study (P) and workshop (E).	5 automotive manufacturers and 21 automotive stakeholders from 7 EU Member States were involved in the preparation of the study (P) and workshop (E).
Output O.1.1.3. Awareness raising of existing technical specifications for cryptographic algorithms	Publication of 2 news items or materials for dissemination covering public documents and activities of the groups/ meetings attended.	Delivery of report on encrypted traffic analysis use cases and capabilities, to raise awareness of areas where widespread encryption can act as a disruptor. Stakeholder engagement through participation in event organised by the Computer Security and Industrial Cryptography research group of Katholieke Universiteit (Catholic University) Leuven. Development of training material for practical cryptography. The course was delivered in the ENISA–FORTH NIS Summer School and was very well received, with participants asking for the training to be repeated.
Output O.1.1.4. Good practices for the security of healthcare services	Engagement of healthcare stakeholders from at least 12 EU Member States in activities related to good practices for security of healthcare services, i.e. a publication (P) and/or a workshop (E) and/ or support (S).	15 healthcare IT professionals from 8 Member States participated in the preparation of the procurement guidelines for hospitals (P). The annual eHealth workshop hosted approximately 100 participants from 17 Member States and EFTA countries (E).
Output O.1.1.5. Good practices for maritime security (port security)	Engagement of 10 maritime sector stakeholders from 5 EU Member States in the preparation of the study (P) and/or the workshop (E).	75 stakeholders from 18 Member States were involved in the preparation of the study (P) and/or the workshop (E).
Objective 1.2. NIS threat landscape and analysis		
Output O.1.2.1. Annual ETL report	Engagement of more than 10 Member States in discussions and work related to the structure and content of the ETL report. More than 5 000 downloads of the ETL report. Engagement of more than 80 CTI experts from industry, academia and Member States. Participation of at least 7 5G experts in the review of the report. Participation of at least 18 Member States in the NIS CG team supporting the activity. At least 10 000 views of the delivered report. Provision of input by at least 10 Member States on the consolidated report. At least 5 000 views of the delivered report.	Delivery of report postponed due to emergent 5G activities. CTI EU Event[15] took place in January 2020. It triggered wide interest (approximately 180 participants and approximately 13 companies participated in showroom; all relevant EU organisations contributed).

15 https://www.enisa.europa.eu/events/2019-cti-eu/2019-cti-eu-bonding-eu-cyber-threat-intelligence

Summary of outputs from Activity 1: EXPERTISE – Anticipate and support Europe in facing emerging NIS challenges		
Outputs	**Performance indicator**	**Results achieved**
Output O.1.2.2. Restricted and public info notes on NIS	Coverage of all major incidents relevant to EU NIS policy priorities. Expanding of coverage to all key ENISA stakeholder groups.	General info notes have not been produced, due to the emergent 5G activities for ENISA.
Output O.1.2.3. Support for 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 small businesses / 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).	28 countries (EU/EFTA/EEA) validated the EU-wide annual telecoms security incidents report and 45 experts from telecoms security authorities joined the Article 13a meetings in Stockholm, Ljubljana and Belgrade (E). 29 countries (EU/EFTA/EEA) validated the EU-wide annual trust services security incidents report and 40 experts from trust service supervisory bodies joined the Article 19 meetings in Tirana and Paris (E). 12 countries and 20 experts were involved in NIS CG work stream 3, which validated the breach-reporting synergies paper (P).
Output O.1.2.4. Regular technical reports on the state of cybersecurity	Engagement of CTI stakeholders and CSIRT community.	Engaged CTI stakeholders and CSIRT community in producing a report on the state of software vulnerabilities for 2018/2019.
Objective 1.3. Research, development and innovation		
Output O.1.3.1. Supporting cybersecurity public–private partnership in establishing priorities for EU research and development	No papers to be produced.	Involved ECSO and its members in the definition and review of the research and development directions for EU digital sovereignty. Secretariat support was provided to the National Public Administration Committee. Two meetings took place: one on 19 February and one on 28 May 2019.
Objective 1.4. Response to Article 14 requests under expertise activity and associated outputs are removed following amendment 5 to the 2019 work programme		

2 ACTIVITY 2: POLICY

Promote NIS as an EU policy priority

2.1 Key results in the implementation of Activity 2: POLICY

2.1.1 Objective 1: Supporting EU policy development – outputs

O.2.1.1. Supporting EU policy development

Main achievement:

- Signing of the CSA on 17 June 2019.

In 2019, ENISA supported the work on the legislative and policy developments leading to the official publication of the CSA, which came into force on 27 June.

ENISA continued working towards meeting preparatory requirements for the certification framework for ICT security products and services by, for example, promoting mutual recognition or harmonisation of certification practices up to a certain level, in line with the provisions of the act. The activities in the area of cybersecurity certification were performed in line with the existing national efforts and interests as well as the principle that, wherever possible, decisions must be taken at the level of government closest to the public (i.e. the principle of 'subsidiarity') that applies in the area of certification, while taking into consideration the ongoing legislative process.

ENISA provided support to the Commission and the Member States in the policy area on certification of products and services within the scope of the approved CSA and to better support the new EU cybersecurity certification framework for products and services. Within this framework, ENISA entered

the final steps of the CSA. ENISA subsequently endeavoured to stimulate the interaction and involvement of Member States' governments as well as public policy and industry stakeholders before the emergence of the EU certification framework. The final approval of the CSA required ENISA to maintain excellent cooperation with Member States' governments while transitioning from policy preparation to policy implementation. The achievement of the CSA is evidence of that success.

ENISA provided support for the organisation of the EU cybersecurity certification framework. It supported the Commission in its role in the European Cybersecurity Certification Group (ECCG) and analysed aspects of functional equivalence of existing certification schemes across the EU with the emerging EU certification framework in order to facilitate the transition to the new EU framework. ENISA further developed its interaction with key stakeholders associated with the EU cybersecurity certification framework.

2.1.2 Objective 2: Supporting EU policy implementation – outputs

O.2.2.1. Recommendations supporting implementation of the eIDAS regulation

Main achievements:

ENISA continued its work on supporting public and private bodies in implementing the electronic identification and trust services (eIDAS) regulation by addressing technological aspects and building blocks for trust services. Deliverables throughout 2020 were determined in consultation with the Commission and with public authorities in the Member States through the eIDAS Expert Group. Interacting with the private sector enhanced ENISA's ability to make further meaningful contributions in this area. In implementing the CSA, ENISA supported the Member States' and the Commission's efforts in electronic identification. The eIDAS Expert Group was consulted for approval on specific ENISA implementation guidelines and technical recommendations addressing operational aspects of trust service providers, conformity assessment bodies and supervisory authorities. ENISA continued to accumulate experience of best-practice and state-of-the-art progress, seeking to emphasise implementation and interoperability. These recommendations complemented the existing knowledge base that ENISA created for the trust service providers. ENISA took into account the recommendations and standards developed by the European Committee for Standardisation (CEN) / the European Committee for Electrotechnical Standardisation (CENELEC), the European Telecommunications Standards Institute (ETSI) and the International Organization for Standardization and sought to avoid both duplication of work and potentially opposing approaches. In this regard, ENISA supported the Commission in assessing the relevant standards by reviewing how they met the requirements of the eIDAS regulation.

O.2.2.2. Supporting the implementation of the work programme of the NIS CG

Main achievements:

ENISA completed another year of strong support of the NIS CG, in close collaboration with the members of the group and the Commission. Projects included the work on the European Parliament elections and on the 5G risks and toolbox. ENISA continued to engage closely with many different groups of sectorial authorities and regulators in the different work streams. ENISA supported all work streams with drafting reports, performing analyses and conducting seminars on various sectors and topics, such as the energy sector, digital service providers (DSPs), the digital infrastructure sector, security measures, dependencies, blueprints, elections, etc.

The working group of DSP authorities, under NIS CG work stream 5, validated and worked closely with ENISA on the NISD digital services scope / decision tree – a working document, validated and delivered to the work stream (accessible via the Communication and Information Resource Centre for Administrations, Businesses and Citizens only).

ENISA hosted work streams 5 (digital services) and 10 (digital infrastructures), organising the following.

- Two working meetings in Athens.
- A joint exercise for authorities.
- A seminar by the **Réseaux IP Européens Network Coordination Centre** (a regional internet registry covering Europe, the former USSR and West Asia; RIPENCC) on internet infrastructure.
- A training session on cloud security. Over the week 60 experts from different authorities attended.

ENISA heavily supported the work on 5G, consolidating national risk assessments and developing a 5G toolbox. This important work was completed on time, and was well appreciated upon its publication by the Commission in January 2020.

O.2.2.3. Assist Member States in the implementation of security requirements for operators of essential services and DSPs

Main achievements:

In 2019, ENISA contributed to addressing the challenge posed by the different security requirements stemming from multiple regulatory frameworks by issuing a report on the provisions on operators of essential services (OESs) and DSPs laid down by the NISD, as well as the general data protection regulation (GDPR). The report aims to provide a harmonised approach to using the available ENISA guidance – an approach that can also be used by any organisation that plans to implement security measures appropriate for the security of network and information systems as well as for personal data protection. The report was disseminated at the NIS CG plenary meeting in September.

In 2019 ENISA developed a web tool that provides interactive mapping of security measures for OESs, defined by the NIS CG[16], onto international standards from different business sectors mentioned in Annex 2 to the NISD. The tool was presented in the last NIS CG plenary of 2019 and was welcomed by the Member States. It is available on the ENISA website[17].

O.2.2.4. Supporting the implementation of the payment services directive

This output was removed following amendment 7 to the 2019 work programme[18] to reflect organisational changes while taking on board new tasks and new priorities (i.e. MeliCERTes, a project funded by the EU to connect CSIRTS around the Member States).

O.2.2.5. Contribute to the EU policy in the area of privacy and data protection with policy input on security measures

Main achievements:

- the seventh Annual Privacy Forum (APF) held in cooperation with the University Tor Vergata and LUISS University and with the support of the Garante per la protezione dei dati personali (the Italian Data Protection Authority);
- report on data pseudonymisation.

Within the scope of security measures required by the legal framework on personal data protection and privacy as well as appropriate provisions of the draft CSA on the role of ENISA in this area, ENISA continued promoting trust and security in digital services by means of technical analyses on the implementation of EU legislation addressing privacy and personal data protection.

In particular, ENISA addressed aspects of shaping technology in accordance with GDPR, with a special focus on data pseudonymisation. The main outcome is a report based on ENISA's past work in the field and provides an analysis of key pseudonymisation techniques, along with specific use cases and relevant scenarios.

In addition, following previous work on the security of personal data processing, ENISA published a web tool[19] and a manual. These were developed to support controllers and processors in performing risk assessments and adopting security measures for the protection of their personal data.

The seventh APF – a conference that has grown to be a major event for ENISA – remained the instrument of choice to bring together key communities, namely those of policy, academia and industry, in the broader area of privacy and data protection while focusing on privacy-related areas of application. The 2019 APF took place in Rome, in cooperation with the University Tor Vergata and LUISS University and with the support of the Italian Data Protection Authority[20].

Cooperation activities with Commission services, the European data protection supervisor (EDPS), the European Data Protection Board and national data protection authorities were further pursued. In this context, a conference on personal data breaches was jointly organised with the EDPS. Moreover, an invitation-only workshop on data pseudonymisation was co-organised by the *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (ULD) (the German data protection authority of Schleswig-Holstein) and ENISA.

ENISA continued promoting the visibility of security measures for data protection and privacy, through considerations of IT security of products on the one hand, and through the area of certification of services on the other. ENISA liaised with stakeholders and policymakers as well as with competent authorities

16 NIS CG Publication 01/2018, 'Reference document on security measures for Operators of Essential Services', available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643

17 https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services

18 https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/MBDecision%202019_3amending%20PD2019%20and%20adjusting%20budget2019.pdf/view

19 https://www.enisa.europa.eu/risk-level-tool/

20 https://2019.privacyforum.eu/

in the Member States and EU institutions to identify potential for synergy between privacy and security and assistance for key stakeholders, namely the Commission and competent EU bodies.

O.2.2.6. Guidelines for EU standardisation in ICT security

Main achievements:

Building on its own policy work, existing standards and the requirements of the Member States, this activity makes recurrent contributions in terms of gap analyses and/or provides guidance on implementing existing cybersecurity standards.

Additionally, ENISA maintains the relationship developed with the EU and international standardisation organisations (CEN/CENELEC and ETSI; International Organization for Standardization and International Electrotechnical Commission). It thus contributes to their standardisation work at the strategic and tactical levels. For instance, it facilitates cooperation between the relevant technical committees of ETSI (Technical Committee – Cybersecurity) and CEN/CENELEC (Joint Technical Committee 13). It also promotes participation in various conference programme committees, and organises highly recognised and well-attended standardisation conferences.

New requirements associated primarily with the implementation and secondly with the transposition of the EU legal instruments in place in the Member States will be taken into account. These requirements include aspects of the NISD and the GDPR, as well as the preparation for the entry into force of the draft ePrivacy regulation, the draft CSA and more.

ENISA contributed to this relationship with its technical and organisational knowledge, which was further leveraged in extending or assessing standards, the objective being to tailor them to stakeholders while making them compliant with the prevailing regulatory framework. Of particular importance is the participation of ENISA in the work of the International Organization for Standardization Subcommittee 27.

In carrying out this work, ENISA consulted the Member States, industry and standard-developing organisations (e.g. ETSI, CEN/CENELEC, International Organisation for Standardization). ENISA organised an annual conference on cybersecurity standards with these organisations and consulted with the Commission services and agencies endowed with competence for policy as appropriate.

O.2.2.7. Supporting the implementation of the European Electronic Communications Code

Main achievements:

- telecoms security event in Stockholm;
- ETIS[21] Information Security Working Group meeting;
- report "security supervision changes under the European Electronic Communications Code" (EECC).

The telecoms security event in Stockholm had an attendance of 75 experts, from both the public and the private sector. At this event, the Commission and ENISA gave talks about the upcoming EECC.

ENISA hosted and organised the ETIS Information Security Working Group in Athens beginning of 2019. At this industry event, one of the most important ISAC groups for telecoms, initial discussions on the EECC took place with the industry experts.

In 2019, ENISA produced and delivered a seminal paper for the future work on the EECC: 'Telecoms security supervision changes under the EECC', based on legal analyses and discussions with regulators, ministries, the Commission and the private sector. The paper was validated by all 28 countries in the group. Intermediate drafts were discussed during meetings held in June and October with the regulator. A solid basis was laid for the future work with the EU Member States on telecoms security supervision.

O.2.2.8. Supporting the sectorial implementation of the NISD

Main achievements:

- Transport Cyber Security Conference organised with DG Mobility and Transport, the European Union Aviation Safety Agency (EASA), EMSA and the European Union Agency for Railways (ERA), held on 23 January 2019;
- establishment of the Transport Resilience and Security Expert Group;
- facilitating the European Rail ISAC;
- energy sector survey.

On 23 January 2019 in Lisbon, ENISA held the first Transport Cyber Security Conference.

21 https://www.etis.org/page/About_Us

The conference had the support of the European Commission (DG Mobility and Transport), EASA, EMSA and ERA.

More than 170 public and private partners from all over Europe, representing all modes of transport, took part in the event. Together, they discussed the EU legal framework for cybersecurity and its relevance for the transport sector, and explored options for further cooperation.

The discussions demonstrated the importance of intensifying the cooperation between DG Mobility and Transport, DG Communications Networks, Content and Technology, ENISA, EASA, EMSA and ERA to raise the level of cybersecurity in transport.

In addition, ENISA established the Transport Resilience and Security Expert Group in 2019 to support its activities in the transport sector.

In 2019, the European Rail ISAC was launched and two general assemblies took place over the course of the year. Cybersecurity professionals from European infrastructure managers and railway undertakings met and exchanged information on cybersecurity issues. Together, they planned the next steps to increase cybersecurity capabilities and raise awareness in the sector. Initially more than eight Member States were members of the European Rail ISAC, which has been heavily supported and facilitated by ENISA (as a partner).

In 2019, ENISA conducted a survey along with a set of interviews with various stakeholders from the energy sector in order to identify challenges and good cybersecurity practices. The preliminary results were examined with the members of the NIS CG work stream 8 (energy) (covering 15 Member States). Based on the information collected, the agency will consider the priorities of the energy utilities and cybersecurity trends in the energy sector in general.

O.2.2.9. Hands-on tasks in the area of certification of products and services

Main achievements:

Having adopted the finally approved CSA and its component on certification, ENISA started to support the Commission and the Member States by carrying out hands-on tasks in this area designed to assist them in deploying the framework.

ENISA is developing a framework for certification schemes, along with carrying out structured interactions with the stakeholder community, and has started to provide the procedures and tools required to implement the new tasks.

Working in cooperation with Member States' certification supervisory authorities, the ECCG and other key stakeholders, ENISA set the stage for implementation. To that end, ENISA supports the functional equivalence of existing certification schemes across the EU (at both the national and the EU level) with the emerging EU cybersecurity certification framework for integrating existing schemes into the new EU framework in a flexible way.

ENISA maintained its cooperation with stakeholders to collect, establish and understand their expectations of the EU cybersecurity certification framework.

ENISA implemented an action plan to accelerate the launch of the new tasks pertaining to the cybersecurity certification framework for the benefit of the Member States.

Practical aspects to be considered included but were not limited to:

- identifying new areas in certification;
- recommendations of next steps to take at EU level;
- analysis of impact of certification for manufacturers;
- Supporting governments and end users;
- recommendations on prioritisation of schemes;
- review of overlaps between and gaps in proposed schemes.

Concretely, ENISA launched two ad hoc working groups to respond to the 2 requests received in the area, specifically on:

(a) a cybersecurity certification scheme in the area of common criteria for transposing the Senior Officials Group Information Systems Security Mutual Recognition Agreement; and on

(b) a cybersecurity certification scheme in the area of cloud services.

ENISA assisted the Commission in launching and supporting the ECCG. It also prepared a proposal in relation to the membership of the Stakeholder Cybersecurity Certification Group.

ENISA carried out support activities in the area of certification through an annual conference and a validation workshop.

ENISA carried out very important preparatory work internally to develop a platform dedicated to

the support of the ad hoc working group in their certification tasks as provided for in the CSA. ENISA worked further on implementing a new infrastructure for web-based activities mandated by the CSA.

2.2 Outputs and performance indicators 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. Support the preparatory policy discussions in the area of certification of products and services	For all activities but the last one: contribution/participation of more than 10 private companies and 10 EU Member State representatives to/in the activity. For the last activity: in close cooperation with the Commission.	Presentation of the action plan for the implementation of the certification management IT platform at a workshop organised by ENISA, attended by more than 50 people from more than 10 Member States and more than 10 private organisations. Validation of the report on transposition of existing schemes, by 17 Member States, and presentation of the report to the ECCG (28 Member States). ENISA's active support for the Commission in the ECCG meetings.
Objective 2.2. Supporting EU policy implementation		
Output O.2.2.1. Recommendations for technical implementations 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.	5 Member States and H422 from the Commission provided detailed feedback and validated the results of the report. Results were further presented and approved by all 27 Member State stakeholders of the Cooperation Network. The qualified trust service provider report was reviewed by private organisations (browsers and qualified trust service providers) and was presented and accepted by more than 20 Member States at the Article 19 event. The 2019 Trust Services Forum was attended by 250 participants.
Output O.2.2.2. Supporting the implementation of the work programme of the NIS CG under the NISD	Engagement of at least 12 Member States in ENISA's contributions to the implementation of the NISD (S). Participation of 10 Member States in the workshop/activity (E). Engagement of at least 12 Member States in ENISA's contributions to NIS CG work on 5G cybersecurity (S).	The working group of DSP authorities (20 Member States), under NIS CG work stream 5, validated the NISD digital services scope / decision tree (S). ENISA hosted meetings on work streams 5 (digital services) and 10 (digital infrastructures) in Athens, attended by 60 experts from different authorities (E). ENISA worked on 5G national risk assessment and the 5G toolbox in collaboration with 28 Member States (S).
Output O.2.2.3. Assist Member States in the implementation of OES and DSP security requirements	Engagement of 12 Member States in taking stock of good practices for OESs and DSPs (P). Participation of more than 10 Member States and 15 OESs in the workshops/activities (E).	The NIS CG (28 Member States) was involved in the design phase of the tool for mapping the baseline security measures (P). In addition, 5 Member States requested that their national security requirements appear in the tool. The report on security requirements from different legal frameworks (P) was discussed and reviewed with various stakeholders: over 40 DSPs during a conference in Helsinki, 25 energy OESs which are members of the European Energy ISAC and the NIS CG (28 Member States). 18 OES representatives from 15 Member States participated in a workshop ENISA organised to validate the dependency scenarios (E).

22 «eGovernment & Trust3» unit of the Direction Générale Communications Networks, Content and Technology (CONNECT) of the European Commission: https://ec.europa.eu/digital-single-market/en/content/egovernment-and-trust-unit-h4.

Summary of outputs from Activity 2: POLICY – Promote NIS as an EU policy priority		
Outputs	**Performance indicator**	**Results achieved**
Output O.2.2.5. Contribute to EU policy in the area of privacy and data protection with policy input on security measures	Engagement of more than 40 participants from relevant communities, including DSPs, data controllers and national bodies, in the activity. Participation of at least 5 representatives from different bodies / Member States in the preparation of the recommendations. More than 60 participants from relevant communities.	195 participants in EDPS–ENISA workshop; 52 participants in closed (i.e. invitation-only) ULD–ENISA workshop. 7 contributors to the report from 5 different Member States; validation of the report at ULD–ENISA workshop (approximately 50 participants from across the EU). 6 contributors to the web tool from different Member States / EU bodies. 198 participants from different communities (data protection authorities, EU bodies, research, industry).
Output O.2.2.6. Guidelines for European standardisation in ICT security	Participation of at least 5 representatives of European standardisation organisations and relevant services of the Commission and/or agencies in the drafting and review of the guidelines.	Papers related to standardisation were drafted by 10 experts and distributed among about 20 further experts on standards for comment. The standardisation conference co-organised by ENISA attracted 250 participants in 2019.
Output O.2.2.7. Supporting the implementation of the EECC	Participation of at least 10 Member States and 5 providers in the activities/ workshops related to the new EECC.	The Commission and ENISA discussed the upcoming EECC and validated their approach during the telecoms security event in Stockholm, Sweden, which had an attendance of 75 experts, from across the public and private sector (E). The paper 'Telecoms security supervision changes under the EECC' (S), based on legal analyses and discussions with regulators, ministries, the Commission and the private sector, was validated by all 28 countries in the group.
O.2.2.8. Supporting the sectorial implementation of the NISD	Engagement of 12 Member States and 10 OES organisations in NISD sector-specific initiatives.	70 energy operators participated in taking stock of good cybersecurity practices for the energy sector (S). The preliminary results were discussed with the members of the NIS CG work stream 8 (energy) (15 Member States). 25 Member States and more than 40 OESs from the transport sector participated in the Transport Cyber Security Conference in Lisbon (S). 13 Member States and 20 OESs from the energy sector participated in the joint NISD work stream 8–European Energy ISAC meeting in Brussels (S).
O.2.2.9. Hands-on tasks in the area of certification of products and services	Engagement of stakeholders from at least 15 EU Member States.	ENISA projects in the area of certification were reviewed and widely discussed among multiple stakeholders from different sectors – the Commission, Member States, industry, etc. Practically all Member States participated in the review.
Objective 2.3. Response to Article 14 requests under policy activity and associated outputs are removed following amendment 8 to the 2019 work programme		

3 ACTIVITY 3: CAPACITY

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

3.1 Key results in the implementation of Activity 3: CAPACITY

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

O.3.1.1. Update and provide technical training for Member States and EU bodies

Main achievements:

- update of guidelines on good practices and of training materials;
- pilot course dedicated to information security risk management co-organised with and hosted by the European Security and Defence College.

In 2019 most of the activities in this area aimed at maintaining and extending the guidelines on good practices and training materials for CSIRTs and other operational personnel.

ENISA supported the development of Member States' incident-response preparedness by providing guidance on good practices in key elements of NIS capacity building. The focus was on CSIRT training and services in order to improve CSIRTs' skills and those of their personnel.

In detail, ENISA performed the necessary updates of the training material, according to the findings of the study taking stock of training needs in NISD sectors. A new set of training materials based on emerging technologies was created in order to improve Member State CSIRTs' skills and capacities to manage cybersecurity incidents more efficiently.

A special emphasis was placed on supporting Member States' CSIRTs and EU bodies with concrete advice such as examples of good practice and concrete actions such as the CSIRT training.

ENISA also directly provided tailor-made technical training and advice to Member States that requested such support.

In 2019, ENISA further enhanced its methodology, seminars and training on:

(a) cyber-crisis management;

(b) the organisation and management of exercises.

These developments stemmed from the existing materials and infrastructure for on-site and online training on these subjects. In addition, this activity included delivering training upon request.

On 12 and 13 September 2019, ENISA, in collaboration with the European Security and Defence College, organised and hosted a pilot course dedicated to information security risk management.

The 2-day course was attended by 27 experts from 9 Member States and 4 EU institutions at the ENISA branch office in Heraklion, Crete. Through bolstering their cybersecurity knowledge and exchanging experiences and good practices, they honed their skills and capabilities in cybersecurity and risk management.

All participants shared the opinion that the course should be made available every year.

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

Main achievements:

- report on good practices and innovation under the national cybersecurity strategies (NCSSs);
- the updated interactive NCSS map;
- seventh national cybersecurity workshop in Warsaw, organised with **Naukowa i Akademicka Sieć Komputerowa** (Research and Academic Computer Network, NASK) Poland.

ENISA issued a report addressing challenges, good practices and recommendations from the Member States in their efforts to execute innovation as a strategic priority of their NCSSs.

The report analyses different Member States' innovation approaches, stakeholders, challenges, funding mechanisms and initiatives that support innovation objectives at a national level. Through interviews, 15 stakeholders from 12 Member States provided input and validated the results of the report.

A new version of the interactive NCSS map was released in 2019. It became an info hub with information provided by the Member States in their efforts to enhance their cybersecurity at national level. Designed with the most up-to-date information, the map is considered a valuable asset by the community.

On 26 September, ENISA, in collaboration with NASK Poland, held the seventh national cybersecurity workshop in Warsaw.

A total of 78 stakeholders from national competent authorities, private and public organisations, academia and CSIRTs were present.

ENISA presented the report on good practices in innovation under NCSSs and the updated NCSS map. The event focused on 'innovation in cybersecurity', covering Member States' approaches and initiatives and presented by officials from Spain, Austria, Poland, the United Kingdom, the Commission and ENISA.

Stakeholders from national and EU ISACs such as those for the energy, financial and rail sectors shared their experiences with the tools they use, good practices and the challenges they face when dealing with information sharing and cooperation.

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

Main achievements:

In 2019, ENISA assisted the Member States in improving their incident-response capabilities by providing an updated perspective on the CSIRT landscape and its development in Europe.

In close cooperation with the NISD CSIRT Network, ENISA supported the development of the Member States' incident-response capabilities by providing recommendations on key dimensions of NIS capability building with a focus on the development and efficient functioning of national and sectorial CSIRTs.

ENISA offered direct support to individual Member States that requested the assessment and improvement of their incident-response capabilities, including assistance in the preparatory phase of the Connecting Europe Facility (CEF) proposals.

ENISA helped Member States and other incident-response stakeholders, such as the EU institutions, bodies and agencies, to develop, extend and deploy their incident-response capabilities and services in order to meet the ever-growing challenges of securing their networks.

The agency further developed and applied its own recommendations for CSIRT baseline capabilities and a maturity framework. It conducted four peer reviews to assess the maturity level of CSIRT Network members and supported CSIRT Network members in conducting their own peer reviews.

ENISA maintained its support for cross-border CSIRT community projects and development of tools, and continued to engage in the global dialogue on common definitions and maturity frameworks in the incident-response domain.

ENISA's experts on incident response became certified Security Incident Management Maturity Model (SIM3) auditors to enhance the performance of CSIRTs in the EU.

In 2019, ENISA assisted the Member States in improving their incident-response capabilities by providing an updated perspective on the CSIRT landscape and its development in Europe.

O.3.1.4. Support EU Member States in the development of ISACs for the NISD sectors

Main achievements:

- 13th European Energy ISAC plenary meeting, on 26 and 27 November 2019;
- first inter-EU-ISAC meeting, on 10 October 2019.

ENISA has been engaged in close cooperation with the EU's OESs over the years.

A number of sectorial expert groups were set up, covering sectors such as transport, finance and health.

ENISA actively supports sectorial ISACs, such as the European Energy ISAC, the European Financial Institutes ISAC and the European Rail ISAC.

On 26 and 27 November 2019, ENISA held the 13th European Energy ISAC plenary meeting.

Energy sector stakeholders had the opportunity to exchange views on critical infrastructure threat analysis, the activities of the energy community and NISD-related challenges for energy operators.

The open session saw participation from 50 experts. On 28 November, a training session on network forensics, tailored to the needs of the energy sector community, was delivered to the plenary participants by ENISA.

The training room was fully booked and the participants expressed a wish to see ENISA organise a similar initiative in the near future. This confirms the success and the need for such an event. Five Member States and three OESs signed up for an extra activity, namely the European Supervisory Control and Data Acquisition and Control System Information Exchange (EuroSCSIE) meeting.

On 10 October 2019, ENISA held the first-ever inter-EU-ISAC meeting. The purpose of the meeting was to bring together the chairs of the existing EU-wide ISACs in order to discuss both administrative and operational challenges and identify possible solutions and ways to ensure close collaboration in the future.

In addition, the event gave the Commission the opportunity to engage the ISACs in the dialogue on the funding opportunities available through the CEF telecoms project.

The participants welcomed this initiative from ENISA and agreed to organise the meeting on a yearly basis from then on.

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

O.3.2.1. Representation of ENISA on the CERT-EU Steering Board and coordination with other EU agencies using CERT-EU services

Main achievements:

The members of the Computer Emergency Response Team for the EU Institutions, Bodies and Agencies (CERT-EU) Steering Board include the participating EU institutions and ENISA, representing the EU agencies using CERT-EU services.

In this context ENISA is actively engaged in the activities of the CERT-EU Steering Board on a permanent basis.

In 2019, ENISA maintained its cooperation with the EU agencies on operational issues related to CERT-EU's activities, in particular through the ICT Advisory Committee of the EU agencies. ENISA's role in this context is to ensure that the viewpoints of the agencies are adequately represented.

ENISA also reports to the CERT-EU Steering Board on the evolution of services required by the agencies.

O.3.2.2. Cooperation with relevant EU bodies on initiatives covering the NIS dimension of their missions

Main achievements:

ENISA has seen its cooperation efforts with a number of EU bodies increase since 2017. ENISA has been involved in the following:

- cooperation with CERT-EU in the context of the WannaCry incident;
- providing support in the context of the annual International Conference on Cyber Conflict (CyCon) between Cyber Europe, Cyber Coalition and Locked Shields;
- contribution to the preparation of the tabletop exercise conducted in the context of the Estonian Presidency.

In this context, ENISA strengthened its cooperation efforts and continued to engage and liaise with the relevant EU bodies[23] (such as EASA, CERT-EU, the European Defence Agency (EDA) – including civil/defence cooperation – etc.).

ENISA also engaged with the European Union Institute for Security Studies and the Commission's Service for Foreign Policy Instruments in delivering the first EU Cyber Forum, and showcased cybersecurity work in the EU.

3.1.3 Objective 3: Assisting in improving private sector capacity building and general awareness – outputs

O.3.3.1. European Cyber Security Challenges

Main achievements:

- supporting the sixth ECSC, in Bucharest from 9 to 11 October 2019.

The sixth ECSC, ECSC 2019, took place in Bucharest from 9 to 11 October.

23 Memorandum of understanding between ENISA, the EDA, Europol's European Cybercrime Centre (EC3) and CERT-EU (see: https://www.eda.europa.eu/docs/default-source/documents/mou–eda-enisa-cert-eu-ec3–23-05-18.pdf).

The event was organised by the *Asociația Națională pentru Securitatea Sistemelor Informatice* (the Romanian national association for information systems security) and the *Centrul Național de Răspuns la Incidente de Securitate Cibernetică* (the national cybersecurity and incident-response team) and held at the Palace of the Parliament.

Each country was represented at the ECSC final by a team of 10 contestants, all winners of the national competitions. The ages of half the participants ranged from 14 to 20 while the other half ranged from 21 to 25.

In total, the event brought together 300 people, representing contestants, coaches and judges, all of whom competed in the ECSC final in Bucharest and covered a total of 20 EU and EFTA countries (Austria, Cyprus, Czechia, Denmark, Estonia, France, Germany, Greece, Ireland, Italy, Liechtenstein, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Switzerland and the United Kingdom).

The participants investigated vulnerabilities in web applications, binaries and document files, solved puzzles with cryptographic componentscryptograms and hacked hardware systems.

However, technical skills were just one part of the story. Teamwork and presentation skills were also evaluated, allowing a significant range of the important skills for an IT security team to be tested. The finalists of ECSC 2019 were the teams from Romania[24], Italy and Austria.

ENISA is actively hosting different platforms and performing different activities to support the ECSC host country and the evolution of the project. These include:

- the main ECSC website;
- the ECSC information-sharing platform;
- a common public affairs strategy;
- designing challenges scenarios.

In addition, ENISA is working closely with the host of each ECSC in order to ensure appropriate and transparent reporting to the steering committee.

O.3.3.2. European Cyber Security Month

Main achievements:

The metrics built into the ECSM show an increased number of participants and a better engagement level in 2019 than in 2018.

The 2019 campaign had a different format to that of previous years. The activities were developed around two themes: cyber hygiene and emerging technology. According to the report, the conferences and workshops attracted nearly three times more visitors than in previous years.

In 2019, ENISA continued to engage with Member States and the public alike to promote cybersecurity.

Previously proposed pillars remain: support for a multi-stakeholder governance approach; encouraging common public–private activities; assessment of the impact of activities, optimising them and adapting to new challenges as appropriate.

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

Main achievements:

ENISA performed an analysis of the EU and international initiatives in the field of cyber skills development and collected input from EU Member States on their policies in the field of cybersecurity education. These gave rise to the two following initiatives.

a. A White Paper entitled **Cybersecurity Skills Development in the EU**. The paper focuses on the state of the cybersecurity education system and its inability to attract more students to the area of cybersecurity. It provides considerations and recommendations for policy interventions at national and EU level in order to address the shortage of cybersecurity skills.

b. The Cybersecurity Higher Education Database. The database's[25] objective is to become the focal point of reference for all members of the EU public who seek to improve their cybersecurity knowledge and skills. This will allow young talent to make informed decisions on the variety of possibilities offered by higher education in cybersecurity and will help universities attract high-calibre students motivated to ensure cybersecurity for the EU.

24 https://europeancybersecuritychallenge.eu/past-editions

25 Cybersecurity Higher Education Database

3.2 Outputs and performance indicators 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. Update and provide technical training for Member States and EU bodies	Update of at least 1 training resource to support operational practices of CSIRTs in Europe. Coverage of at least 1 critical NISD sector in the training session. Support for at least 3 CSIRT personnel training events.	Updated operational training handbook, *Orchestration of CSIRT Tools*, providing deliverables suitable for the NISD sectors. Delivered training to the European Energy ISAC at the ENISA Athens offices on 26 November 2019. The topic was an introduction to network forensics, with an industrial control systems / supervisory control and data acquisition (ICS/SCADA) use case. Three CSIRT personnel training sessions (TRANSITS[26]) were delivered, with the support of ENISA.
Output O.3.1.2. Support EU Member States in the development and assessment of NCSSs	Engagement of stakeholders from at least 2 EU Member States in using the NCSS assessment methodology (S). Engagement of stakeholders (national competent authorities or the private sector) from at least 12 EU Member States in this activity/workshop (P and E).	2 EU Member State stakeholders were engaged in using the NCSS assessment methodology (S). 78 stakeholders from national competent authorities and from the private sector from 20 Member States were engaged in this activity/workshop (P and E).
Output O.3.1.3. Support EU Member States in their incident-response development	Engagement of or support for at least 5 CSIRTs in the development or improvement of incident-response capabilities in Europe. 2 CSIRT inventory updates. During 2019, provision of support or advice to at least 2 CSIRTs to enhance their maturity. Support from ENISA for at least 2 international CSIRT initiatives in community forums like the Forum of Incident Response and Security Teams, TF-CSIRT-TI[27] or the Global Forum on Cyber Expertise.	Assisted Member States in improving their incident-response capabilities by providing an updated overview of the CSIRT landscape and development in Europe. The *EU MS Incident Response Development Status Report* study (https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report) provided recommendations on key dimensions of NIS capacity building with a focus on the development and efficient functioning of national and sectorial CSIRTs (24 CSIRTs engaged in this study). A new version of the interactive map of European CSIRTs was released, with a new look and feel and improved back end. Major updates were deployed in the second and fourth quarters of the year. A dedicated view of CSIRT new members was integrated into the CSIRT Network public website. In 2019 ENISA conducted four peer reviews to assess the maturity level of CSIRT Network members, and reviewed and updated documents on the CSIRT maturity framework: *ENISA Maturity Evaluation Methodology for CSIRTs* and the *ENISA CSIRT Maturity Assessment Model* for the CSIRT Network. ENISA also further coordinated the continuous update of the 'Reference Security Incident Taxonomy' within the official Task Force on CSIRT's working group. ENISA experts had involvement with the Forum of Incident Response and Security Teams' board of directors (FIRST), the Task Force on CSIRT's steering committee[28] and Open CSIRT Foundation-certified Security Incident Management Maturity Model[29] auditors. ENISA further provided input to the Global Forum on Cyber Expertise and MeliCERTes[30] projects throughout the year.

26 Computer-security and incident-response team (CSIRT) personnel training
27 https://tf-csirt.org/trusted-introducer/
28 https://tf-csirt.org/tf-csirt/steering-committee/
29 https://opencsirt.org/csirt-maturity/sim3-and-references/
30 Melicertes is the name of a project funded by the EU to connect CSIRTS around the Member States.

Summary of outputs in Activity 3: CAPACITY – Support Europe in maintaining state-of-the-art NIS capacities

Outputs	Performance indicator	Results achieved
Output O.3.1.4. Support EU Member States in the development of ISACs for the NISD sectors	Engagement of at least 12 organisations representing at least 3 sectors from at least 8 Member States in this activity (S).	The representatives of EU ISACs (covering 5 sectors and 75 organisations from 28 Member States) were engaged in the dialogue concerning the CEF funding opportunities (S). ENISA facilitated this dialogue by organising the first inter-EU-ISAC meeting (S).
Objective 3.2. Supporting EU institutions in capacity building		
Output O.3.2.1. Representation of ENISA on the CERT-EU Steering Board and coordination with other EU agencies using CERT-EU services	Consultation with EU agencies and representation of their views at the level of CERT-EU Steering Board.	ENISA has strengthened the collaboration between itself and CERT-EU in several operational areas. It continues to be an active contributor to the CERT-EU Steering Board. ENISA represented the EU decentralised agencies and acted as the bridge between them on contractual arrangements and any other matter involving the agencies (the ICTAC[31] sub-network of the EU Agencies network) and CERT-EU. ENISA represented the strategic views of the EU Agencies Network's heads of resources on future relations with CERT-EU.
Output O.3.2.2. Cooperation with relevant EU bodies on initiatives covering the NIS dimension of their missions	Engagement of the relevant EU stakeholders (including EASA, CERT-EU, EDA (including civil/ defence cooperation), etc.).	The reporting on the collaboration, on request, with the European Union Institute for Security Studies and the Commission's Service for Foreign Policy Instruments in delivering the first EU Cyber Forum, as part of the report on requests (including former Article 14 requests) delivered at the end of the year (available here: https://www.enisa.europa.eu/publications/Report-Request-to-ENISA %202019).
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 2019 and their participation in the ECSC final.	4 new countries participated in the ECSC final in Bucharest. Award activities performed. ENISA participated in the Connect University 'getaway day' in Brussels.
Output O.3.3.2. Deployment of the ECSM	Participation/support of all 28 EU Member States and at least 10 partners and representatives from different bodies / Member States in/for ECSM 2019 (private and public sectors).	Support provided to the Member States throughout the year in preparation for the campaign and in particular during the campaign month of October with the production of videos, infographics and graphics translated into the Member States' local languages. The evaluation report captured the results of the campaign and the efforts made by each Member State.
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.	Input from all Member States on policies for development of cybersecurity skills and cybersecurity degree certification was collected. More than 20 academic representatives were involved with the Cybersecurity Higher Education Database.
Objective 3.4. Response to Article 14 requests under capacity activity and associated outputs are removed following amendment 11 to the 2019 work programme		

31 The information and communications technologies advisory committee (ICTAC).

4 ACTIVITY 4: COMMUNITY

Foster the emerging European NIS community

4.1 Key results in the implementation of Activity 4: COMMUNITY

4.1.1 Objective 1: Cyber-crisis cooperation – outputs

O.4.1.1. Planning of Cyber Europe 2020 and Cyber SOPEx

Main achievements:

- planning of sixth pan-European cyber exercise – Cyber Europe 2020;
- Cyber Standard Operating Procedures Exercise (SOPEx).

ENISA managed to finalise the preparations for the sixth pan-European cyber exercise, Cyber Europe 2020. The preparations closely followed up on and built on the lessons learned and actions from previous exercises, such as Cyber Europe 2018.

Cyber Europe 2020 was designed to focus on the health sector's testing capabilities and procedures, namely large-scale incident management cooperation procedures at EU and national level.

The crisis escalation scenario includes 18 distinct realistic incidents focused on capturing real life more accurately. The exercise includes explicit scenarios for the CSIRT Network, the EU institutions and the operational cooperation single points of contact and competent authorities as identified in the blueprint.

ENISA also organised the Cyber SOPEx (formerly known as EuroSOPEx) for the CSIRT Network to increase cooperation. As in previous years, the exercise was planned with the support of representatives from the organisations involved.

The exercise had a number of objectives: to raise awareness of cooperation procedures, to train participants in using cooperation infrastructures such as communication and information sharing and ultimately to contribute to increasing trust within the CSIRT Network.

The theme of the scenario was the European Parliament elections.

O.4.1.2. Support activities for cyber exercises

Main achievements:

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

The CEP hosts a number of services that ENISA offers to Member States and EU institutions, such as: exercise organisation and management, an exercise playground with technical incidents, a map of exercises and the hosting of the exercise development community.

In addition, new content and practice incidents and material were developed in order to maintain the interest of the stakeholders and to make the CEP a central tool in cybersecurity practice exercises for all stakeholders.

The CEP opens up new opportunities for ENISA to enlarge its user base and thus offer the operational cybersecurity communities opportunities to practise and gain experience and knowledge.

In 2019, the CEP was used to host a national exercise for the first time. The Portuguese National Cyber Security Centre held Portugal's national cyber exercise in May 2019, using the unique exercise management infrastructure developed by ENISA.

O.4.1.3. Support the implementation and further development of the cyber-crisis collaboration blueprint

Main achievements:

- first EU tabletop exercise, code-named 'EU ELEx19', on 5 April 2019;
- first *cyber law enforcement exercise,* 'CyLEEx19', on 31 October 2019;
- conference on the future of EU cyber-crisis management on 3 and 4 June 2019.

ENISA continued to be committed to supporting the implementation and development of the EU cyber-crisis management blueprint in 2019.

As specified in the blueprint, '[c]yber crisis response activities should be coordinated with other crisis management mechanisms at EU, national or sectoral levels.'

ENISA maintained its efforts to offer continuous support to the Commission in further developing bilateral and multilateral standard operating procedures (SOPs) for cyber-crisis cooperation with

EU bodies and institutions, and to Member States. It does so either through the NIS CG's activities or by responding to individual requests from Member States for the development of SOP blueprints at national level.

In addition, ENISA supported EU institutions and Member States in testing their crisis management structures, as explained below.

The Parliament, the Member States, the Commission and ENISA organised this first EU tabletop exercise, code-named EU ELEx19, on 5 April 2019.

The objective of the exercise, carried out on the Parliament premises, was to test the effectiveness of national and EU crisis response practices and plans. It was also designed to identify how any cybersecurity incidents that might arise and affect the 2019 European Parliament elections could be prevented, detected and mitigated.

The exercise was part of the measures being implemented by the EU to ensure free and fair elections in May 2019. It lasted a full day and the participants included 80 players from 27 Member States, together with observers from the European Parliament, the Commission and ENISA.

Europol's European Cybercrime Centre (EC3) and ENISA successfully co-organised the first-ever cyber law enforcement exercise, called 'CyLEEx19', on 31 October 2019.

This exercise, held in a simulated environment, was designed to:

- test the European Union Law Enforcement Emergency Response Protocol[32];
- identify deficiencies and potential for improvement;
- increase preparedness in case of a real-life cyberattack;
- evaluate the procedure for aligning the law enforcement agencies' response with other EU bodies that play a role in the EU blueprint.

The cyber simulation took place in a single day. It was a lightweight but intellectually intensive exercise that explored the effects of large-scale transnational cyberattacks on the capability of law enforcement and on the partners involved to carry out their tasks in accordance with the protocol.

Furthermore, on 3 and 4 June 2019, the agency held a conference in Athens, focusing on the future of the EU's cyber-crisis management. The advantages and challenges were identified, particularly where the use of AI is concerned.

The objective of the conference was to provide a discussion forum for the EU organisations and bodies that are the main stakeholders of the blueprint proposal for a cyber-crisis cooperation framework. It also aimed to bring together experts on AI from the private sector and academia to discuss the uses and applications of AI and machine learning in the context of cyber-crisis cooperation, such as how AI can support the response to large-scale cross-border cybersecurity incidents at the strategic and political levels.

O.4.1.4. Supporting the implementation of the information hub

Main achievements:

Intelligence supporting decision-making in the cybersecurity domain is scarce, despite today's security information overload[33].

ENISA is at the crossroads of most if not all public–private, cross-sector cybersecurity communities in Europe, from the technical to the strategic level.

As indicated in the Commission communication on building strong cybersecurity for the EU[34], ENISA serves as the 'focal point for information and knowledge in the cybersecurity community'.

As a result, ENISA is in a unique position to leverage its network to gather information, process it and foster timely, tailored and highly relevant situational awareness to support decision-making in both the public and the private European sectors, as recommended by the Commission in the blueprint.

As part of the regular cooperation at a technical and operational level to support EU situational awareness in the context of the blueprint, ENISA issued EU cybersecurity situation reports on incidents and threats, based on publicly available information, its

32 Europol document EDOC#1012248 (see: https://www.europol.europa.eu/newsroom/news/law-enforcement-agencies-across-eu-prepare-for-major-cross-border-cyber-attacks).

33 Scott J. and Spaniel D., 'CISO Solution Fatigue – overcoming the challenges of cybersecurity solution overload', Hewlett Packard Enterprise, Institute for Critical Infrastructure Technology, 2016 (http://icitech.org/wp-content/uploads/2016/06/CISO-Solution-Fatigue.pdf).

34 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN

own analysis and reports shared with it by Member States' CSIRTs (on a voluntary basis) or NISD single points of contact, EC3 at Europol, CERT-EU and, where appropriate, the European Union Intelligence and Situation Centre at the European External Action Service and other EU institutions.

The report was made available to the relevant bodies of the Council, the Commission, the High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the Commission and the CSIRT Network.

To best support the fusion of open-source information for these reports, ENISA migrated the Open Cyber Situational Awareness Machine (OpenCSAM) platform to an operational environment.

The operational OpenCSAM includes enhanced functionalities and capabilities, building on the experience gained from the first prototype.

The tool received wide acceptance by blueprint stakeholders.

As the first brick of a broader capability, the tool is called 'the ENISA Info Hub'. It is meant to assist in the compilation of input from blueprint stakeholders on the development of EU cybersecurity situation reports, supporting a steady increase and offering guarantees of shorter production times, of quality and of consistency.

O.4.1.5. Supporting the implementation of the cyber-crisis collaboration blueprint

This output was replaced by output O.4.1.3 following amendment 13 to the 2019 work programme[35].

4.1.2 Objective 2: CSIRT and other NIS community building – outputs

O.4.2.1. EU CSIRT Network secretariat and support for EU CSIRT Network community building

Main achievements:

ENISA maintained the activities meant to support the Commission and Member States in the implementation of the NISD, in particular in the area of CSIRTs.

ENISA continued to provide the secretariat of the CSIRT Network and actively supported the network's functioning by suggesting ways to improve cooperation and trust building among CSIRTs.

ENISA also supported this cooperation by developing and providing guidance and examples of good practice in the area of operational community efforts. In this way, ENISA responded to the request by members of the CSIRT Network regarding information exchange and secure communication, for instance.

In particular, ENISA worked on the topics of proactive detection of incidents and secure communications, and the preparation of the second report to the NIS CG as defined by the NISD.

In addition, ENISA had an active role in supporting the CSIRTs in the CSIRT Network in activities related to the CEF work programme. ENISA actively supported teams in testing and use of the Core Service Platform (CSP) cooperation mechanism for CSIRTs, known as MeliCERTes[36].

Trust being an important asset for CSIRT operations, ENISA strived to improve the level of trust in the network by providing one trust-building exercise and three face-to-face meetings in coordination with the CSIRT Network management.

ENISA further improved, developed and secured the CSIRT Network infrastructure (i.e. CSIRT Network Cooperation Portal and other means of communication) to ensure smooth cooperation between members and for its use in administration.

O.4.2.2. Support the fight against cybercrime and collaboration between CSIRTs and law enforcement

Main achievements:

- annual workshop for national and governmental CSIRTs and their law enforcement agency counterparts, co-organised with Europol/EC3;
- cooperation between CSIRTs and law enforcement: interaction with the judiciary.

ENISA provided significant support in the cooperation between the CSIRTs and the law enforcement agencies and in the further cooperation with the judiciary.

35 https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/MBDecision%202019_3amending%20PD2019%20and%20adjusting%20budget2019.pdf

36 Project funded by the EU to connect CSIRTS around the Member States.

ENISA produced a roadmap of possible activities on the basis of a broad survey. Specific stakeholders in this field were selected to further enhance the cooperation between the CSIRTs and law enforcement, along with their interaction with the judiciary.

ENISA also continued its efforts in support of the fight against cybercrime, an EU-wide objective, and liaised with various stakeholders at EU level (notably Europol/EC3), together with stakeholders selected at Member State level.

ENISA also prepared training material used in training sessions organised by the European Union Agency for Law Enforcement Training and in the hands-on training delivered in the eighth ENISA–EC3 workshop.

Additionally, a report on technical aspects of cooperation across these two operational communities was drafted to highlight gaps and make concrete recommendations to stakeholders in this field.

ENISA co-organised the annual workshop for national and governmental CSIRTs and their law enforcement agency counterparts with Europol/EC3.

O.4.2.3. Supporting the implementation and development of the MeliCERTes platform

Main achievements:

ENISA took over the central component of MeliCERTes, designed to be the primary cooperation platform between participating Member States' CSIRTs and to improve Member States' preparedness, cooperation and coordination in order to efficiently respond to emerging cyberthreats as well as to cross-border incidents.

ENISA actively supported the platform handover procedure from an operational perspective (i.e. managing the trust circles).

In particular, ENISA engaged in the cooperation with the Commission to ensure a smooth transfer of the knowledge and expertise regarding the trust circles management.

Additionally, ENISA implemented specific mandatory operational procedures for system administration.

4.2 Outputs and performance indicators for Activity 4: COMMUNITY

Summary of outputs in Activity 4: COMMUNITY – Foster the emerging European NIS community

Outputs	Performance indicator	Results achieved
Objective 4.1. Cyber-crisis cooperation		
Output O.4.1.1. Planning of Cyber Europe 2020 and Cyber SOPEx	Confirmation of support from at least 80 % of EU Member States / EFTA countries for Cyber Europe 2020. Confirmation of support from at least 25 CSIRT Network members for Cyber SOPEx 2019.	27 EU Member States and 2 EFTA countries participated in the planning of Cyber Europe 2020. 1 Cyber SOPEx was carried out, with the participation of the majority of the CSIRT Network.
Output O.4.1.2. Support activities for cyber exercises	Use by at least 4 CSIRTs from different Member States of the CEP in alignment with MeliCERTes for cyber exercise-related activities.	1 Cyber SOPEx was carried out, with the participation of the majority of the CSIRT Network. From the point of view of trust circles management, the MeliCERTes facility is available for use in cyber exercises.
Output O.4.1.3. Supporting the implementation of the cyber-crisis collaboration blueprint	At least 2 exercises on the cyber-crisis collaboration blueprint.	CSIRT Network SOPs updated after the Cyber SOPEx. Addressing the gaps identified in operational collaboration in the context of the blueprint, work on the development of EU institution SOPs has been initiated.
Output O.4.1.4. Supporting the implementation of the information hub	Provision of OpenCSAM tool to blueprint stakeholders in Cyber Europe 2020.	All necessary preparations have been made to make the OpenCSAM tool available to blueprint stakeholders as well as to Cyber Europe exercise players.

Summary of outputs in Activity 4: COMMUNITY – Foster the emerging European NIS community		
Outputs	**Performance indicator**	**Results achieved**
Output O.4.1.5. Supporting the implementation of the cyber-crisis collaboration blueprint – replaced by O.4.1.3 following amendment 13 to the 2019 work programme.		
Objective 4.2. CSIRT and other NIS community building		
Output O.4.2.1. EU CSIRT Network secretariat and support for EU CSIRT Network community building	Engagement of all 28 Member States' designated CSIRTs and CERT-EU in the activities described in the network's work programme (action plan midterm goals and objectives). Participation of 90 % of Member States' standing CSIRT representatives and CERT-EU in regular CSIRT Network meetings. Provision of support to CSIRT Network chair in preparation of the next evaluation report to the NIS CG. Provision of at least 1 conference call facility for the needs 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 communications channels readiness. Provision of active support to the facilitator of the exercise during its execution according to SOPs. Provision of assistance to at least 1 CSIRT Network member with the maturity assessment and peer review. First to fourth quarters. Facilitation of preparation of the next evaluation report for the NIS CG (P). First to fourth quarters. Provision of active support to CSIRT Network (e.g. communications support: maintaining and improving available means of communication in line with decisions in the CSIRT Network – e.g. outcome of working groups' efforts) (S). First to fourth quarters. Continuation of improvement of CSIRT Network Cooperation Portal functionalities and security (P). Trust-building exercise (held along with the regular CSIRT Network meeting) (E). Fourth quarter. Provision of further support for CSIRT Network-specific information exchange and secure communications issues (according to the CSIRT Network action plan) (P). Provision of active secretariat support and engagement during the CSIRT Network's 2019 Cyber SOPEx according to the network's SOPs (S). Provision of support for CSIRT maturity assessment and peer review of members of the CSIRT Network (S).	Continuous secretariat support provided to the CSIRT Network management trio – currently Croatia, Romania and Finland, with a Finnish chair. Additionally provided organisational and technical support to the daily operations of users, working groups and teams. 3 face-to-face meetings with 96 % attendance rate and constant participation from all Member States and CERT-EU. Supported the preparation of the second report to the NIS CG and ad hoc briefings of the NIS CG. Deployed CSIRT Network public website. Enabled 24/7 information exchange and document sharing via the dedicated tools. Organised 2 communications checks conducted according to a defined schedule, 1 in the first quarter before Cyber SOPEx 2019 and 1 in the fourth quarter. ENISA deployed 1 of its experts as a liaison to each working group to support the continuity of the group efforts. Penetration tests done regularly during the year for the Cooperation Portal. 1 trust building exercise focusing on how to cooperate during a virus outbreak, during the ninth CSIRT Network meeting. Publication of the study Secure Group Communications – For incident response and operational communities. Survey and mapping of measures on proactive detection of network security incidents available to the CSIRT Network members. Organisationally and technically supported the 2019 Cyber SOPEx, conducted by the CSIRT Network and designed to test the network's SOPs. ENISA performed 4 peer review assessments of CSIRTs in support of the CSIRT Network activities.

Summary of outputs in Activity 4: COMMUNITY – Foster the emerging European NIS community		
Outputs	**Performance indicator**	**Results achieved**
Output O.4.2.2. Support the fight against cybercrime and collaboration between CSIRTs and law enforcement	Participation of at least 5 Member States' CSIRT representatives, 5 Member States' law enforcement representatives, 2 Member States' judiciary representatives and EC3 in the preparation of the roadmap. Participation of at least 15 Member States in annual ENISA–EC3 workshop.	High level of participation from the Member States in collecting data for the roadmap, as shown below. **31 interviews, with:** 12 Member States' CSIRTs, 18 Member States' law enforcement agencies, 1 Member State's judiciary. **33 online survey replies, from:** 11 Member States' CSIRTs, 21 Member States' law enforcement agencies, 1 Member State's CSIRT and law enforcement agency. Training materials (handbooks and toolsets) on 4 thematic areas have been developed. 1 training session delivered to law enforcement community (about 50 participants) upon request from the European Union Agency for Law Enforcement Training. 1 training session delivered to CSIRT and law enforcement representatives (about 18 participants) focusing on the aspects of cooperation between CSIRTs and law enforcement during the eighth ENISA–EC3 workshop. An overview on enhancing technical cooperation between CSIRTs and law enforcement was produced; online survey results were used for this report. Approximately 50 representatives (about 15 Member States and 2 EFTA countries) from CSIRT and LE communities participated – by invitation only – in the eighth ENISA–EC3 workshop.
Output O.4.2.3. Supporting the implementation and development of the MeliCERTes platform	Cooperation with the Commission and the Consortium[37] for a smooth transfer of the knowledge and expertise regarding trust circles management and related services.	In 2019 ENISA took over the management of central trust circles on the MeliCERTes platform. In addition, ENISA provided support for CSIRT Network members with regard to MeliCERTes installations and usage.
Objective 4.3. Response to Article 14 requests under community activity and associated outputs are removed following amendment 16 to the 2019 work programme		

37 "The consortium is composed of three members of the CSIRTs Network, which have a proven track record of both building new tooling and maintaining software over the long-term, such as CERT.at, CERT.PL, CIRCL and CERT EE." Quoted from https://www.enisa.europa.eu/news/enisa-news/open-platform-and-tools-to-facilitate-the-collaboration-among-computer-security-incident-response-teams

5 ACTIVITY 5: ENABLING

Reinforce ENISA's impact

5.2.1 Objective 1: Management and compliance

a. Management

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

The Resources Department oversees a variety of programmes, projects and services regarding ENISA's management and horizontal services, assisting the executive director in areas such as human resources, finance and procurement, internal communications, ICT, facilities management, health and safety, physical security, legal services, protocol and liaison with local authorities.

The aim of the Resources Department is to ensure the operation of these services based on the legal and financial framework and to do so with the highest level of efficient and effective use of the financial and human resources available to ENISA.

The main internal stakeholders in ENISA are the staff, the executive director and the Management Board. Externally, the main stakeholders include, but are not limited to, the IAS of the European Commission, the ECA, the European Ombudsman, the European Anti-Fraud Office and Commission services such as DG Human Resources and Security, DG Budget, DG Communications Networks, Content and Technology, and more.

Significant attention is given to the internal policies related to transparency, fraud prevention, whistle-blower protection, avoidance of conflicts of interest, and so on.

Special attention is given to maintaining a modern and safe public administration, so as to protect the EU public and institutions. The focus is on a constant alignment with achieving the agency's strategy.

Internally and externally, objectives and monitoring strategies are set with the objective of implementing optimal solutions for delivering on ENISA's mandate and work programme, assuring the functioning of the required horizontal services both within adequate risk levels and in full compliance with the legal requirements.

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 Core Operations Department coordinates the delivery of ENISA's core activities. As such, its main role is to deliver on Activities 1–4 of the work programme. It also includes the Policy Office and the Public Affairs Team. The support for the ENISA Advisory Group and National Liaison Officers (NLO) Network is also carried out within the Core Operations Department.

b. Policy Office

ENISA initiated and further developed strategic cooperation with relevant stakeholders active in the cybersecurity community.

For instance, it engaged in policy and strategy discussions with political and policy decision-makers (by participating in or organising e.g. breakfasts with Members of the European Parliament).

In addition, ENISA engaged in strategic relationships to foster further development – for instance with specific industry sectors at the decision-making level (i.e. with industry groups) to identify cybersecurity issues of strategic importance.

ENISA further developed its cooperation with the EDA, CERT-EU and EC3 in the context of the existing memorandum of understanding with those bodies.

More details of the activities delivered by the Policy Office and the Public Affairs Team are given under 'Objective 2: Engagement with stakeholders and international activities' below.

The Policy Office also delivered ENISA's planning activities, including the preparation of the single programming document and coordination of the work programme.

Further to the publication of the CSA, the 2019 work programme was amended; the Policy Office coordinated the work involved.

c. Public Affairs Team

The Public Affairs Team is responsible for coordinating all activities with the media and press, including press releases, news items and interviews.

It also plays a major role in supporting events attended by ENISA, ensuring that ENISA is well represented from a public affairs perspective, that

appropriate publicity material is available and, where appropriate, that booths are arranged and supported.

d. Internal control

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

e. Information technology

ENISA made important decisions in 2019 to improve its security posture and resilience. The implementation of the projects below, initiated in 2019, could not be started until 2020. They are expected to be fully developed by 2021. This came in addition to the constant monitoring of the threat landscape and market evolution.

Some of the main projects/investments initiated in 2019 are as follows:

- a new data centre in the Heraklion office;
- a new data centre in the Athens office;
- a disaster recovery site, using a partnership with a decentralised EU agency in Alicante, Spain – the European Union Intellectual Property Office;
- a set of measures, as identified in a risk assessment, with the objective of increasing preparedness and resilience of the IT security and cybersecurity in ENISA's corporate systems.

In addition to the main projects indicated above, smaller projects were also initiated. These projects are part of the constant effort to improve internal operations, enhancing the security and availability of ENISA services to all ENISA stakeholders.

The corporate IT team also assumed the responsibility for taking over the MeliCERTes project from the Commission. Throughout the year, the team invested an extensive amount of work in the project, in coordination with the Commission and Consortium of suppliers[38].

As planned, in November 2019 the platform was handed over to ENISA and is now successfully running within ENISA's infrastructure.

In addition to running the system, the IT team is also responsible for being the help desk for all the CSIRTs using this facility.

The KPIs defined in the 2019 work programme were all achieved, as shown in the table below.

Task	Objective	Level of completion in 2019
Keep ENISA's systems safe from (external) cybersecurity incidents – prevent and react to threats	Security	100 %
Patching IT-managed servers by deadline (24 hours after being received from supplier)	Security	100 %
Ensure availability of server exchange	Efficiency	95 %
Ensure availability of internal applications	Availability of services	95 %
Help desk: successfully reply to all service requests	Efficiency	95 %

f. Finance and procurement

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

g. Legal Affairs, data protection and information security coordination

Legal Affairs

Legal Affairs continued to provide support for the legal matters associated with the operation of ENISA. This includes dealing with contracts, procurement, employment-related questions, data protection and corporate governance topics. The tasks of Legal Affairs also include dealing with complaints to the European Ombudsman and representing ENISA before the European Union Court of Justice, General Court or Civil Service Tribunal.

Data protection compliance tasks and data protection officer

The main tasks of the data protection officer[39] include the following:

38 "The consortium is composed of three members of the CSIRTs Network, which have a proven track record of both building new tooling and maintaining software over the long-term, such as CERT.at, CERT.PL, CIRCL and CERT EE." Quoted from https://www.enisa.europa.eu/news/enisa-news/open-platform-and-tools-to-facilitate-the-collaboration-among-computer-security-incident-response-teams

39 The tasks of the data protection officer are explicitly mandated in 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

- to inform and advise ENISA of its obligations as provided for in the applicable legal provisions for the protection of personal data and to document this activity and the responses received;
- to monitor the implementation and application of ENISA's policies in relation to the protection of personal data and the applicable legal framework for data protection;
- to monitor the implementation and application of the applicable legal framework for the protection of personal data at ENISA, including the requirements for data security and the provision of information to data subjects and their requests exercising their rights;
- to monitor the documentation, notification and communication of personal data in the context of ENISA's operations;
- to act as ENISA's contact point for the EDPS on issues related to the processing of personal data; to cooperate and consult with the EDPS whenever needed.

In 2019, the Management Board of ENISA adopted the rules for implementing the data protection officer function, pursuant to Article 45(3) of Regulation (EU) 2018/1725.

In addition, ENISA published its internal rules (adopted by a Management Board decision) concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of ENISA, pursuant to Article 25 of Regulation (EU) 2018/1725.

Information security coordination

On 16 July 2019 a full-time information security officer was appointed at ENISA. The information security officer coordinates the information security management system on behalf of the authorising officer.

In particular, the information security officer advises the IT team and all other areas of ENISA using IT systems to develop and implement information security policies, standards, guidelines and baselines that seek to secure the confidentiality, integrity and availability of ENISA's information systems.

The information security officer is instrumental in incident handling, incident response and security event monitoring. The information security officer also leads the security training of ENISA's staff and provides security guidance on all IT projects, including the evaluation and recommendation of technical controls.

In 2019, the information security officer contributed to goals such as the following.

- Developing assurance frameworks to demonstrate ongoing improvement of the information security management system. This includes developing KPIs.
- Monitoring and reporting the following to the IT advisory committee:
  - KPI results;
  - incidents identified and managed;
  - non-compliance with policy identified and addressed.
- Improving ENISA's security posture by planning penetration tests and vulnerability assessments.
- Advising on security policies and updating existing ones in line with the evolution of threats and risks.
- Improving the internal security training of ENISA staff.
- Implementing new systems and tools to support improvements in information security.

The main achievements pertaining to the year 2019 were the following.

- Improved network security, achieved by guiding a network segmentation project and applying security baselines to the networking equipment.
- Guiding the deployment of web application firewalls in front of the ENISA website and in front of the ENISA infrastructure.
- Security assessments of several of ENISA's online tools and systems.
- Regular vulnerability scans of the perimeter.
- Critical patching prioritisation.
- Security requirements for servers and endpoints.
- Continuous monitoring of the network for security incidents.

and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002.

5.2.2 Objective 2: Engagement with stakeholders and international activities

a. Stakeholder communication and dissemination of ENISA's deliverables[40].

In 2019, ENISA maintained its efforts to improve its focus on key activities and engage the highest possible number of stakeholders. This includes the different groups of stakeholders from institutions, academia, industry, the public, etc. In its engagement with the stakeholders, ENISA is guided by principles such as balanced representation, openness, transparency and inclusiveness.

Dissemination and outreach

ENISA further engaged in developing tools and using channels, including its website, for the dissemination of the ENISA's deliverables and for outreach, with a strong emphasis on social media.

ENISA's outreach goals for 2019 to 2021

Area	Metric	Increase from previous year		
		2019	2020	2021
Publication of media material by ENISA	Number of press communications published	30 %	30 %	30 %
Publication of social media items	Number of social media items published	50 %	40 %	40 %
Social media followers	Number of social media followers	30 %	25 %	25 %
Corporate events	Number of corporate events	10 %	40 %	10 %
Website traffic	Number of page views / visits / unique visitors / returning visitors	20 %	30 %	30 %

Internal communications

- In 2019, ENISA made the first step in setting up an internal communications strategy to enhance staff engagement and to exploit opportunities for pooling and sharing resources. With the internal communications tasks now being the responsibility of the Human Resources Unit, the objectives were set as follows:
- to enhance the accessibility of key human resources information for staff members and managers;
- to establish an internal communications strategy that is consistent and reflects the agency's strategic vision;
- to develop internal communications processes / tools / channels / guidance documents to support any organisational change;
- to ensure staff are engaged (e.g. by launching a regular staff survey, dedicated staff survey, etc.);
- to support changes in ENISA's corporate culture.

ENISA's internal communications objectives for 2019 to 2021.

Task	Objective	Level of completion		
		2019	2020	2021
Keep staff informed of ENISA activities (internal communications)	Hold 20 staff meetings per year	90 %	100 %	100 %
Team-building activities	Hold events with participation of all staff	2	2	2
Staff survey	Encourage participation of staff in the staff survey	65 %	70 %	75 %

ENISA Advisory Group

The ENISA Advisory Group was established by the new CSA. It replaces the Permanent Stakeholder Group.

This group, composed mainly of industry, academia and consumer organisation experts, continues to advise ENISA on its performance of its tasks, except with regard to the provisions of Title III ('Certification').

In 2019, two meetings took place, as planned: one meeting of the former Permanent Stakeholder Group and one of the new ENISA Advisory Group.

National Liaison Officers Network

The NLO Network was set up in 2004 as a series of informal points of communication in the Member States.

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

In January 2019, the NLO Network, in its informal capacity, met once – to set up an action plan for 2019.

As of 27 June 2019, the NLO Network is a statutory body of ENISA. It is a point of contact at national level to facilitate cooperation between ENISA and national experts in the context of the implementation of ENISA's annual work programme.

Nominations to the NLO Network were received from Member States in the course of 2019. This led to the adoption of Decision No MB/2020/04 of the Management Board of ENISA, officially establishing the NLO Network.

b. International relations

Under the executive director's guidance and initiative and in line with the approach agreed by the Management Board, ENISA strengthened contacts at an international level in line with the relevant provisions of the new CSA.

LIST OF THE 2019 DELIVERABLES:

All deliverables can be found on the following page of ENISA's website:

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

Activity 1: EXPERTISE – Anticipate and support Europe in facing emerging NIS challenges
Objective 1.1. Improving expertise related to NIS
Output O.1.1.1. Good practices for the security of the IoT *Good Practices for Security of IoT – Secure software development lifecycle* Status: Published *Industry 4.0 Cybersecurity – Challenges and recommendations* Status: Published
Output O.1.1.2. Good practices for the security of smart cars *ENISA Good Practices for Security of Smart Cars* Status: Published
Output O.1.1.3. Awareness raising of existing technical specifications for cryptographic algorithms 'Encrypted Traffic Analysis – Use cases and security challenges' Status: Published
Output O.1.1.4. Good practices for the security of healthcare services Procurement Guidelines for Cybersecurity in Hospitals – Good practices for the security of healthcare services Status: Published
Output O.1.1.5. Good practices for maritime security (port security) *Port Cybersecurity – Good practices for cybersecurity in the maritime sector* Status: Published
Objective 1.2. NIS threat landscape and analysis
Output O.1.2.1. Annual ETL ENISA Threat Landscape for 5G Networks – Threat assessment for the fifth generation of mobile telecommunications networks (5G) Status: Published
Output O.1.2.2. Restricted and public info notes on NIS
Output O.1.2.3. Support for incident-reporting activities in the EU *7 Steps to Shore up BGP* Status: Published *Annual Report Telecom Security Incidents 2018* Status: Published *Trust Services Security Incidents 2018 – Annual report* Status: Published
Output O.1.2.4. Regular technical reports on the state of cybersecurity *State of Vulnerabilities 2018/2019 – Analysis of events in the life of vulnerabilities* Status: Published

Objective 1.3. Research, development and innovation
Output O.1.3.1. Supporting cybersecurity public–private partnership in establishing priorities for EU research and development
Activity 2: POLICY – Promote NIS as an EU policy priority
Objective 2.1. Supporting EU policy development
Output O.2.1.1. Support the preparatory policy discussions in the area of certification of products and services 'ENISA IT System for Certification – An action plan to implement the EU certification framework' Status: Published *Advancing Software Security in the EU – The role of the EU cybersecurity certification framework* Status: Published *Transitioning existing certification schemes to the emerging EU certification framework – The case of SOG-IS MRA* Status: Published
Objective 2.2. Supporting EU policy implementation
Output O.2.2.1. Recommendations for technical implementation of the eIDAS regulation 'Overview of Standards – Specifying formats of advanced electronic signatures and seals' Status: Published *Assessment of ETSI TS 119 403-3 – Eligibility of ETSI TS 119 403-3 for referencing in an eIDAS implementing act* Status: Published *eIDAS Compliant eID Solutions – Security considerations and the role of ENISA* Status: Published *Recommendations for Technical Implementation of the eIDAS Regulation – Towards a harmonised conformity assessment scheme for QTSP/QTS* Status: Published
Output O.2.2.2. Supporting the implementation of the work programme of the NIS CG
Output O.2.2.3. Assist Member States in the implementation of OES and DSP security requirements *Stock taking of security requirements set by different legal frameworks on OES and DSPs – The NISD and the GDPR* Status: Published
Output O.2.2.4. Supporting the implementation of the payment services directive *Power Sector Dependency on Time Service – Attacks against time sensitive services* Status: Published
Output O.2.2.5. Contribute to EU policy in the area of privacy and data protection with policy input on security measures *Online Platform for Security of Personal Data Processing – Reinforcing trust and security in the area of electronic communications and online services* Status: Published *Pseudonymisation Techniques and Best Practices – Recommendations on shaping technology according to data protection and privacy provisions* Status: Published
Output O.2.2.6. Guidelines for European standardisation in ICT security *Standardisation in Support of the Cybersecurity Certification – Recommendations for European standardisation in relation to the Cybersecurity Act* Status: Published Standards Supporting Certification – Analysis of standards in areas relevant to the potential EU candidate cybersecurity certification schemes Status: Published
Output O.2.2.7. Supporting the implementation of the EECC *Security Supervision under the EECC* Status: Published
O.2.2.8. Supporting the sectorial implementation of the NISD
O.2.2.9. Hands-on tasks in the area of certification of products and services
Activity 3: CAPACITY – Support Europe in maintaining state-of-the-art NIS capacities
Objective 3.1. Assisting Member States in capacity building
Output O.3.1.1. Update and provide technical training for Member States and EU bodies *EU MS Incident Response Development Status Report* Status: Published

Output O.3.1.2. Support EU Member States in the development and assessment of NCSSs *Good Practices in Innovation under NCSS – Good practices in innovation on cybersecurity under the national cyber security strategies* Status: Published
Output O.3.1.3. Support EU Member States in their incident-response development *EU MS Incident Response Development Status Report* Status: Published
Output O.3.1.4. Support EU Member States in the development of ISACs for the NISD sectors
Objective 3.2. Supporting EU institutions in capacity building
Output O.3.2.1. Representation of ENISA on the CERT-EU Steering Board and coordination with other EU agencies using CERT-EU services
Output O.3.2.2. Cooperation with relevant EU bodies on initiatives covering the NIS dimension of their missions
Objective 3.3. Assisting in improving private sector capacity building and general awareness
Output O.3.3.1. Cybersecurity challenges 'ECSC 2019 Analysis Report – Maturity assessment and lesson learnt of the European Cyber Security Challenges 2019' Status: Published
Output O.3.3.2. Holding the ECSM 2019 *ECSM Deployment Report – Deployment report* Status: Published
Output O.3.3.3. Support EU Member States in developing cybersecurity skills *Cybersecurity Skills Development in the EU – The certification of cybersecurity degrees and ENISA's Higher Education Database* Status: Published
Activity 4: COMMUNITY – Foster the emerging European NIS community
Objective 4.1. Cyber-crisis cooperation
Output O.4.1.1. Planning of Cyber Europe 2020 and Cyber SOPEx
Output O.4.1.2. Support activities for cyber exercises
Output O.4.1.3. Support activities for cyber-crisis management *Artificial Intelligence – An opportunity for the EU cyber crisis blueprint – Conference report* Status: Published *EU ELEx19 – After action report* Status: Published
Output O.4.1.4. Supporting the implementation of the information hub
Output O.4.1.5. Supporting the implementation of the cyber-crisis collaboration blueprint
Objective 4.2. CSIRT and other NIS community building
Output O.4.2.1. EU CSIRT Network secretariat and support for EU CSIRT Network community building (Scenario 1) Proactive detection – Measures and information sources Status: Published Proactive detection – Good practices gap analysis recommendations Status: Published Proactive detection – Survey results Status: Published
Output O.4.2.2. Support the fight against cybercrime and collaboration between CSIRTs and law enforcement *Roadmap on the Cooperation between CSIRTs and LE* Status: Published *An Overview on Enhancing Technical Cooperation between CSIRTs and LE* Status: Published Online training material – Legal & cooperation Status: Published
Output O.4.2.3. Supporting the implementation and development of the MeliCERTes platform

PART II
MANAGEMENT

1 MANAGEMENT BOARD

In 2019, the Management Board (see Annex 11 – 'List of Management Board members in 2019') met for one ordinary meeting and three extraordinary meetings. The extraordinary meetings took place due to the need to process the selection and appointment of the executive director and the elections of the chair and deputy chair of the Management Board.

In total, the Management Board made 17 decisions during the year, the appointment of ENISA's new executive director being one of the most substantial.

In addition, the 2019–2021 programming document, the 2019 statement of estimates and the 2019 establishment plan were amended pursuant to the entry into force of the CSA.

As part of its functions, the Management Board adopted its analysis and assessment of the 2018 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 2018 and adopted the *ENISA Programming Document 2020–2022*, including the 2020 budget and the 2020 establishment plan.

Sharing information with the Management Board on a regular basis, 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 was informed of any potential risks or matters impacting quality control. The board members remained committed to declaring their interests in order to avoid any conflicts of interest at meetings.

In addition, the Management Board, in agreement with the Commission, continued to engage in the adoption of the necessary implementing measures in accordance with the arrangements provided for in Article 110 of the Staff Regulations.

In 2019, the Management Board took note of the observation on internal controls in the ECA preliminary observations.

The Management Board decisions were prepared by the Executive Board and adopted by the Management Board (Annex 11 – 'List of Management Board decisions adopted in 2019').

The Executive Board had one formal meeting per quarter.

2 MAJOR DEVELOPMENTS

The most important development concerning ENISA was the entry into force on 27 June 2019 of the CSA, conferring a new mandate, with enhanced competences and resources, on the agency.

The new tasks pertain to the areas of cybersecurity certification, providing for the improved coordination of crisis management and for extended responsibilities under the NISD.

These changes presented challenges in relation to budgetary consumption, and led to organisational changes to integrate the new tasks. This necessarily impacted recruitment. The financial resources allocated to ENISA increased by 41 % from 2019 to 2020 (see **table below**).

The establishment plan projected a staff increase of 27 % over the same period (from 98 staff members in 2019 to 124 in 2022).

ENISA's budget overview from 2019 to 2022

Budget amounts per year (in million EUR)				
Area of budget allocation	**2019**	**2020**	**2021**	**2022**
ENISA total	16.3	20.6	22.2	23.0
Breakdown				
Title I. Staff expenditure	9.3	12.1	13.3	13.9
Title II. Infrastructure and operating expenditure	2.1	2.2	2.4	2.6
Title III. Operational expenditure	4.9	6.3	6.4	6.5

ENISA's Management Board appointed a new executive director, Mr Juhan Lepassaar, who took up his duties on 16 October 2019.

3 BUDGETARY AND FINANCIAL MANAGEMENT

a. Financial management

During 2019, the agency operated with a budget of EUR 11.6 million until 31 May 2019 and with a total budget of EUR 16.9 million. The amended 2019 budget was adopted by the Management Board by written procedure on 31 May 2019, and allowed the agency to make use of the new appropriations.

The table below shows ENISA's budget implementation targets and achievements in 2019.

Area	Objective	Target 2019	Level of completion 2019
Budget implementation (appropriations committed through the year)	Efficiency and sound financial management	99 %	97 %
Payments against appropriations of the year (C1 funds)	Efficiency and sound financial management	85 %	70 %
Payments against appropriations carried over from previous year (C8 funds)	Efficiency and sound financial management	93 %	95 %

b. Budget execution of EU subsidy (C1 funds of current year 2019N)

During 2019, ENISA committed an amount of EUR 15 771 526, representing 97 % of the total budget for the year. Payments made during the year amounted to EUR 11 424 194, representing 70 % of the total budget.

Budgetary execution remained high. Compared to 2018, there was a slight decrease in commitment execution (97 % in 2019 compared to 99 % in 2018) as well as a decrease in payment execution (70 % in 2019 compared to 89 % in 2018).

The target commitment rate set by the Commission (DG Budget) for the year (95 %) was reached, despite the adoption of a significant budgetary increase on 31 May 2019.

The commitment appropriations corresponding to the EU subsidy (C1 appropriations) that were not paid at the end of 2019 were carried forward to 2020.

The table below summarises the execution of the budget in 2019.

2019 budget (C1)						
2019 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 2020 (in EUR)**
Title I	7 636 363	7 458 310	97.67 %	7 100 374	92.98 %	357 936
Title II (*)	4 095 835	3 910 898	95.48 %	1 026 856	25.07 %	2 884 042
Title III	4 560 754	4 402 318	96.53 %	3 296 964	72.29 %	1 105 354
TOTAL	**16 292 952**	**15 771 526**	**96.80 %**	**11 424 194**	**70.12 %**	**4 347 332**

(*) Title II does not include the 2019 subsidy of EUR 435 844 received from the Hellenic authorities for the rent of the building (as stipulated in the host country agreement).

Further details on budget execution are provided in Annex 2.

c. Amending budget / budgetary transfers

According to the 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.

At the beginning of 2019 ENISA had an original budget of EUR 11 million. With the adoption of the CSA, conferring a revised mandate with greater competences and resources on the agency, its budget increased to EUR 16.3 million. The Management Board amended the budget accordingly by written procedure on 31 May 2019. The agency integrated and started using the full appropriations provided for 2019 after the decision was made.

During 2019, the executive director made four transfers within the initial budget and six transfers within the amended budget. An additional transfer between titles was approved by the Management Board on 21 November 2019, transferring EUR 1.6 million from Title I to Title II. This transfer was the result of savings under Title I, 'Staff expenditure', mainly due to the late entry into force of the CSA. This delayed the recruitment planning. In order to meet all the requirements of ENISA's new mandate, a revision and update of the agency's IT infrastructure was also needed.

The table below summarises the changes to the budget in 2019.

2019 budget (C1) (in EUR)				
2019 area of budget allocation	**Initial budget**	**Amended budget**	**Transfers approved by the Management Board and the executive director**	**Final budget**
Title I	7 133 783	9 387 948	– 1 751 585	7 636 363
Title II (*)	964 101	2 037 000	2 058 835	4 095 835
Title III	2 901 000	4 868 004	– 307 250	4 560 754
TOTAL	**10 998 884**	**16 292 952**	**0**	**16 292 952**

(*) Title II does not include the 2019 subsidy of EUR 435 844 received from the Hellenic authorities to cover ENISA's office rental costs as established in the host country agreement.

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 2018 were carried forward to 2019 (C8 appropriations).

Compared to 2018, there was an increase of 1 percentage point in the commitment execution (94.93 % in 2019 compared to 93.98 % in 2018) and of 2.6 percentage points in payment execution (94.93 % in 2019 compared to 92.33 % in 2018), showing an improvement in finance management in this regard.

The following table shows the commitment execution and payment execution in 2019.

2019 budget (C8)				
2019 area of budget allocation	**Appropriations carried forward from 2018 to 2019 (in EUR)**	**Payment amount (in EUR)**	**Percentage paid**	**Amount cancelled (in EUR)**
Title I	527 606	505 549	95.82 %	22 057
Title II	323 628	323 122	99.84 %	505
Title III	381 029	341 071	89.51 %	39 958
TOTAL	**1 232 263**	**1 169 742**	**94.93 %**	**62 521**

4 DELEGATION AND SUBDELEGATION

The executive director has delegated the power for budget implementation of a maximum of EUR 500 000 for an unlimited period to the head of the Resources Department for Titles I and II and to the head of the Core Operations Department for Title III. Further financial delegations of a maximum of EUR 100 000 have been granted to heads of unit to implement the budget for an unlimited period for budget items relevant to their assigned tasks.

No further subdelegations have been implemented at ENISA.

Controls on these delegation rights are mainly done through a periodical revision of the rights granted in the main financial system, 'ABAC[41]'.

5 HUMAN RESOURCES MANAGEMENT

The Human Resources Unit supports 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-

41 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

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 2019, ENISA carried out tasks in support of the deployment of the Commission's information management system for human resources ('Sysper').

Compliance remained a priority for the Human Resources Unit both in terms of meeting audit and internal control recommendations and in terms of meeting statutory requirements such as in the area of personal data protection.

In 2019, ENISA increased its efforts to recruit staff to fill all posts according to the establishment plan pursuant to the CSA and to lay the groundwork for recruitment in 2020.

The table below shows ENISA's planned recruitment goals for 2019 to 2021.

Area	Objective	2019 target	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	≤ 5 months
Turnover of staff	Reduced turnover rate of statutory staff (temporary agents and contract agents)	< 15 %	< 15 %	< 15 %
Staff performance management	Implementation and monitoring of the appraisal and reclassification exercises (launching and completion of the exercises)	100 %	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) 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.

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 *EX POST* EVALUATION RESULTS DURING THE REPORTING YEAR

Ex post audit control and exceptions

In 2019, ENISA performed *ex post* controls, as part of the internal control framework, for the 2018 financial year. A total of 180 financial transactions were scrutinised, representing 10.67 % of all of the agency's financial transactions and 67.72 % of the agency's 2018 budget. As a result, recommendations were issued as follows.

Four 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.

In 2019 the agency recorded 38 exceptions: 33 of these were below the relevant materiality level (less than EUR 15 000) and of a minor administrative nature with no financial impact. The remaining five exceptions were linked to a posteriori commitments. 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 2020 carry-forward will be improved.

The ECA is in charge of the annual audit of the agency. It compiles its conclusions in the publication of an annual report in accordance with the provisions of Article 287(1) of the Treaty on the Functioning of the European Union.

For several consecutive years, the ECA's reports have confirmed improvement in the agency's overall internal control environment and performance.

8 ASSESSMENT OF AUDIT AND FOLLOW-UP OF RECOMMENDATIONS AND ACTION PLANS FROM AUDITS

This section discloses and assesses the observations, opinions and conclusions published by auditors in their reports, along with the limited conclusion of the internal auditor on the state of internal control, that may have a material impact on the achievement of the internal control objectives, and therefore on assurance, together with any management measures taken in response to the audit recommendations.

Internal Audit Service

The IAS audit report on human resources management and ethics was issued in September 2019. Four important and three very important recommendations were issued in this audit. An action plan was devised and agreed with the IAS. All issues should be addressed by the end of 2020.

The IAS audit report on stakeholder involvement in deliverables was issued in June 2018. Five recommendations[42] 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 the end of 2019, four recommendations were considered closed by the IAS. One important recommendation[43] was still pending as relevant procedures needed to be revised and approved internally.

European Court of Auditors

Issued in 2019, the ECA report on the 2018 annual accounts did not contain any critical audit findings.

The agency continued to engage in the improvement of its internal systems and remained vigilant for potential risks in its activities within the internal legal and financial framework, in order to strive for the level of non-compliance issues recommended by the IAS and the ECA.

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

One recommendation issued by the European Anti-Fraud Office relating to a recovery order of EUR 5 600 to a supplier has been actively pursued by ENISA and is expected to be positively resolved by end of 2020.

10 FOLLOW-UP OF OBSERVATIONS FROM THE DISCHARGE AUTHORITY

In relation to the 2018 discharge as decided by the European Parliament, the executive director of the agency was granted discharge in respect of the implementation of the agency's budget for the 2018 financial year. The closure of the agency's accounts for the 2018 financial year was also approved.

11 ENVIRONMENTAL MANAGEMENT

While ENISA has not yet adopted a formal environmental management policy, the agency still implemented greening measures in 2019 such as: recycling of office materials, reduction in electricity usage for lighting and heating/cooling, the use of video conferencing equipment instead of face-to-face meetings involving travel, use of teleworking, provision of bicycle racks to promote the use of public transport and implementing green public procurement.

All the measures were taken within the scope of the agency's activities and to the greatest extent allowed by its infrastructure and location.

ENISA presently occupies part of a leased building in Athens. This does not allow the agency to control the heating/cooling system or to access autonomous electricity meters. The agency is therefore unable to directly monitor those systems and assess the impact of the greening measures implemented.

Therefore, ENISA could not seek to obtain the eco-management and audit scheme certification for its main office building given the leasing restrictions. However, achieving this certification will be envisaged for the new premises to be provided by the Hellenic authorities.

42 Three of these five recommendations have been assessed as important while the remaining two were deemed very important.

43 This recommendation was downgraded from very important to important in 2019 as most of the underlying issues had been addressed during the year.

12 COMPLIANCE REGARDING TRANSPARENCY, ACCOUNTABILITY AND INTEGRITY

The agency is committed to maintaining its vigilance and to ensuring openness and transparency. ENISA publishes a wide range of documents and other relevant information on its website (https://www.enisa.europa.eu) to show how the agency is managed and held accountable. This is done with the objective of helping the EU public and any other stakeholder understand how the agency is managed and being held accountable.

As provided for by the ENISA regulation (Regulation (EU) No 2019/881), the Management Board is the governing body of the agency. It is composed of representatives of the EU Member States and the Commission. Its main role is to ensure that the agency carries out its tasks in accordance with its operational and strategic objectives, as adopted through the agency's annual and multiannual work programme. It also supervises all budgetary and administrative matters.

To ensure the transparency of the decisions adopted, the following documents are published on ENISA's website: the internal rules of procedure for the Management Board, the list of its representatives and alternates, the minutes of meetings and the decisions adopted (including annual and multiannual work programmes).

The Management Board has the responsibility of appointing the executive director, who is responsible for implementing the decisions adopted by the Management Board and for the day-to-day administration of the agency.

To ensure the transparency and accountability of the executive function, one of the duties of the executive director is to provide an annual activity report; this report is given to the Management Board for analysis and assessment.

Once approved, and no later than 30 June of the year following the year under review, the annual activity report is formally adopted and communicated to the relevant stakeholders (namely the European Parliament, the European Council, the Commission and the ECA). The report outlines the achievements of the year and the resources used. Once approved, it is made publicly available through ENISA's website. Both the annual accounts (including the budgetary execution report) and the annual adopted budget are published on the website.

The executive director, representing the agency, is accountable to the European Parliament for the execution of the annual budget. The executive director must provide the Parliament with all the information necessary for the discharge procedure. The discharge procedure is a tool whereby the Members of the European Parliament check how public funds were spent and for what purpose. The Parliament can then decide to grant, postpone or refuse a discharge for the specific year.

To help the Parliament in the discharge procedure, independent reviews of the agency are carried out. On an annual basis, the ECA provides assurance of the reliability of the annual financial statements and of the legality and regularity of the transactions conducted by the agency for the year under review. The IAS conducts periodic audits on specific topics, selected based on a risk assessment. The results and follow-up of these audits must be included in the annual activity report (see previous sections). Complementing the external and internal audits, independent evaluations are carried out to assess the performance and long-term impact of the agency's operations.

The agency is committed to maintaining its vigilance and to ensuring openness and transparency. ENISA publishes a wide range of documents and other relevant information on its website to show how the agency is managed and held accountable.

To avoid situations that might impair its independence or impartiality, the agency has implemented a comprehensive set of rules on preventing and managing conflicts of interest. Accordingly, ENISA's Management Board, Advisory Group, executive director and officials seconded

from Member States on a temporary basis need to make a declaration of commitments and a declaration of any interests that might be considered to be prejudicial to their independence. These declarations are made in writing.

ENISA adopted an anti-fraud strategy and action plan in 2014. It achieved significant results in terms of awareness raising by preparing and delivering internal training on fraud prevention to its entire staff. Training is delivered periodically to ensure that all staff are regularly informed about fraud prevention. As from 2018, fraud awareness training sessions are included in the agency's yearly training plan, together with the training on ethics and integrity that is compulsory for all staff. The anti-fraud strategy is expected to be updated and adopted in 2020.

In addition to the staff regulations, the agency has to adhere to the Commission code of conduct for all staff. The code offers comprehensive information and advice on a variety of issues, ranging from ethics to compliance with legal obligations.

In addition to the staff regulations, the agency has to adhere to the Commission code of conduct for all staff. The code offers comprehensive information and advice on a variety of issues, ranging from ethics to compliance with legal obligations. The objective of the code is to ensure that all employees share the values of ENISA as an open, accessible and transparent organisation. Furthermore, in accordance with the code of good administrative conduct issued by the European Ombudsman, ENISA intends to commit to a 2-week deadline for answering requests from members of the public.

13 ASSESSMENT BY MANAGEMENT

Generally performance was very good and in line with expectations, especially given the fact that the agency delivered on its annual work programme while simultaneously managing the transition to the new legal framework.

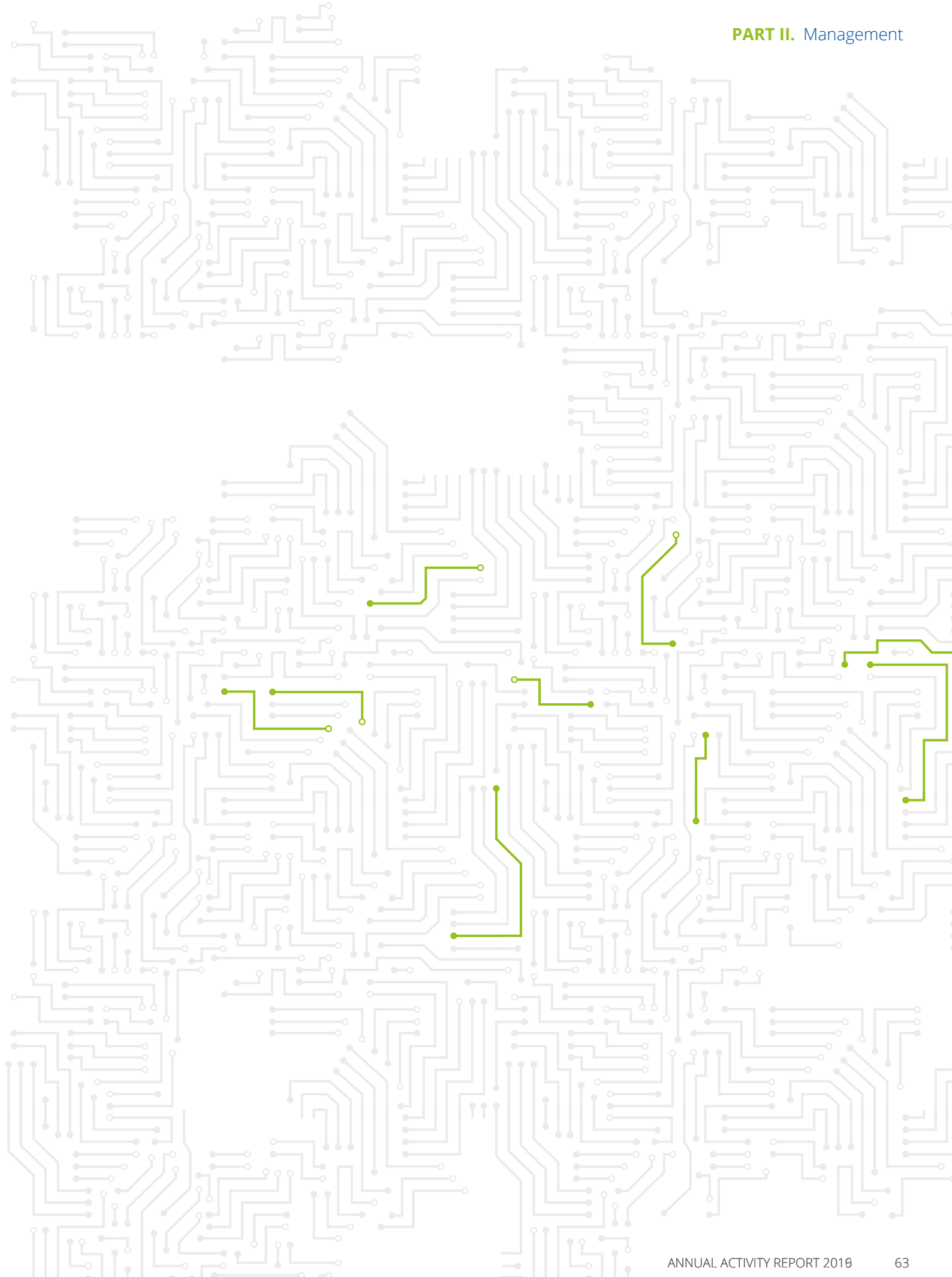
In this respect, a proactive approach to preparing for the new tasks, notably in the area of cybersecurity certification, proved to be well worth the effort. The work on certification is now proceeding smoothly, with clear goals for 2020 and a team that is up to speed.

Work in other key areas, such as implementation of the NISD and the eIDAS regulation, continue to develop well. Indeed, in the implementation of the NISD, ENISA's role is clearly growing, in terms of support for both the NIS CG and the CSIRT Network.

The fact that the agency was not able to commit the budget associated with the CSA until the act had come into force was a major challenge as the budget allocation effectively covered the full year.

Other significant challenges included the Commission's 5G action plan and the cybersecurity exercise that the agency organised in order to support the European Parliament elections. Both these tasks required significant changes to planning and both were done at extremely short notice.

Last but not least, the transition to the new director was very smooth, allowing all annual activities to finish on time.



PART III

ASSESSMENT OF THE EFFECTIVENESS OF THE INTERNAL CONTROL SYSTEMS

a. Effectiveness of internal control systems

ENISA set up the internal control framework at the end of 2019.

ENISA has adopted an internal control framework, based on the Committee of Sponsoring Organizations of the Treadway Commission's framework and on international best practices, following the Commission's revision in 2017. The financial regulation requires the organisational structure and the internal control systems used for the implementation of the budget to be set up in accordance with these principles (Article 36). ENISA has assessed the internal control systems during the reporting year and has concluded that the internal control principles are implemented correctly for its purposes and in adequate proportion to the identified risks.

The current instruments used are the following:

- 100 % verification of financial transactions (ex ante controls);
- internal electronic workflows, assurance of segregation of duties and several layers of review and checks;
- a register of exceptions;
- ex post control report and follow-up measures;
- independent audit from the ECA;
- independent audit from the IAS (performed by the European Commission).

These instruments provide adequate and sufficient assurance as to the completeness and reliability of the information reported.

ENISA adopted the revised internal control framework at the end of 2019. The revised framework follows that of the Committee of Sponsoring Organizations of the Treadway Commission as adopted by the European Commission, and consists of five internal control components and 17 internal control principles.

The effective internal control system of processes and procedures ensures the appropriate management of the risks in relation to the legality and regularity of the underlying transactions, and the nature of payments.

The internal control system designed provides 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.

The established internal control system is based on segregation of duties, the risk management and control strategy, avoidance of conflicts of interest, appropriate audit trails and data integrity in data systems, and established procedures for monitoring

performance and for follow-up of identified internal control weaknesses and threats.

Financial management and control is rooted in such core processes as procurement (from the assessment of needs to the selection of suppliers to the award decision), financial operations (all processes establishing the financial commitment to payment, contract monitoring and recoveries with ad hoc procedures in place are 100 % verified through *ex ante* verification) and supervisory measures (including *ex post* controls and audits), which form the basis for achieving sound financial management.

Legality and regularity is audited independently by the ECA.

b. Conclusions of assessment of internal control systems

In conclusion, management has reasonable assurance that the objective to constantly enhance the assurance of reliability of performance, legality and regularity based on the legal and financial framework was realised and working as intended in 2019. Internal risks were identified and appropriately monitored, and mitigation measures were implemented.

c. 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 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.

Place ..... date .....

(signature) [Paulo Alexandre Neves Empadinhas]

IV

PART IV
MANAGEMENT ASSURANCE

a. 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 transaction, 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.

b. Overall conclusion on assurance

Considering the results of the 2019 annual audits performed by the ECA and the IAS, the 2019 results of the internal controls (*ex post* controls and review of the register of exceptions) and the 2019 results of the key financial and operational indicators, the authorising officer can conclude that ENISA operated in 2019 in such a way as to appropriately manage the risks.

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

V

PART V
DECLARATION OF ASSURANCE

I, the undersigned,

Juhan LEPASSAAR,

Executive Director of the European Union Agency for Cybersecurity,

in my capacity as authorising officer,

declare that the information contained in this report gives a true and fair ([44]) 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, 30 June 2019

[signed]

Juhan LEPASSAAR
Executive Director

44 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	2017	2018	2019
Revenue actually received (+) (*)	11 223 387	11 572 995	16 740 086
Payments made (–)	– 9 901 545	– 10 345 736	– 11 980 352
Carry-over of appropriations (–)	– 1 376 730	– 1 348 657	– 4 357 734
Cancellation of appropriations carried over (+)	90 916	108 302	62 522
Adjustment for carry-over of assigned revenue appropriations carried over (+)	49 519	124 290	116 393
Exchange rate difference (+ / –)	– 12	– 689	– 1 802
Total	**85 535**	**110 505**	**579 113**

(*) Includes the contribution of EUR 435 844 received from the Hellenic authorities to cover office leasing expenditure and other administrative revenues for EUR 11 290 (such as reimbursement of travelling expenditure for staff invited as guest speakers to events).

Execution of commitment appropriations in 2019

	Chapter	Commitment appropriations authorised (*) (in EUR)	Commitments made in EUR	Commitment rate
A-11	Staff in active employment	5 627 276	5 627 276	100.0%
A-12	Recruitment expenditure	299 119	254 762	85.2%
A-13	Socio-medical services and training	255 655	222 200	86.9%
A-14	Temporary assistance	1 553 475	1 453 234	93.5%
	Title I	7 735 524	7 557 471	93.5%
A-20	Buildings and associated costs	806 546	801 693	99.4%
A-21	Movable property and associated costs	45 905	45 391	98.9%
A-22	Current administrative expenditure	83 068	81 829	98.5%
A-23	ICT	3 623 918	3 436 156	94.8%
	Title II	4 559 436	4 365 069	94.8%
B-30	Meetings and missions	979 875	913 755	93.3%
B-32	Horizontal operational activities	588 775	524 689	89.1%
B-36	Core operational activities	2 996 003	2 966 700	99.0%
	Title III	4 564 653	4 405 144	99.0%
	Total	**16 859 614**	**16 327 684**	**96.84 %**

(*) 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 2019

	Chapter	Payment appropriations authorised (*) (in EUR)	Payments made (in EUR)	Payment rate
A-11	Staff in active employment	5 627 276	5 627 276	100.0%
A-12	Recruitment expenditure	299 119	174 763	58.4%
A-13	Socio-medical services and training	255 655	137 484	53.8%
A-14	Temporary assistance	1 553 475	1 260 013	81.1%
	Title I	7 735 524	7 199 536	93.1%
A-20	Buildings and associated costs	806 546	715 007	88.7%
A-21	Movable property and associated costs	45 905	31 951	69.6%
A-22	Current administrative expenditure	83 068	52 177	62.8%
A-23	ICT	3 623 918	681 892	18.8%
	Title II	4 559 436	1 481 027	32.5%
B-30	Meetings and missions	979 875	822 508	83.9%
B-32	Horizontal operational activities	588 775	255 366	43.4%
B-36	Core operational activities	2 996 003	2 221 915	74.2%
	Title III	4 564 653	3 299 789	72.3%
	Total	**16 859 614**	**11 980 352**	**71.06 %**

(*) 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).

Breakdown of commitments (with open amounts as of 31 December 2019)

	Chapter	Commitments made (in EUR)	Payments made (in EUR)	Amount to be paid in 2020 (in EUR)	Percentage of amount to be paid
A-11	Staff in active employment	5 627 276	5 627 276	0	0.0%
A-12	Recruitment expenditure	254 762	174 763	79 999	31.4%
A-13	Socio-medical services and training	222 200	137 484	84 716	38.1%
A-14	Temporary assistance	1 453 234	1 260 013	193 221	13.3%
	Title I	7 557 471	7 199 536	357 936	4.7%
A-20	Buildings and associated costs	801 693	715 007	86 686	10.8%
A-21	Movable property and associated costs	45 391	31 951	13 440	29.6%
A-22	Current administrative expenditure	81 829	52 177	29 652	36.2%
A-23	ICT	3 436 156	681 892	2 754 264	80.2%
	Title II	4 365 069	1 481 027	2 884 042	66.1%
B-30	Meetings and missions	913 755	822 508	91 247	10.0%
B-32	Horizontal operational activities	524 689	255 366	269 323	51.3%
B-36	Core operational activities	2 966 700	2 221 915	744 784	25.1%
	Title III	4 405 144	3 299 789	1 105 354	25.1%
	Total	**16 327 684**	**11 980 352**	**4 347 332**	**26.6%**

(*) 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).

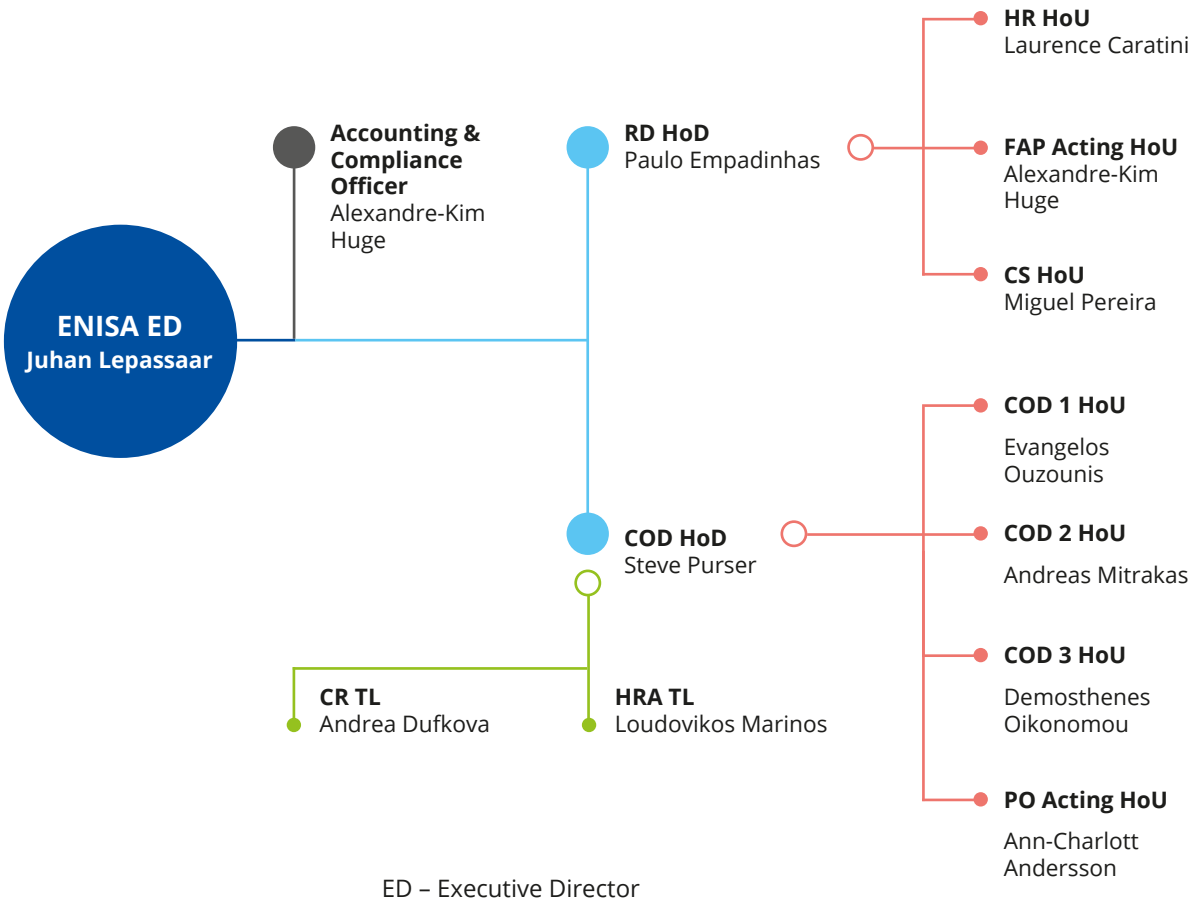
Revenue and income during 2019 (in EUR)

Type of revenue	Entitlements established	Revenue received	Amount outstanding at the end of the year
Subsidy from the EU budget	16 292 952	16 292 952	0
Subsidy from Hellenic authorities	435 844	435 844	0
Revenue from administrative operations	115 691	11 290	104 400
Total	**16 844 487**	**16 740 086**	**104 400**

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 December 2019).



- Executive Director
- Head of Department
- Head of Unit
- Team Leader

ED – Executive Director
RD – Resource department
HR – Human Resources
FAP – Finance and Procurement
CS – Corporate Services
EDO – Executive Director Office
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

ANNEX 4

2019 ESTABLISHMENT PLAN AND ADDITIONAL INFORMATION ON HUMAN RESOURCES MANAGEMENT

2019 establishment plan

Function group (FG) (administrator (AD) / assistant (AST) / assistant-secretary (AST/SC)) and grade	Establishment plan in 2019 voted EU budget		Positions filled as of 31.12.2019[45]	
	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		4
AD 8		19		10
AD 7				6
AD 6				6
AD 5				1
Total number of ADs		43		37
AST 11				
AST 10				
AST 9				
AST 8				
AST 7		3		2
AST 6		7		2
AST 5		5		4
AST 4		1		4
AST 3				1

45 51 temporary agents (47 temporary agents already in employment and 4 temporary agents offered a position but not yet in employment).

AST 2				1
AST 1				
Total number of ASTs		16		14
AST/SC 6				
AST/SC 5				
AST/SC 4				
AST/SC 3				
AST/SC 2				
AST/SC 1				
Total number of AST/SCs				
TOTAL		**59**		**51**

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

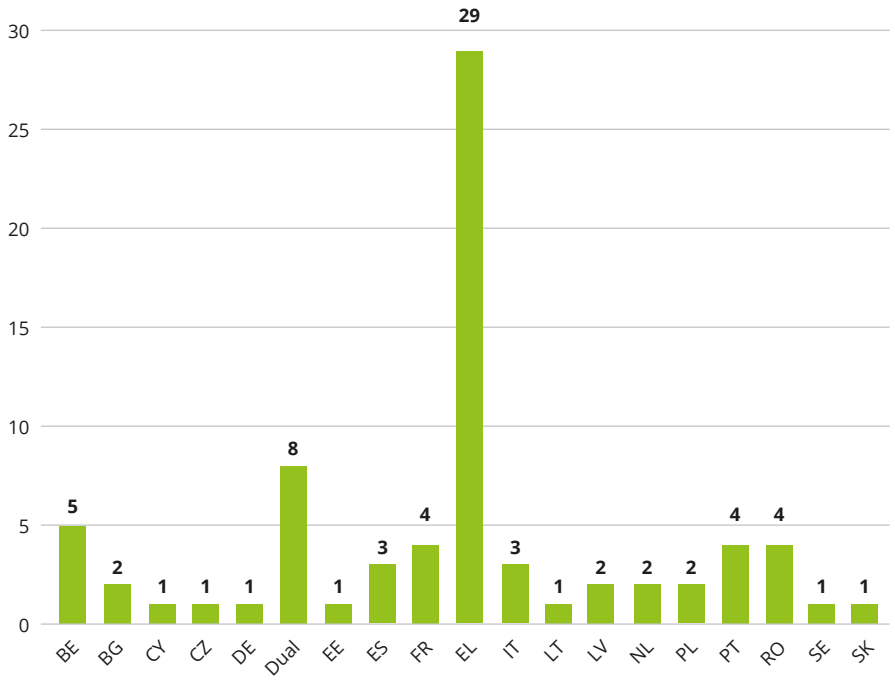
Job type	2019	2018	2017
Total administrative support and coordination	**18.37 %**	**22.89 %**	**19.28 %**
Administrative support	15.31 %	19.28 %	15.66 %
Coordination	3.06 %	3.61 %	3.61 %
Total operational	**70.41 %**	**62.65 %**	**66.27 %**
Total operational coordination	5.10 %	7.23 %	7.23 %
General operational	65.31 %	55.42 %	59.04 %
Total neutral	**11.22 %**	**14.46 %**	**14.46 %**
Finance and control	11.22 %	14.46 %	14.46 %

The bechmarking exercise follow the European Commission's methodology.

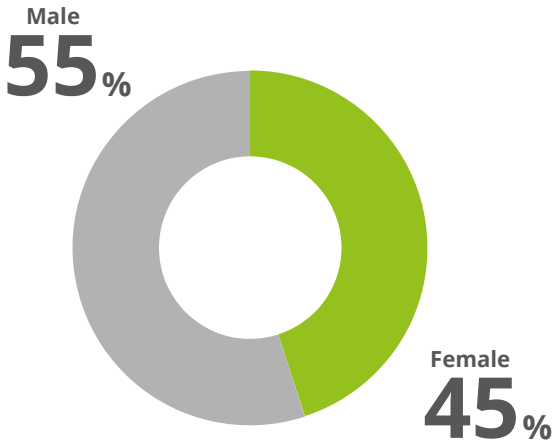
Human resources statistics

On 31 December 2019, the agency had a total of 75 statutory staff in-house.

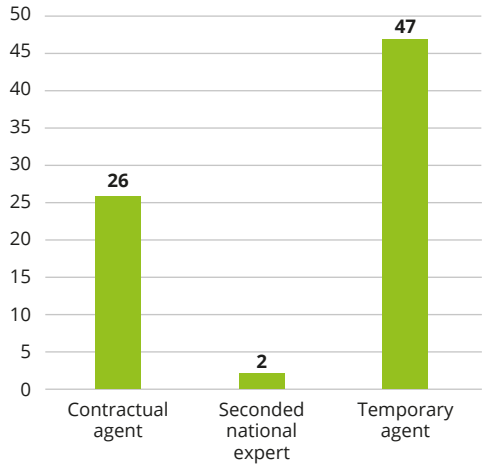
Employees by nationality



Gender distribution – all departments



Number of employees by contract type



Implementing rules

Decision No MB 14/2019 of the Management Board adopting the implementing rules on the general provisions for implementing Article 79(2) of the conditions of employment of other servants of the European Union, governing the conditions of employment of contract staff employed under the terms of Article 3a thereof.

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 in facing emerging NIS challenges	11.51	9
Activity 2: POLICY. Promote NIS as an EU policy priority	27.45	16.9
Activity 3: CAPACITY. Support Europe in maintaining state-of-the-art NIS capacities	11.81	7.5
Activity 4. COMMUNITY. Foster the emerging European NIS community	11.81	10.6
Activity 5: ENABLING. Improve ENISA's impact	35.42	43.57
Total Activities 1–5	98.00	87.57

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

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 2019 leasing expenditure of its offices.

In addition, ENISA signed 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) 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.

ANNEX 7
ENVIRONMENTAL MANAGEMENT

No additional information available for 2019 in relation to Part II.11, 'Environmental management'.

ANNEX 8
ANNUAL ACCOUNTS

Statement of financial position

Assets and liabilities	Financial position on 31.12.2019 (in EUR)	Financial position on 31.12.2018 (in EUR)
I. Non-current assets	746 216	672 006
Intangible fixed assets	52 469	79 844
Tangible fixed assets	677 247	575 662
Guarantee for leased building	16 500	16 500
II. Current assets	5 084 080	1 595 549
Short-term receivables	180 191	62 589
Cash and cash equivalents	4 903 889	1 532 960
TOTAL ASSETS (I + II)	**5 830 296**	**2 267 555**
III. Non-current liabilities	0	0
Long-term provision for risk and charges	0	0
IV. Current liabilities	1 392 974	570 855
Commission pre-financing received	579 113	110 505
Accounts payable	41 578	54 603
Accrued liabilities	772 283	405 747
TOTAL LIABILITIES (III + IV)	**1 392 374**	**570 855**
V. Net assets	4 437 322	1 696 700
Accumulated result	1 696 700	1 855 736
Surplus (/deficit) for the year	2 740 622	– 159 036
TOTAL LIABILITIES AND NET ASSETS (III + IV + V)	**5 830 296**	**2 267 555**

Statement of financial performance

Revenue and expenses	2019 financial performance (in EUR)	2018 financial performance (in EUR)
Revenue from the EU subsidy	15 713 839	10 667 121
Revenue from administrative operations	557 472	753 419
Total operating revenue	16 271 311	11 420 540
Administrative expenses	– 10 411 311	– 9 430 560
Staff expenses	– 6 369 310	– 6 205 185
Fixed-asset-related expenses	– 234 090	– 281 880
Other administrative expenses	– 3 807 911	– 2 943 495
Operational expenses	– 3 115 939	– 2 147 214
Total operating expenses	– 13 527 250	– 11 577 774
Surplus (/deficit) from operating activities	2 744 061	– 157 234
Financial revenues	0	0
Financial expenses	– 1 637	– 1 113
Exchange rate loss	– 1 802	– 689
Surplus (/deficit) from non-operating activities	– 3 439	– 1 802
Surplus (/deficit) from ordinary activities	2 740 622	– 159 036
Surplus (/deficit) for the year	2 740 622	– 159 036

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
SOP	standard operating procedure
SOPex	SOP exercise

ANNEX 10
LIST OF POLICY REFERENCES

The agency arranges its work within the wider context of the legal and policy environment as laid out below. Its activities and tasks are fulfilled as defined by its regulation and integrated into this broader legal framework and policy context.

Topics	Policy/legislation reference – with titles and hyperlinks
2019	
CSA	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN
Seat agreement	Seat Agreement between the Government of the Hellenic Republic and the European Union Agency for Network and Information Security (ENISA), the 'European Union Agency for Cybersecurity (ENISA)'
2018	
2018 work programme	ENISA Programming Document 2018–2020
2017	
Proposed ePrivacy regulation	Proposal for a Regulation on Privacy and Electronic Communications
2017 work programme	ENISA Programming Document 2017–2019 with Amendments – Including multiannual planning, work programme 2017 and multiannual staff planning – Consolidated version with amendments adopted by the Management Board on 05/09/2017 (Decision No MB/2017/6)
ENISA strategy	ENISA Strategy – 2016–2020, available at: https://www.enisa.europa.eu/publications/corporate/enisa-strategy
2017 cybersecurity strategy	Joint communication to the European Parliament and the Council – Resilience, deterrence and defence: building strong cybersecurity for the EU, JOIN(2017) 450 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN
CSA, proposed ENISA regulation	Proposal for a regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on information and communication technology cybersecurity certification ('Cybersecurity Act'), COM(2017) 477 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN
Council conclusions on 2017 cybersecurity strategy	Council conclusions of 20 November 2017 on the Joint communication to the European Parliament and the Council – Resilience, deterrence and defence: building strong cybersecurity for the EU, available at: http://www.consilium.europa.eu/media/31666/st14435en17.pdf
Proposed ePrivacy regulation	Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (regulation on privacy and electronic communications), COM(2017) 10 final available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010&from=EN

Topics	Policy/legislation reference – with titles and hyperlinks
NISD	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1, available at: http://data.europa.eu/eli/dir/2016/1148/oj
Commission Communication COM(2016) 410 on the contractual public–private partnership on cybersecurity	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Strengthening Europe's cyber resilience system and fostering a competitive and innovative cybersecurity industry, COM(2016) 410 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0410
Commission Decision C(2016) 4400 on the contractual public–private partnership on cybersecurity	Commission decision of 5.7.2016 on the signing of a contractual arrangement on a public–private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation, C(2016) 4400 final, available (along with the annex) at: https://ec.europa.eu/digital-single-market/en/news/commission-decision-establish-contractual-public-private-partnership-cybersecurity-cppp
Joint communication on countering hybrid threats	Joint communication to the European Parliament and the Council – Joint framework on countering hybrid threats – a European Union response, JOIN(2016) 18 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (general data protection regulation), OJ L 119, 4.5.2016, p. 1, available at: http://data.europa.eu/eli/reg/2016/679/oj
Law enforcement agency data protection directive	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89, available at: http://data.europa.eu/eli/dir/2016/680/oj
Passenger name record directive	Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132, available at: http://data.europa.eu/eli/dir/2016/681/oj
2015	
Digital single market strategy for Europe	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A digital single market strategy for Europe, COM(2015) 192 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX:52015DC0192
Payment services directive	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23.12.2015, p. 35, available at: http://data.europa.eu/eli/dir/2015/2366/oj
European agenda on security	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – The European agenda on security, COM(2015) 185 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2015:0185:FIN
2014	
eIDAS regulation	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73, available at: http://data.europa.eu/eli/reg/2014/910/oj
Commission communication on a thriving data-driven economy	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Towards a thriving data-driven economy, COM(2014) 442 final, available at: https://ec.europa.eu/digital-agenda/en/news/communication-data-driven-economy

Topics	Policy/legislation reference – with titles and hyperlinks
2013	
Council conclusions on the cybersecurity strategy	Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint communication on the cybersecurity strategy of the European Union: An open, safe and secure cyberspace, agreed by the General Affairs Council on 25 June 2013, available at: http://register.consilium.europa.eu/pdf/en/13/st12/st12109.en13.pdf
Cybersecurity strategy of the EU	Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Cybersecurity strategy of the European Union: An open, safe and secure cyberspace, JOIN(2013) 1 final, available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667
ENISA regulation	Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, OJ L 165, 18.6.2013, p. 41, available at: http://data.europa.eu/eli/reg/2013/526/oj
Directive on attacks against information systems	Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14.8.2013, p. 8, available at: http://data.europa.eu/eli/dir/2013/40/oj
Framework financial regulation	Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council, OJ L 328, 7.12.2013, p. 42, available at: http://data.europa.eu/eli/reg_del/2013/1271/oj
Commission Regulation (EU) No 611/2013 on the measures applicable to the notification of personal data breaches	Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, OJ L 173, 26.6.2013, p. 2, available at: http://data.europa.eu/eli/reg/2013/611/oj
2012	
Action plan for an innovative and competitive security industry	Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee – Security industrial policy action plan for an innovative and competitive security industry, COM(2012) 417 final, available at: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX %3A52012DC0417
European cloud computing strategy	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Unleashing the potential of cloud computing in Europe, COM(2012) 529 final, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF
European Parliament resolution on critical information infrastructure protection (CIIP)	European Parliament resolution of 12 June 2012 on critical information infrastructure protection – achievements and next steps: towards global cyber-security (2011/2284(INI)), available at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167
2011	
Council conclusions on CIIP	Council conclusions on critical information infrastructure protection 'Achievements and next steps: towards global cyber-security' (CIIP) http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010299%202011%20INIT
Commission communication on CIIP (old – focus up to 2013)	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on critical information infrastructure protection – 'Achievements and next steps: towards global cyber-security', COM(2011) 163 final, available at: http://ec.europa.eu/transparency/regdoc/rep/1/2011/EN/1-2011-163-EN-F1-1.Pdf
EU-LISA regulation	Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, OJ L 286, 1.11.2011, p. 1, (consolidated version, after amendments), available at: http://data.europa.eu/eli/reg/2011/1077/2015-07-20

Topics	Policy/legislation reference – with titles and hyperlinks
Single market act	Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – Single market act – twelve levers to boost growth and strengthen confidence – 'working together to create new growth', COM(2011) 206 final, available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52011DC0206
Telecoms Ministerial Conference on CIIP	Telecoms Ministerial Conference on CIIP organised by the Presidency in Balatonfüred, Hungary, 14 and 15 April 2011
2010	
Internal security strategy for the European Union	EU Internal Security Strategy, 6870/10, available at: https://data.consilium.europa.eu/doc/document/ST-6870-2010-INIT/en/pdf
Digital agenda	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A digital agenda for Europe, COM(2010) 245 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010DC0245&from=EN
2009	
Commission communication on IoT	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Internet of things – An action plan for Europe, COM(2009) 278 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2009:0278:FIN
Council resolution of December 2009 on NIS	Council Resolution of 18 December 2009 on a collaborative European approach to network and information security, OJ C 321, 29.12.2009, p. 1, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex %3A32009G1229(01)
2002	
Framework Directive 2002/21/EC	Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (framework directive), OJ L 108, 24.4.2002, p. 33 (consolidated version, after amendments), available at: http://data.europa.eu/eli/dir/2002/21/2009-12-19
ePrivacy Directive 2002/58/EC	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37, (consolidated version, after amendments), available at: http://data.europa.eu/eli/dir/2002/58/2009-12-19

ANNEX 11
LIST OF MANAGEMENT BOARD MEMBERS IN 2019

List of ENISA Management Board representatives and alternates
Commission representatives

Representative	Alternate
Despina SPANOU Director Digital Society, Trust and Cybersecurity DG Communications Networks, Content and Technology Tel. +32 22990245 Email: despina.spanou(at)ec.europa.eu	**Miguel GONZALEZ-SANCHO** Head of Unit Cybersecurity Technology and Capacity Building DG Communications Networks, Content and Technology Email: miguel.gonzalez-sancho-bodero(at)ec.europa.eu **Jakub BORATYNSKI** Head of Unit Cybersecurity and Digital Privacy Policy DG Communications Networks, Content and Technology Tel. +32 22969452 Email: jakub.boratynski(at)ec.europa.eu
Ken DUCATEL Chief Information Security Officer DG Informatics Email: ken.ducatel(at)ec.europa.eu	**Grzegorz MINCZAKIEWICZ** Head of Unit Information Technology Unit DG Informatics Email: qrzegorz.minczakiewicz(at)ec.europa.eu

Member State representatives

Member State	Representative	Alternate
Belgium (Belgique/België)	**Miguel DE BRUYCKER** Director Centre for Cybersecurity Tel. +32 22040561 info(at)ccb.belgium.be Email: miguel.debruycker(at)ccb.belgium.be	**Phédra CLOUNER** Vice-Director Centre for Cybersecurity
Bulgaria (България)	**Krasimir SIMONSKI** Executive Director Executive agency 'Electronic Communication Networks and Information Systems' Email: ksimonski(at)e-gov.bg	**Vasil GRANCHAROV** Director Network and Information Security Directorate Executive agency 'Electronic Communication Networks and Information Systems' Email: vgrancharov(at)e-gov.bg
Czechia (Česko)	**Jaroslav SMID** Deputy Director National Centre for Cyber Security National Security Authority of the Czech Republic Email: j.smid(at)nukib.cz	**Roman PACKA** Assistant Director of National Security Authority of the Czech Republic Email: r.packa(at)nukib.cz
Denmark (Denmark)	**Thomas LUND-SORENSEN** Director Centre for Cyber Security Danish Defence Intelligence Service Email: Policy(at)cfcs.dk	**Thomas WULFF** Senior Adviser Danish Ministry of Defence Centre for Cyber Security Tel. +45 40375344 Email: thowul(at)cfcs.dk

Member State	Representative	Alternate
Germany (Deutschland)	**Horst SAMSEL** Head of Department Federal Office for Information Security	**Martin BIERWIRTH** Federal Office for Information Security Email: SIB(at)bsi.bund.de
Estonia (Eesti)	**Margus NOORMAA** Director-General Information System Authority Email: margus.noormaa(at)ria.ee	**Piret URB** Head of International Relations Information System Authority Email: piret.urb(at)ria.ee
Ireland (Éire/Ireland)	**Kevin FOLEY** National Cyber Security Unit Department of Communications, Energy and Natural Resources Email: kevin.foley(at)dcenr.gov.ie	
Greece (Ελλάδα/Ellada)	**Antonis TZORTZAKAKIS** Secretary-General of Telecommunications and Post Ministry of Digital Governance Email: a.tzortzakakis(at)mindigital.gr	**Theofanis ANAGNOSTOPOULOS** Head of Electronic Communications Department Directorate-General of Telecommunications and Post Secretariat-General of Telecommunications and Post Ministry of Digital Policy, Telecommunications and Media Email: f.anagnostop(at)mindigital.gr Tel. +30 2109098861
Spain (España)	**Alejandro PINTO GONZALEZ** Adviser on Cybersecurity National Security Department Tel. +34 915997349 Email: ajpinto(at)dsn.presidencia.gob.es	**Maria del Mar LOPEZ GIL** Head of Cybersecurity Office National Security Department
France (France)	**Jean-Baptiste DEMAISON** CHAIR OF ENISA MANAGEMENT BOARD *Agence nationale de la sécurité des systèmes d'information* Email: international.enisa-mb(at)ssi.gouv.fr	
Croatia (Hrvatska)	**Damir SUŠANJ** IT Department Manager Croatian Regulatory Authority for Network Industries Email: damir.susanj(at)hakom.hr	
Italy (Italia)	**Eva SPINA** Director-General Ministry of Economic Development Tel. +39 0654444952 Email: eva.spina(at)mise.gov.it	**Fabrizio GENTILI** Counsellor Telecommunications and Information Society, Audiovisual, Postal Services Permanent Representation of Italy to the EU Tel. + 32 22200574 Email: tlc(at)rpue.esteri.it
Cyprus (Κύπρος)	**Antonis ANTONIADES** Senior Officer Office of the Commissioner of Electronic Communications and Postal Regulation Email: antonis.antoniades(at)ocecpr.org.cy	**Costas EFTHYMIOU** Officer of Technical Affairs Office of the Commissioner of Electronic Communications and Postal Regulation Email: costas.efthymiou(at)ocecpr.org.cy
Latvia (Latvija)	**Sanita ZOGOTA** Head of National Cyber Security Policy Coordination Section Crisis Management Department Ministry of Defence sanita.zogota(at)mod.gov.lv lv_enisa_mb(at) mod.gov.lv	**Viktors LIPENITS** Head of Transport and Communications Division Ministry of Transport and Communications Email: viktors.lipenits(at)sam.gov.lv
Lithuania (Lietuva)	**Rytis RAINYS** Director of National Cyber Security Centre Ministry of Defence Tel. +370 61114018 Email: rytis.rainys(at)kam.lt	**Viktoras PINKEVICIUS** Head of Critical Infrastructure Division National Cyber Security Centre Ministry of Defence Email: viktoras.pinkevicius(at)kam.lt

Member State	Representative	Alternate
Luxembourg (Luxembourg)	**François THILL** *Accréditation, notification et surveillance des prestataires de services de confiance* Email: francois.thill(at)eco.etat.lu	**Paul HERLING** High Commission for National Protection National Agency for the Security of Information Systems Email: paul.herling(at)anssi.etat.lu
Hungary (Magyarország)	**Zoltan RAJNAJ** Cyber Coordinator of Hungary Ministry of Interior	**Bela Ferenc VERECKEI** President National Information Security Authority Ministry of Interior Email: bela.vereckei(at)govcert.hu
Malta (Malta)	**John AGIUS** Director of Critical Infrastructure Protection Malta Critical Infrastructure Protection Directorate Cabinet Office Office of the Prime Minister Email: john.f.agius(at)gov.mt Email: maltacip(at)gov.mt	**Matthew YEOMANS**
Netherlands (Nederland)	**Hans DE VRIES** Head of the National Cyber Security Centre and Deputy Director of Cyber Security, Ministry of Security and Justice Email: hans.devries(at)ncsc.nl	**Pieter VAN DEN BERG** National Coordinator for Security and Counterterrorism Directorate for Cyber Security Ministry of Justice and Security Email: p.j.van.den.berg1(at)nctv.minvenj.nl
Austria (Österreich)	**Reinhard POSCH** Chief Information Officer for the Austrian government. Email: reinhard.posch(at)cio.gv.at	**Herbert LEITOLD** Secure Information Technology Centre Austria Institute for Applied Information Processing and Communication, Graz Email: herbert.leitold(at)iaik.at
Poland (Polska)	**Krzysztof SILICKI** Deputy Head of NASK Director for Cybersecurity and Innovation Tel. +48 223808345 Email: krzysztof.silicki(at)nask.pl	**Przemyslaw JAROSZEWSKI** Chief Security Specialist Head of CERT Polska, NASK
Portugal (Portugal)	**Lino SANTOS** Head of National Cybersecurity Centre Email: secretariado(at)cncs.gov.pt	**Isabel BAPTISTA** Head of Development and Innovation Unit National Cybersecurity Centre Email: secretariado(at)cncs.gov.pt
Romania (România)	**Catalin Petrica ARAMA** Director-General CERT Romania Email: catalin.arama(at)cert-ro.eu	**Iulian ALECU** CERT Romania Tel. +40 745750816 Email: iulian.alecu(at)cert.ro
Slovenia (Slovenija)	**Uroš SVETE** Acting Director Information Security Administration Ministry of Public Administration Email: uros.svete(at)gov.si	**Marjan KAVČIČ** Information Society Directorate Ministry of Public Administration Email: marjan.kavcic1(at)gov.si
Slovakia (Slovensko)	**Rastislav JANOTA** Chair of Cybersecurity Committee Security Council of Slovak Republic Director of Slovakian CERT National Security Authority	**Martina LISICKA** Director of Euro–Atlantic Relations Division National Security Authority Email: martina.lisicka(at)nbu.gov.sk
Finland (Suomi/Finland)	**Olli LEHTILÄ** Senior Officer Ministry of Transport and Communications Data Department, Safety and Security Unit Tel. +358 503212806 Email: olli.lehtila(at)lvm.fi	**Heidi KIVEKÄS** Senior Specialist National Cyber Security Centre Finland Finnish Transport and Communications Agency Email: heidi.kivekas(at)traficom.fi

Member State	Representative	Alternate
Sweden (Sverige)	**Vacant**	**Staffan LINDMARK** Head of Section Swedish Post and Telecoms Authority Network Security Department Email: staffan.lindmark(at)pts.se
United Kingdom	**Sarah BAILEY** EU Cyber Security Policy Cyber Security Data and Cyber Security Directorate Email: sarah.bailey(at)culture.gov.uk	**Colin WHORLOW** Head of International Standards National Cyber Security Centre Email: colin.whorlow(at)ncsc.gov.uk

EEA country representatives (observers)

Iceland	**Sigurdur Emil PALSSON** Chief National Cyber Security Adviser Department of Digital Communication Ministry of Transport and Local Government Email: sigurdur.palsson(at)srn.is	
Liechtenstein	**Rainer SCHNEPFLEITNER** Director Office for Communications Tel. +423 2366480 Email: rainer.schnepfleitner(at)llv.li	**Markus SKAROHLID** Legal Officer Office of Communications Tel. +423 2366481 Email: markus.skarohlid(at)llv.li
Norway	**Hilde Goutal Muller** Ministry of Transport and Communication Email: hilde-goutal.mueller(at)kmd.dep.no	**Martin KJELLSEN**

ANNEX 12
LIST OF MANAGEMENT BOARD DECISIONS ADOPTED IN 2019

MB/2019/1	On the statement of estimates for 2020 and programming document 2020–2022
MB/2019/2	Implementing rules concerning the tasks, duties and powers of the data protection officer pursuant to Article 45(3) of Regulation (EU) 2018/1725
MB/2019/3	Amending the programming document 2019–2021 and statement of estimates 2019 with Annex 1 and Annex 2
MB/2019/4	On the final accounts of the financial year 2018
MB/2019/5	On analyses and assessment of the Annual Activity Report 2018
MB/2019/6	Appointing the executive director of ENISA and adopting the annex to the Management Board decision (contract).
MB/2019/7	Authorising an occupational activity after leaving the service
MB/2019/8	On financing rules
MB/2019/9	On a transfer from Title 1 'Staff expenditure' to Title 2 'Buildings, equipment and miscellaneous operating expenditure' for an amount of EUR 1.6 million
MB/2019/10	On internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of ENISA
MB/2019/11	On the establishment and operation of ad hoc working groups for European cybersecurity certification scheme
MB/2019/12	On the internal control framework for effective management applicable to the European Union Agency for Cybersecurity
MB/2019/13	Delegating the relevant appointing authority powers to the executive director
MB/2019/14	Adopting implementing rules on the general provisions for implementing Article 79(2) of the Conditions of Employment of Other Servants of the European Union, governing the conditions of employment of contract staff employed under the terms of Article 3a thereof
MB/2019/15	Amending the Decision No MB/2013/6 on internal rules of procedure for the ENISA Management Board and for the ENISA Executive Board
MB/2019/16	Adopting the programming document 2020–2022, the statement of estimates 2020 and the establishment plan 2020
MB/2019/17	On public access to ENISA documents

TPAB-20-001-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 on 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

ISBN 978-92-9204-348-3