EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ANNUAL ACTIVITY REPORT

2018

ISSN 2314-9434

CONTACT

For contacting ENISA please use the following details:
press@enisa.europa.eu
Info@enisa.europa.eu
website: www.enisa.europa.eu

COPYRIGHT NOTICE

Print	ISBN 978-92-9204-298-1	ISSN 1830-981X	doi:10.2824/884806	TP-AB-19-001-EN-C
PDF	ISBN 978-92-9204-297-4	ISSN 2314-9434	doi:10.2824/582430	TP-AB-19-001-EN-N

ANNUAL ACTIVITY REPORT 2018

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA MANAGEMENT BOARD ASSESSMENT

THE ANALYSES AND ASSESSMENT BY THE MANAGEMENT BOARD OF ENISA OF THE CONSOLIDATED ANNUAL ACTIVITY REPORT FOR THE YEAR 2018 OF THE AUTHORISING OFFICER OF ENISA

The Management Board takes note of the Annual Activity Report (AAR) for the financial year 2018, submitted by the Executive Director of the European Union Agency for Cybersecurity (ENISA) in accordance with Article 47 of the Financial Regulation applicable to ENISA.

The Management Board received a copy of the 2018 Annual Activity Report produced by the Executive Director of ENISA in his quality of Authorising Officer for the implementation of the annual budget on 21 June 2019.

In analysing and assessing the AAR 2018, the Management Board makes the following conclusions:

- The AAR presents key results of the implementation of the ENISA Work programme 2018 and leads to conclusion that the Agency completed all deliverables agreed with the Management Board in the Work Programme 2018.

- ENISA produced 40 reports on different aspects of network and information security. A relevant set of published reports, papers, workshops, meetings and events are listed as part of the result achieved by the Agency. Impact indicators show that the Agency's results exceeded the targets established in the Work Programme 2018, against the framework of the ENISA Strategy 2016-2020.

- At the same time, there was an increased focus on communicating ENISA's work and concepts to the European Parliament, the Council and the European Commission, along with other EU agencies. In 2018 following on from last year's tradition, ENISA organised several events such as the Annual Privacy Forum, IoT Security Conference and the Cyber Exercise.

- Two major European projects were also supported by ENISA: the EU Cyber Security Month — a specific month dedicated to activities on cybersecurity and security/ privacy awareness— and the EU Cybersecurity Challenge event — a competition based on a series of technical challenges between teams of students from different Member States.

- Overall, the AAR is in line with the ENISA Work Programme 2018 and ENISA's work is well aligned with the overall European Union agenda for digital single market. A coherent link is provided between activities planned in the Work Programme 2018 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 expenditure appropriations were committed at a rate of 99.9 %. The respective payment rate on expenditure appropriations was 89,25% in 2018.

- The AAR also provides a follow up of the 2016 Discharge and control results. The agency has three open recommendations from the Internal Audit Service in 2018. This section also notes the main categories of deviation that led to exceptions reported. In

2018 the agency recorded 33 exceptions. 26 of them are under the materiality levels and are minor administrative nature with no financial impact. Of the seven remaining, a posteriori commitments were reported.

- 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 2018. The Management Board notes with satisfaction that ENISA could deliver work programme 2018 in spite of high staff turnover and under condition of limited budgetary resources. 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 2018 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.

TABLE OF CONTENTS

ENISA Management board assessment 2
A message from the Executive Director 8
Introduction 11

PART I
ACHIEVEMENTS IN THE IMPLEMENTATION OF THE 2018 WORK PROGRAMME 17

1.1 KEY RESULTS IN THE IMPLEMENTATION OF ACTIVITY 1 — EXPERTISE: ANTICIPATE AND SUPPORT EUROPE IN FACING EMERGING NETWORK AND INFORMATION SECURITY CHALLENGES 18
1.1.1 Objective 1.1. Improving the expertise related to network and information security 18
1.1.1.1 Output O.1.1.1. Good practices for security of the internet of things (priority 1) 18
1.1.2 Objective 1.2. Network and information security threat landscape and analysis 18
1.1.2.1 Output O.1.2.1. Annual European Union Agency for Network and Information Security threat landscape (priority 1) 18
1.1.2.2 Output O.1.2.2. Restricted and public info notes on network and information security (priority 1) 19
1.1.2.3 Output O.1.2.3. Support incident reporting activities in the European Union 19
1.1.3 Objective 1.3. Research and development, innovation 20
1.1.3.1 Output O.1.3.1. Guidelines for European standardisation in the field of information and communications technology security (priority 1) 20
1.1.3.2 Output O.1.3.2 Priorities for European Union research and development (priority 1) 20
1.1.4 Objective 1.4. Response to Article 14 requests under expertise activity 20
1.1.4.1 Output O.1.4.1 — Response to requests under expertise activity (priority 1) 20
1.1.5 Type of outputs and performance indicators for each outputs of Activity 1 — expertise 21
1.1.6 Specific results: mapping of outputs into papers, publications or activities 22

1.2 KEY RESULTS IN THE IMPLEMENTATION OF ACTIVITY 2 — POLICY: PROMOTE NETWORK AND INFORMATION SECURITY AS A EUROPEAN UNION POLICY PRIORITY 22
1.2.1 Objective 2.1. Supporting European Union policy development 22
1.2.1.1 Output O.2.1.1 Support the policy discussions in the area of certification of products and services (priority 1) 23
1.2.1.2 Output O.2.1.2 Towards a framework for policy development in cybersecurity (priority 1) 23
1.2.2 Objective 2.2. Supporting European Union policy implementation 23
1.2.2.1 Output O.2.2.1 Recommendations supporting implementation of the eIDAS regulation (priority 1) 23
1.2.2.2 Supporting the implementation of the network and information systems directive (priority 1) 23
1.2.2.3 Output O.2.2.3. Baseline security recommendations for the operator of essential services sectors and digital service providers (priority 1) 24
1.2.2.4 Output O.2.2.4 Supporting the payment services directive implementation (priority 1) 24
1.2.2.5 Output O.2.2.5. Contribute to European Union policy in the area of privacy and data protection (priority 2) 24
1.2.2.6 Output O.2.2.6. Network and information systems directive transposition (priority 1) 25
1.2.3 Objective 2.3. Response to Article 14 requests under policy activity 25
1.2.3.1 Output O.2.3.1. Response to requests under policy activity (priority 1) 25
1.2.4 General results: achievement of performance indicators for Activity 2 26
1.2.5 Specific results: mapping of deliverables into papers, publications or activities 28

1.3 KEY RESULTS IN THE IMPLEMENTATION OF ACTIVITY 3 — CAPACITY: SUPPORT EUROPE IN MAINTAINING STATE-OF-THE-ART NETWORK AND INFORMATION SECURITY CAPACITIES 29
1.3.1 Objective 3.1. Assist Member States' capacity building 29
1.3.1.1 Output O.3.1.1. Update and provide technical training for Member State and European Union bodies (priority 1) 29
1.3.1.2 Output O.3.1.2. Support European Union Member States in the development and assessment of national cybersecurity strategies 29
1.3.1.3 Output O.3.1.3 — Support EU Member States in their incident response development (Priority 1) 30
1.3.2 Objective 3.2. Support European Union institutions' capacity building 30
1.3.2.1 Output O.3.2.1 Representation of the European Union Agency for Network and Information Security on the Steering Board of CERT EU and representation of the EU agencies using the CERT EU service (priority 1) 30
1.3.3 Objective 3.3. Assist in improving private sector capacity building and general awareness 31
1.3.3.1 Output O.3.3.1, Cybersecurity challenges (priority 1) 31
1.3.3.2 Output O.3.3.2. European Cyber Security Month deployment (priority 1) 31
1.3.4 Objective 3.4. Response to Article 14 requests under capacity activity 31
1.3.4.1 Output O.3.4.1. Response to requests under capacity activity (priority 1) 31
1.3.5 General results: achievement of performance indicators for Activity 3 32
1.3.6 Specific results: mapping of deliverables into papers/publications/activities 33
1.4 KEY RESULTS IN THE IMPLEMENTATION OF ACTIVITY 4 — COMMUNITY: FOSTER THE EMERGING EUROPEAN NETWORK AND INFORMATION SECURITY COMMUNITY 34
1.4.1 Objective 4.1. Cyber crisis cooperation 34
1.4.1.1 Output O.4.1.1 — Cyber Europe 2018 (priority 1) 34
1.4.1.2 Output O.4.1.2 — Lessons learnt and advice related to cyber crisis cooperation (priority 1) 35
1.4.1.3 Output O.4.1.3 — Support activities for cyber exercise planning and cyber crisis management (priority 1) 35
1.4.2 Objective 4.2. Computer security incident response teams and other network and information security community building 36
1.4.2.1 Output O.4.2.1. European Union computer security incident response teams network secretariat and support for European Union computer security incident response teams network community building (priority 1) 36
1.4.2.2 Output O.4.2.2. Support the fight against cybercrime and collaboration between computer security incident response teams and law enforcement agencies (priority 1) 36
1.4.3 Objective 4.3. Response to Article 14 requests under community activity 36
1.4.3.1 Output O.4.3.1 — Response to requests under community activity (priority 1) 36
1.4.4 General results: achievement of performance indicators for Activity 4 37
1.4.5 Specific results: mapping of deliverables into papers/publications/activities 38
General results from previous years 38
1.5 KEY RESULTS IN THE IMPLEMENTATION OF ACTIVITY 5 — ENABLING: REINFORCE THE EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY'S IMPACT 39
1.5.1 Objective 5.1. Management and compliance 39
1.5.1.1 Management 39
1.5.1.2 Data protection compliance tasks and data protection officer 39
1.5.1.3 Information Security Officer 40
1.5.2 Objective 5.2. Engagement with stakeholders and strong international activities 40

PART II
ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL 43

2.1 FINANCIAL MANAGEMENT AND INTERNAL CONTROL 43
2.1.1 Financial management 43
2.1.1.1 Budget execution of European Union subsidy (current year 2018 - C1 funds) 43
2.1.1.2 Amending budgets and budgetary transfers 43
2.1.1.3 Carry forward of commitment appropriations 44
2.1.2 Controls 45
2.1.2.1 Internal Controls 45
2.1.2.2 Audit observations and recommendations 46
2.1.3 Assessment of the effectiveness of the internal control systems 48

2.2 DECLARATION OF ASSURANCE 48
2.2.1 Review of the elements supporting assurance 49
2.2.2 Human resources management 49

ANNEX 1
HUMAN RESOURCES 53

A.1.1 ORGANISATIONAL CHART 53

A.1.2 ESTABLISHMENT PLAN 2018 55

A.1.3 INFORMATION ON ENTRY LEVEL FOR EACH TYPE OF POST 56

A.1.4 INFORMATION ON BENCHMARKING EXERCISE 56

A.1.5 HUMAN RESOURCES STATISTICS 57

A.1.6 HUMAN RESOURCES BY ACTIVITY 58

ANNEX 2
FINANCIAL RESOURCES 59

A.2.1 PROVISIONAL ANNUAL ACCOUNTS 2018 59

A.2.2 FINANCIAL REPORTS 2018 60

ANNEX 3
OTHER ANNEXES 64

A.3.1 LIST OF ACRONYMS AND INITIALISMS 64

A.3.2 LIST OF POLICY REFERENCES 65

A MESSAGE FROM THE EXECUTIVE DIRECTOR

I am proud to report another successful year for the European Union Agency for Network and Information Security (ENISA): 2018 was a challenging but overall very rewarding year for the agency. ENISA delivered on the priorities set out in the work programme including vital work in areas supporting the digital single market.

The year 2018 saw successful negotiations on the proposed Cybersecurity Act, including the new mandate for ENISA, which will allow the agency to better serve the cybersecurity needs of Europe. A political agreement on the Cybersecurity Act was reached in December 2018 establishing a permanent mandate and reinforced role for ENISA. The cybersecurity certification framework that was agreed will offer an opportunity for ENISA to prepare candidate schemes.

Additionally, 2018 was also a year where the majority of EU Member States transposed the directive on network and information systems directive (NISD), which ENISA supported by contributing to the work of the Cooperation Group and developing the computer security incident response teams (CSIRT) network. The successful outcome of this implementation and that of the second payment services directive means that we are enhancing Europe's cybersecurity but also increasing trust in the digital single market.

ENISA continued working on its annual flagship deliverables such as the cyber exercises, the Annual Privacy Forum, the internet of things (IoT) security conference and the cyberthreat landscape. The CSIRTs network has also developed its midterm work programme objectives. The ENISA inventory of incident response teams listed 383 teams in December 2018 compared to 342 at the end of previous year demonstrating a continual growth of incident response capabilities in Europe. ENISA continues to support EU Member States in developing a harmonised approach to supervision of security requirements and cybersecurity breach reporting in the EU telecoms and electronic trust services sectors.

ENISA fully achieved its 2018 objectives: it successfully completed the work programme in a timely manner, within budget and in compliance with our legal framework, due to the robust management of internal resources and implemented procedures. The 'introduction' section contains a summary with highlights of ENISA activities during 2018.

The agency has successfully reached its targets due to the commitment of its staff, effective collaboration with its stakeholders and the valuable cooperation and direction provided by the Management Board. I take this opportunity to thank the members of the Management Board for their contributions and dedication during 2018.

As we look toward the future, there is no doubt that 2019 will be a challenging year as the new Cybersecurity Act is adopted and ENISA will take on a new role in cybersecurity certification.

Udo Helmbrecht

Executive Director, ENISA

INTRODUCTION

THE EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY IN BRIEF

ENISA was established in 2004 by Regulation (EC) No 460/2004 of the European Parliament and the Council. 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 introduced a small change in the name, updated its objectives and extended its mandate until 19 June 2020.

ENISA is a centre of expertise for network and information security and cybersecurity in Europe. ENISA supports the European Union and its Member States in enhancing and strengthening their ability and preparedness to prevent, detect and respond to network and information security problems and incidents. ENISA's vision is to secure and enable Europe's information society and to use its unique competencies to help to drive the cyber landscape in Europe.

The agency works closely with members of both the public and private sectors to deliver advice and guidelines based on solid operational experience. ENISA also supports the development of EU policies and laws on matters relating to network and information security (NIS), thereby contributing to economic growth in the EU's internal market.

Last but not least, ENISA coordinates the pan-European cybersecurity exercise, which is unique in its scope and impact and brings together all of the EU Member States every 2 years to test their cooperation mechanisms while working in their own operational environments.

THE YEAR IN BRIEF

The key achievements of 2018 are as follows.

ENISA produced 40 reports on different aspects of network and information security. These include the latest version of the ENISA threat landscape, guidelines on assessing the security of digital service providers (DSPs) and the compliance of operators of essential services (OESs) with the security requirements set out in the NISD. Additionally, ENISA reports focused on an IoT security standards gap analysis, economics of vulnerability disclosure and information and communication technology (ICT) security certification opportunities in the healthcare sector.

ENISA continued to strongly support the process of assisting EU Member States in implementing the NISD, the first piece of EU-wide legislation on cybersecurity that provides legal measures to boost the overall level of cybersecurity in the EU.

ENISA supported the organisation of the CSIRTs network meetings in Greece, Bulgaria and Austria that saw the participation of CSIRT representatives from

all Member States, the European Commission and the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU).

Following on from last year's tradition, ENISA organised several high-profile events such as the fifth Network and Information Security Summer School 2018 and a conference preparing for the EU cybersecurity certification framework. Other events included the ENISA industry event and the Annual Privacy Forum. ENISA also hosted a number of important thematic workshops and sessions, gathering together experts in the field to discuss cybersecurity topics.

Two major European projects were also supported by ENISA: the European Cyber Security Month (ECSM) a specific month dedicated to activities on cybersecurity and privacy awareness, and the European Cyber Security Challenge (ECSC) event (a competition based on a series of technical challenges between teams of students and school pupils from different Member States). The final stage of the ECSC 2018 took place in London. More than 200 people representing 17 countries competed at this year's final.

The pan-European cybersecurity exercise, Cyber Europe 2018, was successfully organised and executed. Focusing on the aviation sector, it involved close to 1 000 cybersecurity professionals from 30 EU and European Free Trade Association (EFTA) countries and over 300 organisations. In addition, ENISA participated in the 2018 European Union Hybrid Exercise, a multilayer exercise testing EU crisis management mechanisms against hybrid threats, including cyberthreats.

During 2018, the NISD was effectively implemented across the EU. Throughout the year, ENISA supported and contributed to the work of the Cooperation Group and was instrumental in developing the CSIRTs network. In the context of the Cooperation Group, the agency supported notably the good practices on interdependencies between OES and DSP information security audit frameworks for OESs and incident reporting under the NISD.

ENISA issued a number of 'cybersecurity info notes' analysing various incidents over the year. These information notes provided an overview of significant incidents by establishing the context to the materialised cyberthreats, thus complementing the *ENISA threat landscape report 2018*. During 2018, ENISA worked on a capability maturity framework for cyberthreat intelligence, which will help its users to understand their requirements and take informed decisions on the desired maturity level.

Finally, the year ended with political agreement on the Cybersecurity Act, which establishes a permanent mandate for the agency and significantly expands the scope of its activities.

While not being exhaustive, these achievements amply illustrate the variety of ways in which the agency contributes to a stronger and more secure EU.

ACHIEVEMENT OF STRATEGIC PRIORITIES AND OBJECTIVES

In 2018, the agency delivered against its annual work programme, and all outputs and deliverables met or exceeded the key performance indicators set (see Part I for more details). Notable achievements are mentioned hereunder, along with examples of how the agency reached its goals.

ENISA continued to deliver on the priorities of its strategy, including work in areas supporting the digital single market (and on specific technologies such as the IoT), finance, privacy and trust. ENISA further contributed to the implementation of the NISD concerning baseline security measures for OES sectors and DSP, as well as supporting the implementation of the second payment services directive (PSD2). The agency also supported the Member States and the European Commission in the NISD transposition.

Key achievements include the following.

- In the context of the NISD, the agency built on the work from previous years and produced a number of deliverables supporting the respective working streams established within the Cooperation Group, including incident notification, baseline security measures, the identification of OES (see performance indicator for outputs O.2.2.2 and O.2.2.6) and eElection security.
- In supporting the implementation of the NISD, ENISA strengthened its engagement with stakeholders in specific OES sectors (e.g. air transport, finance and healthcare) to better understand and document examples of sectorial specificities vis-à-vis the sectorial requirements. Relevant input was provided to the Cooperation Group (horizontal and sectorial standards) to enhance its specific knowledge of these sectors (see performance indicator for output O.2.2.6).
- For the second time ENISA, together with the National Security Authority of Slovakia, organised a conference on critical information infrastructure

protection with the aim to bring together the needs of security professionals, public authorities, and the relevant industries for a constructive dialogue. More than 100 experts from private as well public sectors participated.

- As part of its activities to develop good practices and recommendations for IoT security, ENISA organised together with the European Union Agency for Law Enforcement Cooperation (Europol) the second IoT security conference that was attended by over 350 participants and achieved significant visibility in the community. Additionally, more than 40 IoT stakeholders and experts were involved in the relevant study, including the ENISA IoT Security and Industry 4.0 Cyber Security Experts Groups and the European Commission's Joint Research Centre (see performance indicator for output O.1.1.1).

- Supporting the finance sector ENISA has developed good practices for implementation of the PSD2. For this study, more than 15 Member States as well as more than 10 private financial institutions were engaged in providing feedback. ENISA organised the Financial Institutes - Information Sharing and Analysis Centre (FI-ISAC) meeting in Athens, where more than 35 participants discussed the latest developments in cyber-related issues in the sector.

- ENISA supported the Member States in the development and assessment of national cybersecurity strategies (NCSSs) by developing an evaluation tool and by further updating the ENISA NCSS map. ENISA, building on previous years' work, assisted the Member States in deploying existing good practices in related areas and offering targeted and focused assistance with specific NCSS objectives. The evaluation tool was created with the aim of helping Member States evaluate their NCSSs in an easy, quick and user-friendly manner. Its objective was to help Member States create second or third versions of their NCSSs by evaluating their strategic objectives. The tool functions by providing questions on specific key performance indicators for each strategic objective and then generating advice and ideas for improving cybersecurity at a national level. More than 20 Member States participated in ENISA's activities regarding this output (see performance indicator for output O.3.1.2).

- In 2018, the CSIRTs network reviewed, updated and adopted its mid-term work programme objectives and key performance indicators, the terms of reference and rules of procedures, and formally handed its first report to the Cooperation Group.

- ENISA supported the operational readiness of the CSIRTs network through well-established and secure tools and communication.

- The ENISA inventory of incident response teams listed 383 teams in December 2018 against 342 the end of the previous year. This steady increase in the number of teams clearly indicates a growth in incident response capabilities across Europe.

- The 2018 edition of the Cyber Europe exercise was the largest and most complex of its kind. Cyber Europe 2018 was very successful, proving once again the vast experience of ENISA in organising operational as well as tabletop exercises. This is also manifested in the numerous requests that ENISA receives from both EU bodies and national authorities to provide its support in the organisation and conducting of exercises.

- The ECSC held in London in October 2018 as part of the ECSM was a major success. In less than 5 years ECSC has been transformed from a competition between five countries into a well-defined international event with the participation of teams from 17 countries. ENISA plays a key role, being responsible for the competition's governance model as well as gameplay, content, etc.

- ENISA supported the European incident response community in building a common language and terminology for exchanging information in the event of incidents, attacks or disruptions. The Reference Security Incident Taxonomy Working Group was formally recognised as a working group under the Task Force on Security Incident Response Teams (TF-CSIRT) — the European CSIRT community — and the first version of the taxonomy was released on GitHub.

- The agency continued supporting the Commission and the Member States towards the establishment of an EU cybersecurity certification framework for products, services and processes. While closely following the legislative process of the Cybersecurity Act proposal, ENISA undertook a study, in support of the Commission and EU Member States that are participating in the Senior Officials Group Information Systems Security Mutual Recognition Agreement (SOG-IS MRA), exploring aspects of a possible transposition of the existing SOG-IS MRA to the new EU framework.

- ENISA contributed asset models and a threat and risk assessment to the network and information system Cooperation Group (NIS CG) *Compendium on cybersecurity of election technology* (CG Publication 03/2018), which later became part of the Commission's recommendation to Member States on the security and fairness of the upcoming European Parliament elections.

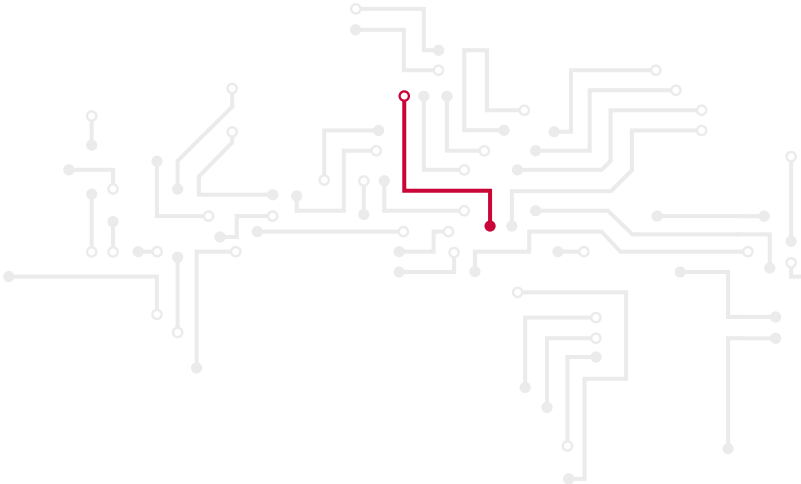
KEY CONCLUSIONS ON FINANCIAL MANAGEMENT AND INTERNAL CONTROL

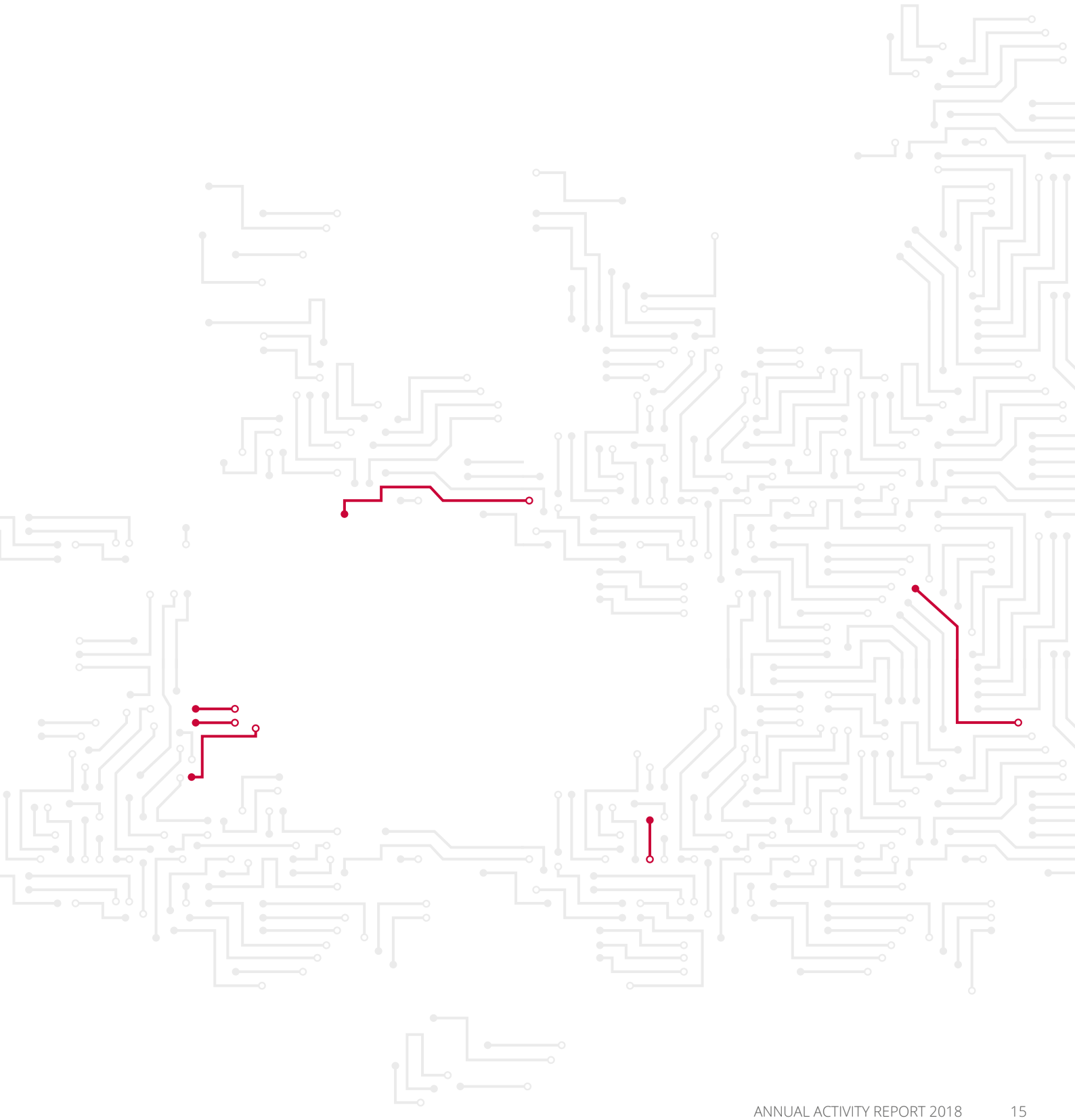
ENISA's staff conducted its 2018 activities in compliance with the applicable legal and financial framework, working in an open and transparent manner and meeting the expected high level of professional and ethical standards.

ENISA has adopted a set of internal control principles, based on international best practices, aimed to ensure the achievement of policy and operational objectives. The financial regulation requires that the organisational structure and the internal control systems used for the implementation of the budget are set up in accordance with these principles. ENISA has assessed the internal control systems during the reporting year and has concluded that the internal control principles are implemented and function as intended.

In addition, ENISA has systematically examined the available control results and indicators as well as the observations and recommendations issued by the Internal Audit Service (IAS) of the European Commission and the European Court of Auditors (ECA). These elements have been assessed to determine their impact on the management team's assurance as regards the achievement of control objectives.

In conclusion, management has reasonable assurance that, overall, suitable controls are in place and working as intended; risks are being appropriately monitored and mitigated; and necessary improvements and reinforcements are being implemented.





PART I

ACHIEVEMENTS IN THE IMPLEMENTATION OF THE 2018 WORK PROGRAMME

This *Annual activity report 2018* follows the structure of the 2018 ENISA work programme to assist the reader in understanding the achievements of the year. The 2018 work programme was aligned with the structure of the ENISA strategy document [1], which was created with the aim of supporting ENISA's executive director and Management Board in the production and adoption of consistent multiannual and annual work programmes [2]. This strategy defines five strategic objectives that form the basis of future multiannual plans [3].

These strategic objectives are derived from the ENISA regulation, along with inputs from the Member States and relevant communities, including the private sector. They state that ENISA, in cooperation with and in support of the Member States and the EU institutions, will carry out the following tasks.

#Expertise: **anticipate and support Europe in facing emerging network and information security challenges,** by collating, analysing and making available information and expertise on key NIS issues potentially impacting the EU taking into account the evolutions of the digital environment.

#Policy: **promote network and information security as an EU policy priority,** by assisting the EU institutions and Member States in developing and implementing EU policies and law related to NIS.

#Capacity: **support Europe in maintaining state-of-the-art network and information security capacities,** by assisting the EU institutions and Member States in reinforcing their NIS capacities.

#Community: **foster the emerging European network and information security community,** by reinforcing cooperation at EU level among EU institutions, Member States and relevant NIS stakeholders, including the private sector.

#Enabling: **reinforce ENISA's impact,** by improving the management of its resources and engaging more efficiently with its stakeholders, including the EU institutions and Member States, as well as at international level.

In the following sections the results of the implementation of the 2018 work programme are presented for each of the abovementioned activities. After the description of the specific results for each activity and output, the achievements are presented in tables against indicators and the detailed results for each output.

1 *ENISA strategy 2018-2020,* available at: https://www.enisa.europa.eu/publications/corporate/enisa-strategy

2 In accordance with Article 13 of Regulation (EU) No 526/2013 of the European Parliament and of the Council concerning ENISA.

3 In order to achieve the multiannual strategic objectives laid out in this document, the multiannual work programme provides prioritised mid-term operational objectives to be achieved by ENISA within a period of 3 years. Specific annual activities (outputs) are identified in the annual work programme, using a recursive approach in order to achieve the mid-term operational objectives and, in the long term, the strategic objectives.

1.1 KEY RESULTS IN THE IMPLEMENTATION OF ACTIVITY 1 — EXPERTISE: ANTICIPATE AND SUPPORT EUROPE IN FACING EMERGING NETWORK AND INFORMATION SECURITY CHALLENGES

1.1.1 Objective 1.1. Improving the expertise related to network and information security

1.1.1.1 Output O.1.1.1. Good practices for security of the internet of things (priority 1)

IoT is at the core of operations for many essential service operators as defined in the NISD, especially considering recent initiatives concerning smart infrastructure, Industry 4.0 [4], 5G [5], smart grids [6], etc. IoT security should thus be considered in this context [7].

The agency identified and analysed existing security practices and standards in the area of IoT security for critical infrastructure and smart infrastructure, taking into consideration existing national expertise and practices. ENISA compared these practices and standards and developed good practices for IoT security, with a particular focus on the impact on end users.

In this endeavour the agency took into account existing EU policy and regulatory initiatives (the NISD, the communication 'Internet of things — An action plan for Europe', the Alliance for Internet of Things Innovation (AIOTI) [8] and the 5G Infrastructure Public–Private Partnership [9]).

The agency developed targeted IoT case studies to identify risks and vulnerabilities, by defining appropriate attack scenarios, and provided relevant recommendations and good practices. Moreover, it defined IoT security requirements to ensure 'security for safety'.

The agency also validated the results of the study (e.g. via joint workshops) with relevant national and EU initiatives (e.g. the Alliance for Internet of Things Innovation) and interacted with all important IoT stakeholders from the public sector, such as the Directorate-General for Communications Networks, Content and Technology and the Joint Research Centre and, and from the private sector, including critical information infrastructure providers, integrators and manufacturers.

This work built on the previous work of ENISA in the areas of IoT, intelligent cars, smart cities, smart hospitals and smart airports (2015-2016 work programme).

1.1.2 Objective 1.2. Network and information security threat landscape and analysis

1.1.2.1 Output O.1.2.1. Annual European Union Agency for Network and Information Security threat landscape (priority 1)

The *ENISA Threat Landscape report 2018* provides an overview of the top 15 cyberthreats identified throughout the year. It includes both tactical and strategic information about each cyberthreat, including points of interest, trends, involved threat agents, attack vectors and mitigation controls.

The report is produced based on information collection of open source material, such as annual incident reports, consolidated threat reports of vendors, articles, blogs, etc. Based on this information, an analysis and consolidation effort is being performed. It results to an extensive description of each cyberthreat. ENISA shared the references of all relevant material collected throughout the year. Interested stakeholders may use this information to find technical details related to each assessed cyberthreat.

The visualisation and quick availability of threat information was set as priority in 2018. For this reason, the ENISA threat landscape (ETL) has been made available by means of an end user (web-based) application that provides the entire ETL information online (https://etl.enisa.europa.eu). In this manner, ETL users are in a position to selectively access ENISA threat information in an efficient manner.

In 2018, ENISA continued its cooperation efforts with CERT-EU in the area of threat landscaping. This was carried out through information exchanges, use of CERT-EU services and organisation of

4 See https://ec.europa.eu/digital-single-market/en/fourth-industrial-revolution

5 See https://ec.europa.eu/digital-single-market/en/towards-5g

6 See https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters

7 Nevertheless, non-critical operators, who might also be involved in IoT activities, face no regulation and may have little incentive to invest in securing their systems. Considering the particularities of IoT, security should be seen as a primary concern even for the latter operators.

8 More information on the Alliance for Internet of Things Innovation is available at: https://ec.europa.eu/digital-single-market/en/alliance-internet-things-innovation-aioti

9 More information on the 5G Infrastructure Pubic–Private Partnership (5G PPP) is available at: https://5g-ppp.eu/

common meetings and events. By carrying out this work, synergies with related experts (i.e. the ETL Stakeholder Group) and vendors (through memorandums of understanding) were maintained and expanded.

1.1.2.2 Output O.1.2.2. Restricted and public info notes on network and information security (priority 1)

ENISA provides guidance on important NIS events and developments through info notes. The general info notes produced in 2018 covered significant developments, events and announcements in the field of cybersecurity. ENISA provided balanced and neutral information regarding events, issues, points of action, mitigation measures, summaries, related practices, etc. Hence, the objective of this work was to provide regular updates containing a neutral overview of the state of play regarding an incident.

1.1.2.3 Output O.1.2.3. Support incident reporting activities in the European Union

For the seventh year, ENISA published its annual report on significant security incidents in the European electronic communications sector, which are reported to ENISA and the European Commission under Article 13a of the framework directive (Directive 2009/140/EC) by the national regulatory authority (NRA) of each of the 28 EU Member States and two EFTA countries.

The report published in 2018 covers the incidents that occurred in 2017 and gives an aggregate analysis of the incident reports about severe outages across the EU. Some key findings from the 169 major incidents reported include the fact that mobile telephony and mobile internet are most affected; system failures is the dominant root cause; and outages caused by natural phenomena increased from 5% in previous years to almost 20%, with extreme weather appearing to be the primary cause.

ENISA supports a group of experts from the NRA, called the ENISA Article 13a Expert Group. ENISA organised three Article 13a meetings during the year, which were attended by most of the EU NRAs – typically 20-25 countries attend. The agency also develops and maintains an online incident-reporting tool for the NRAs to facilitate annual summary reporting about incidents.

Under Article 19 of the eIDAS regulation [10], every year ENISA publishes an aggregate overview of the incidents reported to national supervisory bodies under Article 19 of the eIDAS regulation, and subsequently to ENISA as part of annual summary reporting. The *Annual report trust services security incidents 2018* therefore marks the second full year of annual reporting about significant security incidents in the EU's trust services sector.

10 Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

In order to facilitate the process of incident notifications, ENISA manages an expert group on the matter called the 'ENISA Article 19 Expert Group' and composed of the supervisory authorities from a number of Member States. The group meets twice a year to debate incidents and incident reporting, along with other topics.

ENISA also kicked off the work on incident reporting under the NISD, which came into force in 2018. ENISA developed, in close collaboration with the NIS CG, two guidelines for NISD incident reporting, one each for OESs and DSPs. ENISA also developed templates used by the Member States in the first round of annual summary reporting about significant incidents, to the NIS CG.

1.1.3 Objective 1.3. Research and development, innovation

1.1.3.1 Output O.1.3.1. Guidelines for European standardisation in the field of information and communications technology security (priority 1)

This activity provided a preliminary analysis of the IoT-related landscape of standards aiming at pinpointing potential areas of improvement in securing the IoT. Elements of a holistic approach towards IoT security can be found in a series of standards; however, further work is needed to achieve an overarching approach that protects the entire IoT ecosystem. In parallel, ENISA elaborated further on the thematic area of privacy-oriented standards, considering the developments at legislative, policy and standardisation level. Through a respective study, the agency explored how the standards-developing world is responding to the fast-changing, demanding realm of privacy by mapping existing available standards and initiatives in the area and provided insights into the 'state-of-the-art' of privacy standards in the information security context through a relevant gap analysis.

In carrying out this work, ENISA consulted with representatives from academia, industry and standards organisations (e.g. the European Telecommunications Standards Institute (ETSI), the European Committee for Standardization, the European Committee for Electrotechnical Standardization) while also co-organising a well-attended conference and actively participating in renowned standardisation conferences (e.g. ETSI Security Week).

1.1.3.2 Output O.1.3.2 Priorities for European Union research and development (priority 1)

Based on desk research and interviews with more than 20 experts from academia, government and private sectors, ENISA depicted the threats to European society and the societal changes brought by innovation in the digitally connected world. This work was summarised in the report *'Analysis of the European R & D priorities in cybersecurity'* and was also presented at the Research Working Group annual meeting of the European Cyber Security Organisation in order to support their work.

In addition, ENISA published a specific report on the economics of vulnerability disclosure, which highlighted the economic factors, incentives and motivations that influence the behaviour of all those involved in vulnerability disclosure, as well as two case studies of recently disclosed high-profile vulnerabilities.

During 2018, the agency offered support to the National Public Authority Representatives Committee by providing a secretariat function.

Moreover, ENISA participated in dissemination meetings of some European Research funded cybersecurity projects in order to identify the further research efforts needed for making Europe "a global leader in cybersecurity by 2025", as stated at the Tallinn Digital Summit in September 2017.

1.1.4 Objective 1.4. Response to Article 14 requests under expertise activity

1.1.4.1 Output O.1.4.1 — Response to requests under expertise activity (priority 1)

The national research institute of Poland requested ENISA's support in setting up their certification framework, in line with the projected European one. For this purpose, a workshop in Warsaw was held, where representatives of all Polish stakeholders in the area of certification were present. The workshop provided for opportunity to discuss all burning issues and laid the foundations for potential future collaboration in this area.

1.1.5 Type of outputs and performance indicators for each outputs of Activity 1 — expertise

Summary of outputs in Activity 1 — expertise: anticipate and support Europe in facing emerging network and information security challenges		
Outputs	**Performance indicator**	**Achieved result**
Objective 1.1. Improving the expertise related to network and information security		
Output O.1.1.1. Good practices for security of the internet of things	Engage 5 leading IoT developers Engage 5 leading stakeholders from 5 EU Member States	37 leading IoT developers engaged in the development of the study. 42 leading IoT stakeholders engaged in the development of the study from 10 Member States and 1 EEA state.
Objective 1.2. NIS threat landscape and analysis		
Output O.1.2.1. Annual ENISA threat landscape	Engage more than 10 Member States in discussions and work related to implementing NISD incident reporting.	An Expert Group, representing more than 10 Member States, was involved in the development and revision of the 2018 ETL report. Furthermore, ENISA organised a workshop (CTI-EU) with 120 participants, from multiple Member States, to validate the threat intelligence collected. The 2018 ETL report includes information about incidents that were relevant to the NISD incident reporting process.
Output O.1.2.2. Restricted and public info notes on NIS	Coverage of all major incidents relevant to EU NIS policy priorities. Expand coverage to all key ENISA stakeholder groups.	13 info notes produced in 2018 covered major cybersecurity incidents, relevant to all ENISA stakeholder groups.
Output O.1.2.3, Support incident reporting activities in EU	More than 20 NRAs/EU Member States contribute to preparation of the report (Article 13a) 3 workshops per year (Article 13a) More than 10 supervisory bodies/ EU Member States contribute to preparation of the report (Article 19) 2 workshops per year (Article 19) Engage more than 10 Member States in discussions and work related to implementing NISD incident reporting	28 NRAs from EU Member States and 2 EFTA countries contributed incident reports, reviewed a draft report and agreed to its publication. ENISA organised three Article 13a workshops. 28 NRAs from EU Member States and 2 EFTA countries contributed incident reports, reviewed a draft report and agreed to its publication. ENISA organized two Article 19 workshops. The incident reporting guidelines were developed in an NIS CG work streams, and reviewed and adopted by 28 Member States in the NIS CG.
Objective 1.3. Research and development, innovation		
Output O.1.3.1. Guidelines for European standardisation in the field of ICT security	Participation in drafting and review of the guidelines of at least 5 representatives of European standard developing organisations (SDOs) and relevant services of the European Commission	6 representatives of European standard developing organisations participated in drafting and reviewing the guidelines.
Output O.1.3.2. Priorities for EU research and development	Involve at least 5 representatives from different stakeholders — research, industry, governmental	More than 20 experts from academia, public and private sectors provided their inputs for identifying the European research and development priorities in cybersecurity.
Objective 1.4. Response to Article 14 requests under expertise activity		
Output O.1.4.1. Response to requests under expertise activity	Answers to requests.	Answer provided. See https://www.enisa.europa.eu/publications/enisa-article-14-requests-2018

1.1.6 Specific results: mapping of outputs into papers, publications or activities

Activity 1 — expertise: anticipate and support Europe in facing emerging network and information security challenges
Objective 1.1. Improving the expertise related to critical information infrastructures
Output O.1.1.1. Good practices for security of the internet of things ***Good practices for security of internet of things in the context of smart manufacturing*** https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot
Objective 1.2. NIS threat landscape and analysis
Output O.1.2.1 Annual ENISA threat landscape ***ENISA threat landscape report 2018*** https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/
Output O.1.2.2 Restricted and public info notes on NIS ***ENISA cybersecurity info notes*** https://www.enisa.europa.eu/publications/info-notes
Output O.1.2.3. Annual incident analysis report for trust service providers (Article 19) ***Annual Report Trust Services Security Incidents 2017*** https://www.enisa.europa.eu/publications/annual-report-trust-services-security-incidents-2017 Output O.1.2.3. Annual incident analysis report for the telecom sector (Article 13a) ***Annual report Telecom security incidents 2017*** https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2017 Output O.1.2.3. Incident reporting framework for NISD ***Guideline on notification of operators of essential services incidents*** http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53677 ***Guidelines on notification of digital service providers incidents*** http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53675
Objective 1.3. Research and development, innovation
Output O.1.3.1. Guidelines for European standardisation in the field of ICT security ***IoT security standards gap analysis*** https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis/ ***Guidance and gaps analysis for European standardisation-Privacy standards in the information security context*** https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation/
Output O.1.3.2. Priorities for EU Research & Development ***Economics of vulnerability disclosure*** https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure ***Analysis of the European R&D priorities in cybersecurity*** https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity
Objective 1.4. Response to Article 14 requests under expertise activity
Output O.1.4.1. Response to requests under expertise activity ***ENISA Article 14 requests: report on 2017 requests*** https://www.enisa.europa.eu/publications/enisa-article-14-requests

1.2 KEY RESULTS IN THE IMPLEMENTATION OF ACTIVITY 2 — POLICY: PROMOTE NETWORK AND INFORMATION SECURITY AS A EUROPEAN UNION POLICY PRIORITY

1.2.1 Objective 2.1. Supporting European Union policy development

ENISA provided high-quality information, data and advice to support policymaking in the Commission and Member States.

In the area of policy development the agency collaborated with public- and private-sector stakeholders to develop insights, reach consensuses and provide recommendations in areas that further develop its policy. Examples of such cooperation took place in the domains of information technology (IT) security certification and the digital single market.

1.2.1.1 Output O.2.1.1 Support the policy discussions in the area of certification of products and services (priority 1)

As a first step towards sketching a point of reference for policy-makers tackling the issue of cybersecurity and establishing a relevant framework for policy development, a study was produced to provide an overview of representative application domains of autonomous agents to complement relevant initiatives at EU level by providing insights and considerations, relating to both security and privacy.

The agency continued supporting the Commission and the Member States towards the creation of an EU cybersecurity certification framework for products, services and processes. While closely following the legislative process of the Cybersecurity Act proposal, ENISA undertook a study, in support of the Commission and EU Member States that are participating in SOG-IS MRA, exploring aspects of a possible transposition of the existing SOG-IS MRA to the new EU framework. In parallel, emerging application areas such as the healthcare sector were analysed with a view to identifying and providing a preliminary mapping of the aspects to be considered.

ENISA continued to stimulate dialogue with standards developing organisations (ETSI, etc.), ICT certification stakeholders (test labs, certification and accreditation bodies, SOG-IS, the Common Criteria Recognition Arrangement, etc.) and ICT security products through the organisation of two conferences on the broad thematic area of cybersecurity certification framework.

1.2.1.2 Output O.2.1.2 Towards a framework for policy development in cybersecurity (priority 1)

ENISA focused on providing an overview of representative application domains of autonomous agents and attempts to complement relevant initiatives at EU level by providing insights and considerations relating to both security and privacy. In parallel to this activity, the agency also touched upon privacy enhancing technologies (PETs) and explored the notion of an online platform where emerging technologies could be maintained and evaluated. Lastly, a workshop with a specific focus on the research and academic community was conducted, in order to explore the further evolution of this platform in the context of privacy and security.

1.2.2 Objective 2.2. Supporting European Union policy implementation

1.2.2.1 Output O.2.2.1 Recommendations supporting implementation of the eIDAS regulation (priority 1)

ENISA supported public and private bodies in implementing the eIDAS regulation by addressing technological aspects and building blocks for trust services.

Specifically, ENISA developed a report on the global acceptance of eIDAS audits, continued its work on the assessment of eIDAS-related standards in order to assist the European Commission in updating the related implementing acts and organised the fourth edition of the Trust Services Forum. These were directed at all the stakeholders involved: trust service providers, supervisory bodies and conformity assessment bodies. More than 20 experts in the area of trust services were involved in preparing and validating the reports. The reports were disseminated through different communication channels, including the European Commission's distribution channels, the Article 19 ENISA Expert Group mailing list and ENISA contacts from the Trust Services Forum. The findings of the reports were presented in several different workshops and conferences, including the Trust Services Forum, the Article 19 ENISA Expert Group, ETSI Security Week, World e-ID and the trust services providers compliance info day on eIDAS, ETSI and Certification Authority Browser Forum requirements.

Moreover, the fourth edition of the Trust Services Forum received a high number of registrations and was attended by over 130 participants that actively contributed in the discussions and the panels.

1.2.2.2 Supporting the implementation of the network and information systems directive (priority 1)

ENISA is an active member of the NIS CG, the official group for strategic collaboration and providing guidance to Member States on the implementation of the NISD.

ENISA supported, together with the Cooperation Group, the development of a guideline and templates for the implementation of Article 5(4), for Member States to use when identifying OESs, notifying the Commission about their identification of OESs, and in notification of cross-border dependencies.

ENISA supported the development of templates and tools for incident notification by taking stock

of incident notification templates and notification methods in use across the EU, showing the different approaches, commonalities and divergences. This analysis has been circulated inside the NIS CG but has not been published because in 2018 the situation was uncertain as many Member States had not yet transposed the NISD.

ENISA published a report on good practices regarding interdependencies between OESs and DSPs with a view to supporting OESs in their risk assessments. In relation to the latter, an important element of the risk to be assessed is the dependencies of the services offered on other services of either OES or DSPs. These dependencies might be national or cross-border in nature. The report proposes a four-phase interdependency identification and assessment approach to the OESs, DSPs and national competent authorities (NCAs) as well as a set of recommendations to effectively address interdependencies in their risk assessments. The agency has involved the NIS CG as well as 19 stakeholders from the OES community to take stock of the existing practices. The report has been validated in a workshop, which took place in Bratislava with more than 100 attendees representing both the private and the public sectors.

ENISA is actively supporting the NIS CG and plays a key role in all the NIS CG work streams, by drafting guidelines and contributing to Member State initiatives. For instance, ENISA contributed asset models and a threat and risk assessment to the NIS CG *Compendium on cybersecurity of election technology* (CG Publication 03/2018), which later became part of the Commission recommendation to Member States about security and fairness of the upcoming European Parliament elections. This compendium is a broad set of guidelines that are based on the experiences and best practices across the Member States, and contains practical and workable measures that can be taken by cyber security organisations and election management bodies as well as those advising or overseeing them to secure the technology involved in elections.

ENISA also organised two NISD related workshops. ENISA co-organised, jointly with NSU Slovakia a cybersecurity workshop involving both OESs and sectorial authorities on critical information infrastructure protection (CIIP) and the NISD.

ENISA also organised the fourth eHealth Security conference in cooperation with the Dutch Ministry of Health, Welfare and Sport. The conference was hosted by the Erasmus University Medical Center Rotterdam.

1.2.2.3 Output O.2.2.3. Baseline security recommendations for the operator of essential services sectors and digital service providers (priority 1)

ENISA, building on its expertise in security requirements developed for DSPs and OESs, worked closely with Member States and the private sector to identify effective practices and security maturity frameworks that would constitute the basis for guidelines for Member States to assess the compliance of DSPs and OESs with security requirements set by the NISD. In this light, ENISA published a report with guidelines on the use of information security audit and self-assessment frameworks. On the whole, this report aims to provide guidance to the NCAs in auditing in line with the security requirements of the NISD. The report presents a complete set of options for NCAs to meet these provisions. The agency worked in close collaboration with the NIS CG and with experts from the private sector to develop this report.

1.2.2.4 Output O.2.2.4 Supporting the payment services directive implementation (priority 1)

The main goal of the PSD2 is to promote competition and innovation in financial services and to protect the security of payment services users. The PSD2 focuses on the use of technology in financial services, introducing new technological requirements and measures to guarantee the confidentiality, integrity, availability, and authenticity of user information. The main objective of this study is to identify the good practices introduced by Member States in the implementation of the PSD2. In particular, the aim is to analyse the adaptation of the PSD2 guidelines in the field of security, such as measures for operational and security risks, and the notification of major incidents. The study also provides a parallel between the incident reporting mechanism and the NISD incident notifications. Additionally, the security measures identified in the PSD2 are mapped to the security measures identified in the NISD.

1.2.2.5 Output O.2.2.5. Contribute to European Union policy in the area of privacy and data protection (priority 2)

Technical measures in the field of data protection have been a key part of the involvement of ENISA in this policy area in an effort to support the implementation of the General Data Protection Regulation (GDPR). In particular, in 2018 the agency, on the basis of previous relevant work, elaborated on the state-of-the-art with regard to security measures for the protection of personal data (in correlation

with Article 32 GDPR). Moreover, the agency provided two sets of guidelines related to the technical implementation of GDPR in the areas of data pseudonymisation and the notion of data protection by default. In this sixth edition, the Annual Privacy Forum was used to bring together key communities across research, policy and industry to disseminate work in this area. Cooperation activities with the European Data Protection Supervisor (EDPS) and national data protection authorities were continued and further enhanced. In this context, two workshops were also organised in the field of security measures and data protection by design, in collaboration with the data protection authorities of Italy and Greece.

1.2.2.6 Output O.2.2.6. Network and information systems directive transposition (priority 1)

The European Commission developed an online map to display the NISD transposition status in the Member States. In order to avoid duplication of efforts, ENISA NISD tool does not display the NISD transposition status but it facilitates the concept of a 'one-stop shop' for the NISD.

Through this tool, ENISA is supporting the Member States and the private sector by providing information about the Member States' relevant laws, their adopted NCSSs and the appointed NCAs for both OESs and DSPs.

The NISD tool is an interactive online tool and its functionality includes:

- links to the relevant national laws and regulations in each Member State, as well links to documents explaining OES identification, security measures and incident notification requirements, etc.;
- links to ENISA's relevant sectorial work or sub sectorial work;
- lists of the relevant NCAs for each sector (both for OESs and DSPs);
- hyperlinks to the webpages of these competent authorities.

In addition, the tool also links to the ENISA NCSS map, the European Commission's NISD map, and ENISA's CSIRTs network web page.

Moreover, for this output ENISA organised the first Transport Cybersecurity Conference in cooperation with the European Commission (Directorate-General for Mobility and Transport), the European Aviation Safety Agency, the European Union Agency for Railways and the European Maritime Safety Agency. This conference, which took place at the premises of the European Maritime Safety Agency, brought together public bodies and stakeholders from all transport modes to look at the European regulatory environment (NISD, Cybersecurity Act), its relevance for the sector including in light of past incidents, and to explore synergies among transport modes.

In addition, ENISA wrote technical guidelines on the implementation of Article 5(7) together with the Commission. The objective of the document is to provide the Member States with non-binding technical guidelines on how to implement Article 5(7) with a view to:

a) avoiding unnecessary divergence or inconsistencies when submitting information to the Commission;

b) simplifying the submission process; and

c) maximising the value of the information received by the Commission as a means of the directive implementation assessment.

1.2.3 Objective 2.3. Response to Article 14 requests under policy activity

1.2.3.1 Output O.2.3.1. Response to requests under policy activity (priority 1)

The 2018 outcomes of the Article 14 requests under policy activity are as follows.

- In 2017, ENISA received a request from the Commission's Directorate-General for Health and Food Safety to support the eHealth Network's activities on cybersecurity for healthcare, which are carried out within the joint action on eHealth (health programme 2017). In 2018, ENISA actively participated in Task 7.3, 'Data and system security', of work package 7, which addresses the issues on 'Implementation challenges and impact'.

- ENISA received a request from the Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs to support the implementation of the IT security requirements introduced by the two new regulations on medical devices, 2017/745 (medical device regulation) and 2017/746. In 2018, ENISA provided expertise to the medical device regulation Cybersecurity Task Force established by the Commission and is supporting the Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs with respect to the technical coordination of the project.

- The Cooperation Group on cross-border dependencies aims to establish voluntary guidelines or recommendations that would help

Member States and their competent authorities to assess and mitigate the cross-border dependencies affecting their essential services. ENISA provided a stocktake of the political and regulatory frameworks of the EU relevant for this work stream.

- ENISA received a request from the Directorate-General for Energy to create a sector-specific subgroup of the NIS CG, to establish a cybersecurity guidance document for the energy sector (tackling its specificities) and to provide more formal support for the European Energy Information Sharing and Analysis Centre (EE ISAC).
- The National Cyber Security Authority of Greece requested support for national operators of essential services to raise their security awareness and guide them through the adoption of best practices in the NIS area.
- The European Union Agency for Railways requested support in NISD implementation for the rail sector, especially support in the development of a sectorial information sharing and analysis centre (ISAC) for infrastructure managers and railway undertakings, as well as capacity building (organising training and awareness-raising sessions).
- The Austrian Presidency requested support on creating an institutional map on cybersecurity capabilities in Member States.
- Austria requested help in drafting a reference document on approaches in identifying OESs in different Member States.
- The Bulgarian Presidency requested support in the preparation of a reference document on a common taxonomy for large scale incidents and crise that will include the preparation of a template for situational reports describing the technical causes and impacts of cybersecurity incidents.
- The National Cyber Security Authority of Greece requested the help of ENISA in support of identifying good practices for the identification of OESs.
- The European Central Bank requested support in developing the EUROSystem red team testing framework.
- The European Union Aviation Safety Agency requested support in developing the objectives of the European Centre for Cybersecurity in Aviation, in raising cybersecurity awareness and in the sectorial implementation of the NISD.
- A request was received from Poland on NISD implementation, specifically concerning OESs including examples of the approach to the essential services definitions (with thresholds) and identification of OESs, sectorial criteria and thresholds for the incidents having significant disruptive effect.
- ENISA received a request from Cyprus and delivered direct support to the Cypriot national CSIRT by providing tailored technical training in the areas of incident management, malware analysis and memory forensics.

1.2.4 General results: achievement of performance indicators for Activity 2

Summary of outputs in Activity 2 — policy: promote network and information security as an EU policy priority

Outputs	Performance indicator	Achieved results
Objective 2.1. Supporting EU policy development		
Output O.2.1.1. Support the policy discussions in the area of certification of products and services	More than 10 private companies and 10 EU Member State representatives contribute to or participate in the activity	15 private companies and 18 EU Member State representatives participated in the activity.
Output O.2.1.2. Towards a framework for policy development in cybersecurity	More than 10 private companies and 10 EU Member State representatives contribute to orparticipate in the activity	11 private companies and 10 Member State representatives participated in the activity

Summary of outputs in Activity 2 — policy: promote network and information security as an EU policy priority		
Outputs	**Performance indicator**	**Achieved results**
Objective 2.2. Supporting EU policy implementation		
Output O.2.2.1. Recommendations for technical implementation of the eIDAS regulation	Engaging at least 5 representatives from different bodies/Member State 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 State. More than 50 stakeholders participate in the activity	7 representatives from different bodies and Member States were engaged in the preparation and validation of the recommendations. 20 stakeholders from eight Member States have reviewed and validated the recommendations. 130 stakeholders attended the Trust Services Forum and 175 were registered expressing interest in ENISA work on eIDAS
Output O.2.2.3. Baseline security recommendations for the OES sectors and DSPs	Engage 20 Member States in the development of good practices for OES and DSPs Engage 15 private sector companies in the development of good practices for OESs and DSPs More than 10 Member States and 15 OESs participate in the workshops.	27 representatives from different bodies and Member States were engaged in the preparation and validation of the recommendations. 26 private stakeholders from 10 Member States have reviewed and validated the recommendations. Over 60 OESs from 24 Member States have participated in two ENISA workshops.
Output O.2.2.4. Supporting the payment services directive (PSD) implementation	Engaging at least 15 Member State regulatory bodies and at least 10 private financial institutions in this study.	Engaged 19 Member States and 12 private institutions.
Output O.2.2.5. Contribute to EU policy in the area of privacy and data protection	Engage more than 40 participants from relevant communities, including providers, data controllers and national bodies in the activity. At least 5 representatives from different bodies/Member States participate in the preparation of the recommendations. At least 5 representatives from different bodies/Member States participate in the preparation of the recommendations. More than 60 participants from relevant communities	90 participants attended ENISA's workshop in quarter 1 (with Italian data protection authority (DPA)). 150 participants attended ENISA's workshop in quarter 4 (with Greek DPA). Participants were representatives of all relevant communities (providers, controllers, national bodies). 9 representatives from different bodies and Members States were engaged in the preparation and validation of the recommendations. 6 representatives from different bodies and Members states were engaged in the preparation and validation of the recommendations. 120 participants attended the Annual Privacy Forum 2018 from all relevant communities.
Output O.2.2.6. NIS directive transposition	At least 15 Member States participate in the stock-taking exercise.	15 Member States participated in the validation of the ENISA NISD tool 24 Member States participated in the 1st Transport Cybersecurity Conference.
Objective 2.3. Response to Article 14 requests under policy		
Output O.2.3.1. Response to requests under policy activity	Answers to requests.	Answers provided. See https://www.enisa.europa.eu/publications/enisa-article-14-requests-2018

1.2.5 Specific results: mapping of deliverables into papers, publications or activities

Activity 2 — Policy: promote network and information security as an EU policy priority
Objective 2.1. Supporting EU policy development
Output O.2.1.1 — Support the policy discussions in the area of certification of products and services ***ICT security certification opportunities in the healthcare sector*** https://www.enisa.europa.eu/publications/healthcare-certification/ ***Supporting the transposition to the European cybersecurity certification framework*** Distribution will be limited
Output O.2.1.2 — Towards a framework for policy development in the cybersecurity ***Towards a framework for policy development in cybersecurity - Security and privacy considerations in autonomous agents*** https://www.enisa.europa.eu/publications/considerations-in-autonomous-agents/ ***ENISA's PETs Maturity Assessment Repository*** https://www.enisa.europa.eu/publications/enisa2019s-pets-maturity-assessment-repository/ This report is an internal ENISA document that aims to support further decision making within ENISA with regard to the PETs repository
Objective 2.2. Supporting EU policy implementation
Output O.2.2.1 — Recommendations supporting implementation of the eIDAS Regulation ***Assessment of standards related to eIDAS*** https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas ***Towards global acceptance of eIDAS audits*** https://www.enisa.europa.eu/publications/towards-global-acceptance-of-eidas-audits
Output O.2.2.2 — Supporting the implementation of the NIS directive ***Guidelines on the parameters of the identification of OES (implementation of Article 5(7))*** ***Guidelines for collecting and analysing security incidents for OESs and DSPs*** Not published but circulated in the NIS CG because the picture is fluid and incomplete due to lack of transposition by MS. ***Good practices on interdependencies between OESs and DSPs*** https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps
Output O.2.2.2 — Supporting the implementation of the NIS directive ***Guidelines on the parameters of the identification of OES (implementation of Article 5(7))*** ***Guidelines for collecting and analysing security incidents for OESs and DSPs*** Not published but circulated in the NIS CG because the picture is fluid and incomplete due to lack of transposition by MS. ***Good practices on interdependencies between OESs and DSPs*** https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps
Output O.2.2.3 - Baseline Security Recommendations for the OES Sectors and DSPs ***Guidelines on assessing DSP security and OES compliance with the NISD security requirements*** https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements
Objective 1.4. Response to Article 14 requests under expertise activity
Output O.2.2.4 - Supporting the payment services directive (PSD) Implementation ***Good practices for PSD2 implementation*** https://www.enisa.europa.eu/publications/good-practices-on-the-implementation-of-regulatory-technical-standards
Output O.2.2.5 — Contribute to EU policy in the area of privacy and data protection ***Recommendations on shaping technology according to GDPR provisions: an overview on data pseudonymisation*** https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions ***Recommendations on shaping technology according to GDPR provisions: exploring the notion of data protection by default*** https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2/ ***Reinforcing trust and security in the area of electronic communications and online services: sketching the notion of 'state-of-the-art' for SMEs in security of personal data processing*** https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-in-the-area-of-electronic-communications-and-online-services/
Output O.2.2.6 — NIS directive transposition ***ENISA NISD tool*** https://www.enisa.europa.eu/topics/nis-directive/nis-visualtool
Objective 2.3. Response to Article 14 requests under policy activity
Output O.2.3.1. Response to requests under policy activity ***ENISA Article 14 requests*** https://www.enisa.europa.eu/publications/enisa-article-14-requests-2018

1.3 KEY RESULTS IN THE IMPLEMENTATION OF ACTIVITY 3 — CAPACITY: SUPPORT EUROPE IN MAINTAINING STATE-OF-THE-ART NETWORK AND INFORMATION SECURITY CAPACITIES

1.3.1 Objective 3.1. Assist Member States' capacity building

1.3.1.1 Output O.3.1.1. Update and provide technical training for Member State and European Union bodies (priority 1)

In 2018 most of the activities in this area were aimed at maintaining and extending the collection of good practice guidelines and training for CSIRT and other operational personnel. The agency supported the development of Member States' national incident response preparedness by providing good practice guidance on key elements of NIS capacity building, with a focus on CSIRT training and services to improve the CSIRT teams' skills.

More specifically, the agency provided an update of the technical training material, which is highly regarded. The updated technical training material is on network forensics and provides a new set of materials that includes both; a thorough theoretical introduction and three sectorial use cases that are part of the hands-on section of the training material. The scenarios allow the training to be delivered in a modular way, tailored to the needs of the Member State CSIRTs and their constituency. This was done in order to reinforce Member State CSIRT skills and expertise to efficiently manage cybersecurity events. In this output, special emphasis was put on supporting Member State CSIRTs and EU bodies with concrete advice (like good practice material) and concrete action (like CSIRT training). ENISA delivered, upon request, direct support by providing tailored technical training on incident management.

In 2018, ENISA further enhanced its methodology, seminars and training on: (a) cyber crisis management and (b) the organisation and management of exercises. This activity included the development of material and infrastructure for onsite and online training on these subjects. In addition, this activity covered the delivery of these training programmes upon request.

As part of its continuous effort, ENISA maintains and regularly updates its training material. In 2018, ENISA also created new training material for the financial sector. The training includes a case study based on malware attacking a mobile banking application. The new material is now part of the updated training portfolio of the agency.

Finally, ENISA continued to support TRANSITS training delivery, with three courses being successfully delivered. TRANSITS provides trainings for both new and experienced CSIRT personnel and to date has directly trained more than 500 professionals in the European region.

1.3.1.2 Output O.3.1.2. Support European Union Member States in the development and assessment of national cybersecurity strategies

In 2018 ENISA supported the Member States in the development and assessment of NCSS by developing a tool for evaluating NCSSs and by further updating the ENISA NCSS map. ENISA, building on previous years' work, assisted Member States in deploying existing good practices in the related areas and offer targeted and focused assistance on specific NCSS objectives.

The evaluation tool was created with the aim of helping Member States evaluate their NCSSs in an easy, quick and user-friendly manner. The objective of the tool was to help Member States create second or third versions of their NCSS by evaluating their strategic objective. The tool's functionality provides questions on specific KPIs for each strategic objectives and depending on the answers, the tool generates advice and ideas for improving cybersecurity at a national level.

In 2018, ENISA published a new version of the online NCSS map. New features were included on the map. At first, the EFTA countries were displayed giving an overview of their strategic documents and objectives. The list of all Member States' strategic objectives were enriched with more examples, giving a clear outline of the status of each country. A new field of past versions has been added in the map, providing a complete overview of each country's strategies from past years.

ENISA also supported Switzerland by providing input for a book developed by Deutor and Springer Verlag that deals with best practice in cyber security for states, companies, the IT industry, law enforcement, the EU, international organisations and academia.

In addition, ENISA organised the sixth NCSS workshop in cooperation with the Finnish Communications Regulatory Authority. This conference focused on the development, implementation and evaluation of NCSSs and the creation of national, European and sectorial ISACs.

Representatives from both the public and private sector discussed about NCSSs, and shared best practices for the creation and running of ISACs.

1.3.1.3 Output O.3.1.3 — Support EU Member States in their incident response development (Priority 1)

ENISA's inventory of incident response teams listed 383 teams in December 2018, an increase of 41 teams in 1 year. The steady increase in teams clearly indicates the growth of incident response capabilities in Europe. For almost 15 years, ENISA has been supporting Member States and CSIRT communities in building and advancing their CSIRT capabilities, and ENISA continues to receive spontaneous requests from new teams all over Europe to be included in its inventory.

In 2018, ENISA concentrated its efforts on assisting Member States with their incident response capabilities by providing a state-of-the-art overview of the CSIRT landscape and development in Europe. This study helps ENISA identify and draw conclusions about the recent and current evolution of CSIRTs and incident response capabilities in Europe towards 2025. Building on the existing knowledge gathered in the European CSIRT inventory, this study aims to delve deeper into the 'blind spots' that may exist in this mapping. The study also points to interesting trends and identifies important issues, for example that more hardware vulnerabilities are being discovered in the components that are at the basis of our digital society and that the majority of these components are developed and manufactured outside of the EU. In close cooperation with the NISD CSIRTs network, the agency supports the development of Member States' national 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.

The main objectives of this output in 2018 was to help Member States and ENISA's 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 in securing their networks. Another objective of this output was to further develop and apply ENISA recommendations for the CSIRT baseline capabilities and maturity assessment framework. ENISA has continued supporting cross-border CSIRT community projects and tool development, as well as the global dialogue about common definitions and the maturity framework in the incident response domain.

1.3.2 Objective 3.2. Support European Union institutions' capacity building

1.3.2.1 Output O.3.2.1 Representation of the European Union Agency for Network and Information Security on the Steering Board of CERT EU and representation of the EU agencies using the CERT EU service (priority 1)

In 2018, the operations of CERT-EU were placed on a formal legal basis by way of a draft arrangement among a number of EU institutions. A Management Board was created to supervise the activities of CERT-EU, and a number of EU bodies and institutions are represented on it.

The growing need for IT security professionals is widely acknowledged; Europe has to make an effort to attract and retain talent in cybersecurity and to create solid and powerful education, entrepreneur and business structures relating to cybersecurity.

CERT-EU was set up to provide CERT services to the EU bodies and institutions. ENISA is appointed to CERT EU's Steering Board to represent itself and a list of EU agencies that may use their services.

In this context ENISA has been participating in the Steering Board of CERT-EU and liaising with the EU agencies on operational issues related to CERT-EU's activities in order to ensure that the viewpoints of the EU agencies are adequately represented. The cooperation with CERT-EU and role of coordination between the EU agencies and CERT-EU has been working very well and some important discussions were held in 2018. The needs of the EU decentralised agencies and ENISA are represented in the decision taken by the Steering Board.

ENISA will continue to represent the views on the evolution of services required by EU agencies in the CERT-EU Steering Board.

1.3.3 Objective 3.3. Assist in improving private sector capacity building and general awareness

1.3.3.1 Output O.3.3.1, Cybersecurity challenges (priority 1)

The growing need for IT security professionals is widely acknowledged; Europe has to make an effort to attract and retain talent in cybersecurity and, at the same time, create solid and powerful education, entrepreneur and business structures relating to cybersecurity which will allow us to develop the needed capabilities to prevent, react to and protect citizens against cyberthreats. In order to promote this capacity building on NIS among the emerging young generation of cybersecurity experts in Member States, ENISA will continue to promote and advise the Member States on national cybersecurity challenge competitions being held in 2019.

The agency will also continue its annual ECSC. Its support to national and European activities will be aimed at schoolchildren and university students, as well as young talent and security practitioners from the industry. The goal will be to increase interest and future opportunities in NIS for these communities by promoting excellence in the form of competitions. In order to do so, ENISA is attracting a large number of participants from different Member States for the final European competition.

At the same time, ENISA is supporting additional activities in order to measure and increase the impact of the cyber competitions at both national and European level and is participating in different Commission events and initiatives to promote young participants and put them on the spotlight.

1.3.3.2 Output O.3.3.2. European Cyber Security Month deployment (priority 1)

ECSM continued its efforts to educate people in and raise awareness of cybersecurity best practices. The campaign outperformed expectations, as evidenced by the increased number of participants and activities, and the increased engagement year-on-year. In 2018 ENISA focused on reaching the general public via social media, specifically during the week 2 theme 'Get Cyber Skilled' for which it collaborated with the European Schoolnet and the SaferInternet4EU campaign of the European Commission.

1.3.4 Objective 3.4. Response to Article 14 requests under capacity activity

1.3.4.1 Output O.3.4.1. Response to requests under capacity activity (priority 1)

No requests were received under capacity activity

1.3.5 General results: achievement of performance indicators for Activity 3

Summary of outputs in Activity 3 — capacity: support Europe in maintaining state-of-the-art network and information security capacities		
Outputs	**Performance indicator**	**Achieved results**
Objective 3.1. Assist Member States' capacity building		
Output O.3.1.1. Update and provide technical training for Member States and EU bodies	At least 10 Member States participate in the sectorial training At least 1 item of training material updated to support improved operational practices of CSIRTs in at least 15 Member States. Support at least 3 events. At least 70 % of participants in training (online or onsite) evaluate the experience as positive or very positive	European FI-ISAC group training (financial sector) 76 % are positive or very positive in overall evaluation 8 countries (Belgium, Portugal, Czechia, Ireland, Finland, Greece and Netherlands) participated in the European FI-ISAC group training – the number of Member States is based on the current Member State representation in the FI-ISAC established group. In total of 14 people received the training Updated the training course on network forensics. Three (3) TRANSITS Trainings delivered: 11-13 April 2018, Amsterdam (The Netherlands) 16-18 Oct 2018, Utrecht (The Netherlands) 6-8 Nov 2018, Prague (Czech Republic)
Output O.3.1.2. Support EU Member States in the development and assessment of NCSS	Engage at least 20 Member States in this activity/workshop.	In total 20 Member States were engaged in the activity/workshop
Output O.3.1.3. Support EU Member States in their incident response development	CSIRTs landscape report based on input from at least 30 European countries 2 inventory updates (Q2, Q4) During 2018, support provided at least for 2 incident response stakeholders to enhance their CSIRT baseline capabilities or maturity. At least 2 international CSIRT entities involved in the CSIRT maturity: common definitions and terminology project	Input collected from all 28 EU Member States and other European countries (Albania, Belarus, Bosnia and Herzegovina, Kosovo ([11]), Moldova, Montenegro, Norway, Serbia, Ukraine). In total input collected from 37 European countries. Inventory updated in 06/2018 and 12/2018 Already more than 30 CSIRTs supporting the taxonomy initiative. 4 CSIRTs involved in maturity pilot project, namely Portugal, Belgium, France and Latvia.
Objective 3.2. Support EU institutions' capacity building		
Output O.3.2.1. CERT EU engagement on behalf of ENISA and EU agencies	Consultation with EU agencies and representing their views at CERT EU Steering Board level.	CERT EU services adapted to the ENISA and EU decentralised agencies requirements. New price model adopted and many other discussions and about the future intended services.

11 This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.

Summary of outputs in Activity 3 — capacity: support Europe in maintaining state-of-the-art network and information security capacities		
Outputs	**Performance indicator**	**Achieved results**
Objective 3.3. Assist in improving general awareness		
Output O.3.3.1. Cyber security challenges	At least 2 additional EU Member States organise national cybersecurity challenges in 2018 and participate in the European Cyber Security Challenge Final.	2 New participants. Belgium and France organised national competitions and participated in ECSC 2018 edition.
Output O.3.3.2. European Cyber Security Month deployment	All 28 EU Member States and other partners and representatives from different bodies/Member States participate in/support ECSM 2018 (private and public sectors).	Activities took place across Europe from all 28 Member States and support for the campaign from different bodies across Europe helped increase visibility.
Objective 3.4. Response to Article 14 requests under capacity activity		
Output O.3.4.1. — Response to requests under capacity activity	Answers to requests.	Answers provided. See https://www.enisa.europa.eu/publications/enisa-article-14-requests-2018

1.3.6 Specific results: mapping of deliverables into papers/publications/activities

Activity 3 — capacity: support Europe in maintaining state-of-the-art network and information security capacities
Objective 3.1. Assist Member States' capacity building
Output O.3.1.1. Update and provide technical trainings for MS and EU bodies ***Introduction to network forensics*** https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material
Output O.3.1.2 — Support EU MS in the development and assessment of NCSS ***Updated ENISA map on NCSS in the EU*** https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map
Output O.3.1.3 — Support EU MS in their Incident Response Development ***Study on CSIRT landscape and IR capabilities in Europe 2025*** https://www.enisa.europa.eu/publications/study-on-csirt-landscape-and-ir-capabilities-in-europe-2025/
Objective 3.2. Support EU institutions' capacity building
Output O.3.2.1 — Representation of ENISA on the Steering Board of CERT-EU and representation of the EU Agencies using the CERT-EU service CERT-EU services adapted to the ENISA and EU decentralised agencies requirements New price model adopted and many other discussions and about the future intended services.
Objective 3.3. Assist in improving general awareness
Output O.3.3.1 — Cyber Security Challenges ***ECSC 2018 analysis report*** https://www.enisa.europa.eu/publications/ecsc-2018-analysis-report/
Output O.3.3.2 — European Cyber Security Month deployment ***European Cybersecurity Month 2018 deployment report*** https://www.enisa.europa.eu/publications/ecsm-2018-deployment-report/ ***Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*** https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity/
Objective 3.4. Response to Article 14 requests under capacity activity
Output O.3.4.1. Response to requests under capacity activity ***ENISA Article 14 requests*** https://www.enisa.europa.eu/publications/enisa-article-14-requests-2018

1.4 KEY RESULTS IN THE IMPLEMENTATION OF ACTIVITY 4 — COMMUNITY: FOSTER THE EMERGING EUROPEAN NETWORK AND INFORMATION SECURITY COMMUNITY

1.4.1 Objective 4.1. Cyber crisis cooperation

1.4.1.1 Output O.4.1.1 — Cyber Europe 2018 (priority 1)

In 2018 ENISA organised two pan-European exercises: Cyber Europe 2018 and CyberSOPEx 2018.

CYBER EUROPE 2018

Cyber Europe 2018 was the fifth pan-European cyber crisis exercise organised by ENISA. The exercise engaged around 900 participants, from the public authorities and private companies, mainly in the aviation sector, from all 28 EU Member States as well as two EFTA countries, Norway and Switzerland.

The exercise simulated an intense realistic crisis caused by a large-number of cybersecurity incidents (over 600) that occurred during the 2 days, 6-7 June 2018. The exercise was built on three main pillars:

a. the sound use of business continuity and crisis management plans within an organisation

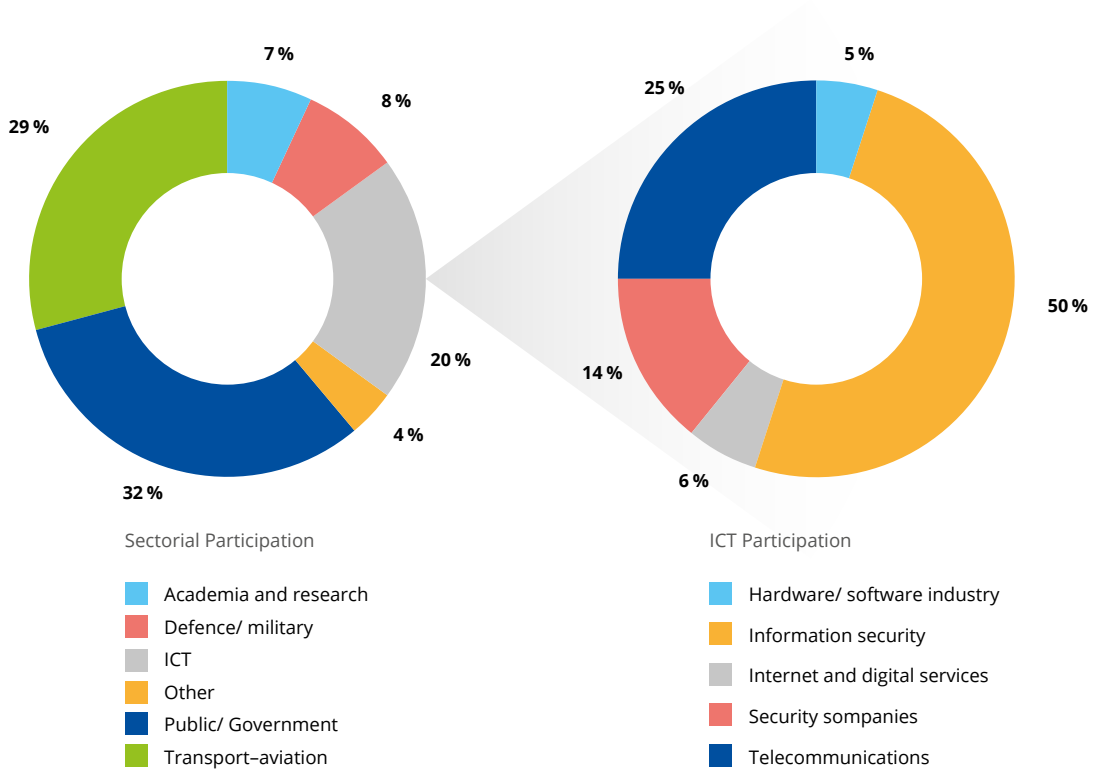
b. national-level cooperation and use of contingency plans

c. cross-country cooperation and information exchange

In addition, the exercise gave the opportunity for the technical teams to test their skills in cybersecurity with a vast variety of technical challenges, including malware analysis, forensics, mobile malware, advanced persistent threats, network attacks, IoT device infection, etc.

The exercise brought up the importance of cooperation between those involved in simulated cybersecurity incidents (victims and authorities), security providers and national authorities. It proved to participants that only through information exchange and collaboration,

Sectorial representation in Cyber Europe 2018



is it possible to respond to such extreme situations with a large number of simultaneous incidents. We have witnessed a large number of instances of public–private and private–private cooperation. Participants had to follow existing business processes, agreements, communication protocols and regulations to effectively mitigate the situations presented to them. Nevertheless, the level of preparedness varied significantly between participants, the information flow sometimes felt to be unidirectional and structured private-public cooperation procedures were immature or non-existent. The NISD identifies many of the associated shortcomings and proposes measures to improve the situation.

EU-level cooperation has undoubtedly improved over the past years. In particular, technical-level cooperation has proven mature and effective. The introduction of the CSIRTs Network as defined in the NISD has provided EU Member States with an effective formal structure to exchange technical information but also to collaborate in order to resolve complex, large-scale incidents. The exercise proved that at this level the EU is well equipped to respond. Some minor gaps were identified and have already been tackled by those involved. On the other hand, operational-level cooperation was exercised to a lesser extent. It is not so obvious how these levels will interact in real-life, and furthermore how they will implement the strategic vision of political leaders. Future exercises will try to test these aspects as well.

Finally, the technical aspects of the exercise provided an excellent opportunity for the cybersecurity teams to enhance their capabilities and expertise to deal with a variety of cybersecurity challenges. The operational capacity as well as the technical skills in all participating organisation proved to be at the highest level. Participating teams from non-cybersecurity private companies in the aviation sector analysed the majority of incidents successfully, and proved that their skillset is certainly very high. The only shortcoming in some cases was not the lack of skills but the actual number of available resources for IT security.

CYBERSOPEX 2018

In 2018, ENISA organised the CyberSOPEx pan-European exercise having as target audience solely the members of the CSIRTs network. This was the first time ever that the CSIRTs network took part in an extremely useful activity, with the aim of maturing technical-level cooperation in the European Union.

The high-level objective of this exercise was to improve the CSIRTs network's overall ability to cooperate, focusing on testing the network's standard operating procedures, as well as the supporting collaboration tools and infrastructures.

As planned, the exercise raised awareness of the cooperation procedures among the members of the CSIRTs network, trained participants in using the cooperation infrastructures, such as communication and information sharing, and finally contributed to identifying the elements that can improve cooperation and ultimately enhance trust within the CSIRTs network.

1.4.1.2 Output O.4.1.2 — Lessons learnt and advice related to cyber crisis cooperation (priority 1)

ENISA continued with the next phase of development of the Open Cyber Situational Awareness Machine (OpenCSAM) that aims at supporting the 'blueprint awareness' and 'reporting' pillars. The specifications and a tender for the next phase have been prepared based on feedback received by relevant stakeholders from EU institutions, the private sector and academia, who beta-tested the first version of OpenCSAM.

1.4.1.3 Output O.4.1.3 — Support activities for cyber exercise planning and cyber crisis management (priority 1)

ENISA aims to develop, maintain and enhance its ability to support all activities related to cyber exercises. This ability includes the possession of internal knowledge and expertise on the topic as well as the supporting tools and infrastructures. The latter, collectively called ENISA's cyber exercise platform (CEP), is of paramount importance in order be able organise multiple complex and large-scale exercises in a tractable manner.

Initial versions of CEP were conceptualised and developed by ENISA as early as 2014. CEP aims to host a number of services that ENISA offers to the Member States and EU institutions, such as exercise organisation and management, technical exercises, competitions and training, etc.

In 2018, ENISA improved the existing infrastructure. In particular, the efforts focused on:

(a) Building new functionality, most notably the Exercise Universe (see below);

(b) Improving the design of the infrastructure;

(c) Boosting the scalability features and responsiveness performance;

(d) Enhancing the user interface and user experience; and

(e) Safeguarding the cybersecurity of the infrastructure.

The ENISA Exercise Universe, part of CEP, is a unique type of cyber range. It is a set of IT systems and applications that mimic real-world infrastructures in an interactive way. These include mainstream media, social media, corporate and governmental websites, directories, repositories, etc. The Universe supports a single-sign-on capability, allowing the user to browse through the applications and services during an exercise in the same way as they would in equivalent real-life infrastructures. The Universe was tested during ENISA's organised exercises (see previous section) and has received positive reviews, along with feedback for further improvements in the future.

Finally, new content, challenges and material have been developed in order to keep up the interest of the stakeholders and make CEP a central tool in cybersecurity exercising for all stakeholders.

1.4.2 Objective 4.2. Computer security incident response teams and other network and information security community building

1.4.2.1 Output O.4.2.1. European Union computer security incident response teams network secretariat and support for European Union computer security incident response teams network community building (priority 1)

ENISA continued its support to the Commission and Member States in the implementation of the NISD, in particular in the area of CSIRTs as defined in Article 12, which establishes the CSIRTs network. As part of this activity, ENISA established the secretariat of the CSIRTs network and actively supported cooperation among the CSIRTs. The agency organised meetings of the CSIRTs network, stimulated discussion by proposing discussion topics, and hosted a variety of tools in support of active cooperation. It also provided its expertise and advice both to the Commission and Member States, either in the form of guidance or in response to specific requests. The agency also supported this cooperation by developing and providing guidance and good practices in the area of operational community efforts, such as on information exchange and secure communication, at the request of the members of the CSIRTs network. In particular, the agency was proactive in stimulating discussions within the CSIRTs network. The aim was to provide content to support discussions on policy and technical initiatives according to the CSIRTs network's own work programme (2017-2022). In 2018, the CSIRTs network reviewed, updated and adopted the mid-term objectives and goals of the work programme, as well as the terms of reference and rules of procedures, and formally handed its first report to the Cooperation Group.

In addition, ENISA took an active role in supporting CSIRTs in the CSIRTs network in activities relevant to the Connecting Europe Facility work programme.

Trust is an important asset for CSIRT operations and so ENISA continued the improvement of trust levels in the network by providing trust-building exercises and events in coordination with the CSIRTs network's governance. The agency continued to improve, develop and secure the CSIRTs network infrastructure for enabling a smoother operational and collaboration environment (CSIRTs network portal and other communication means), advancing swift and effective operational cooperation in the EU.

1.4.2.2 Output O.4.2.2. Support the fight against cybercrime and collaboration between computer security incident response teams and law enforcement agencies (priority 1)

In 2018 ENISA broadened its scope of cooperation between CSIRTs and Law Enforcement Agencies (LEAs), to also include the judiciary. Conclusions were drawn in the areas of legal shortcomings and trainings. Moreover, tools can be further leveraged by all groups concerned. In addition, ENISA continued its effort to support the EU-wide objectives on the fight against cybercrime by liaising with its CSIRT and law enforcement stakeholders in the EU by co-organising its annual workshop with Europol and the European Cybercrime Centre (EC3).

1.4.3 Objective 4.3. Response to Article 14 requests under community activity

1.4.3.1 Output O.4.3.1 — Response to requests under community activity (priority 1)

In 2018 ENISA supported the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) in its efforts to better enhance its proficiency in cybersecurity and business continuity. In particular, ENISA provided its expertise in exercise organisation and scenario development, as well as offering the fully-developed ENISA CEP to eu-LISA in order organise a preparedness exercise for one of the vital IT systems of the European Union.

1.4.4 General results: achievement of performance indicators for Activity 4

Summary of outputs in Activity 4 — community: foster the emerging European network and information security community		
Outputs	**Performance indicator**	**Achieved results**
Objective 4.1. Cyber crisis cooperation		
Output O.4.1.1. Cyber Europe 2018	At least 80 % of EU/EFTA Member States and countries confirm their support for Cyber Europe 2018	29 EU and EFTA Member States, plus EU institutions represented by CERT-EU, confirmed their support by participating in the exercise (bringing participants through extensive publicity).
Output O.4.1.2 Lessons learnt and advice related to cyber crisis cooperation	At least 80 % of the participating Member States agree to the developed operational procedures	28 EU Member States plus CERT-EU have agreed on a roadmap for the development of operational procedures following ENISA's gap analysis on the blueprint.
Output O.4.1.3 Support activities for cyber exercise planning and cyber crisis management	At least 70 % of CEP users evaluate it positively. Over 80 % of the countries in the Governance Board approve the handover roadmap.	Through the evaluation survey at the end of the exercise, more than 75 % evaluated CEP and the exercise positively ('good' to 'excellent').
Objective 4.2. CSIRT and other NIS community building		
Output O.4.2.1. EU CSIRTs network secretariat and support for EU CSIRTs network community building	Engage all 28 designated Member State CSIRTs and CERT-EU in the activities described in the network work programme (action plan 2017-2022) 28 Member States' dedicated CSIRTs and CERT-EU participated in CSIRTs Network regular meetings Work of ENISA successfully reflected by existing CSIRT communities (FIRST, TF-CSIRT, EU CSIRTs Network) and other national CSIRTs networks. Input received from at least 10 Member State CSIRTs network teams for the portal's further development Provide guidelines for CSIRTs Network members for performing the self-assessment and peer review. Review, update and adoption of the mid-term goals of the action plan.	The 28 Member States, the Commission and CERT-EU were active and engaged in the CSIRTs network activities described in the work programme. The 28 Member States, the Commission and CERT-EU actively participated in the CSIRTs network's regular meetings. Reference Security Incident Taxonomy Working Group was formally recognised as an official working group by TF-CSIRT in September 2018, and the first version of the taxonomy was released on GitHub. The CSIRT maturity assessment framework was successfully recognised and used by the Forum of Incident Response and Security Teams and the CSIRTs network. Portal development received input from 11 Member States (Germany, Estonia, France, Luxembourg, Malta, Netherlands, Austria, Portugal, Slovenia, Slovakia, Finland) and 13 teams. Guidelines were provided regarding CSIRT maturity self-assessment and peer review and the self-assessment was also integrated with an online tool available on the ENISA website. In July 2018 the CSIRTs network reviewed, updated and adopted the action plan and formally reported its activities to the Cooperation Group in August 2018.
Output O.4.2.2. Support the fight against cybercrime and collaboration between CSIRTs and LEA	At least 5 Member State CSIRT representatives and 5 Member State LEA representatives participate in the preparation of the report. At least 15 Member States participate in the ENISA/EC3 annual workshop.	**Report** **Interviews Online Survey** 9 Member State CSIRTs 8 Member State CSIRTs 7 Member State LEAs 17 Member State LEAs 4 Member State Judiciaries 7 Member State Judiciaries **ENISA/EC3 annual workshop** 11 Member State CSIRTs 17 Member State LEAs
Objective 4.3. Response to Article 14 requests under community activity		
Output O.4.3.1. Response to requests under community-building activity	Answers to requests	Answers provided. See https://www.enisa.europa.eu/publications/enisa-article-14-requests-2018

1.4.5 Specific results: mapping of deliverables into papers/publications/activities

Activity 4 — Community: foster the emerging European network and information security community
Objective 4.1. Cyber crisis cooperation
Output O.4.1.1 . Cyber Europe 2018 ***Cyber Europe 2018: after action report*** https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report
Output O.4.1.2. Lessons learnt and advice related to cyber crisis cooperation **OpenCSAM** The project aims to provide a decision support tool for the blueprint. Status: the initial prototype was delivered in 2018 and was evaluated by ENISA and external experts from the EU institutions and Member States. Based on this evaluation, the second phase of development is starting in 2019.
Output O.4.1.3. Support activities for cyber exercise planning and cyber crisis management **2018 EU parallel and coordinated exercises** ENISA contributed to the planning of the 2018 EU parallel and coordinated exercises, organised by the European Commission and the European Council. ENISA also participated for the first time as part of the audience.
Objective 4.2. CSIRT and other NIS community building
Output O.4.2.1. EU CSIRTs network secretariat and support for EU CSIRTs network community building Encrypted communications solutions for the CSIRTs network. Mapping CSIRT capabilities to EU NIS requirements: business continuity Mapping CSIRT capabilities to EU NIS requirements: physical security Mapping CSIRT capabilities to EU NIS requirements: human resources staffing These reports are available to the CSIRTs network's members only.
Output O.4.2.2. Support the fight against cybercrime and collaboration between CSIRTs and LEA **Cooperation between CSIRTs and law enforcement: interaction with the judiciary** https://www.enisa.europa.eu/publications/csirts-le-cooperation/
Objective 4.3 Response to Article 14 requests under community activity
Output O.4.3.1. Response to requests under community-building activity ***ENISA Article 14 requests*** https://www.enisa.europa.eu/publications/enisa-article-14-requests-2018

GENERAL RESULTS FROM PREVIOUS YEARS

Summary of deliverables from previous years		
Work package	**Performance indicator**	**Achieved results**
Objective 3.		
4.3.2 WPK3.2. Supporting European Union policy implementation 4.3.2.1 WPK3.2.A. Assist EU MS and Commission in the implementation of the NIS directive	• By 2018, five MS deploy ENISA's guidelines on NIS directive in a 3 sectors/services. • By 2018, 10 private organisations deploy ENISA's guidelines on NIS directive in a 3 sectors/services.	ENISA consults with the Cooperation Group for the guidelines on the NISD, thus all the Member States have deployed, to a certain extent, these documents in all NIS sectors. Furthermore, the NCAs have incorporated the provisions of these non-binding guidelines into their national approaches to different NISD requirements, e.g. incident reporting, security measures for OESs and security assessments, thus making the OESs and the DSPs in each Member State deploy the ENISA guidelines.

1.5 KEY RESULTS IN THE IMPLEMENTATION OF ACTIVITY 5 — ENABLING: REINFORCE THE EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY'S IMPACT

Activity 5 covers the following two main objectives.

- Management and compliance.
- Engagement with stakeholders.

1.5.1 Objective 5.1. Management and compliance

1.5.1.1 Management

The Executive Director is responsible for the overall management of the agency.

To support the policy, legal and strategy activities of the agency, a Policy Office unit was established. The tasks covered by this unit include policy advice, legal advice and coordination of the work programme.

During 2018, policy and legal advice extended to all aspects of the agency's work and included advice in relation to both the operational and resources departments of the agency.

In 2018 the Management Board Secretariat continued to support the Management Board and the Executive Board in their functions by providing administrative assistance.

In relation to the Management Board, one ordinary meeting and three informal meetings were organised during 2018. The Management Board portal was maintained as well. Four meetings of the Executive Board were held.

1.5.1.2 Data protection compliance tasks and data protection officer

As of December 2018, Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the EU institutions, offices and agencies[12] is applicable to ENISA, replacing the previous data protection regulation (Regulation (EC) No 45/2001). Regulation 2018/1725 sets out the main tasks of the data protection officer (DPO) as follows [13]:

- to inform and advise ENISA of its obligations pursuant to Regulation 2018/1725 and to other EU data protection provisions;
- to ensure in an independent manner the internal application of Regulation 2018/1725; to monitor compliance with this Regulation, with other applicable EU law containing data protection provisions and with the policies of ENISA in relation to the protection of personal data, including the assignment of responsibilities, the raising of awareness and training of staff involved in processing operations, and the related audits;
- to ensure that data subjects are informed of their rights and obligations pursuant to Regulation 2018/1725;
- to provide advice where requested as regards the necessity for a notification or a communication of a personal data breach pursuant to Articles 34 and 35 of Regulation 2018/1725;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 39 of Regulation 2018/1725 and to consult the EDPS in case of doubt as to the need for a data protection impact assessment;
- to provide advice where requested as regards the need for prior consultation of the EDPS pursuant to Article 40 of Regulation 2018/1725; to consult the EDPS in case of doubt as to the need for a prior consultation;
- to respond to requests from the EDPS; within the sphere of the DPO's competence, to cooperate and consult with the EDPS at the latter's request or on the DPO's own initiative;
- to ensure that the rights and freedoms of data subjects are not adversely affected by processing operations.

During 2018 one of the main tasks of the DPO was to support ENISA's transition from the previous data protection framework to Regulation 2018/1725. To this end, several actions were undertaken, including guidance on the creation and maintenance of records

12 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1725

13 See articles 43 to 45 of Regulation 2018/1725 for a more detailed description regarding the designation, position and tasks of the DPO.

of data processing activities across the agency, a new central register for the maintenance of these records, internal policies for specific data processing activities, guidance on the update of ENISA's web services, etc. A data protection training course was delivered by EDPS in quarter 1 for all ENISA staff, followed up by specific data protection presentations of the ENISA DPO later in the year. The DPO and deputy DPO closely followed the activities of the EDPS and the EU institutions' network of DPOs and participated in relevant meetings, discussions and information exchange.

1.5.1.3 Information Security Officer

The information security officer (ISO) coordinates the information security management system on behalf of the authorising officer. In particular, the ISO advises the Corporate Service unit in developing and implementing information security policies, standards, guidelines and baselines that seek to secure the confidentiality, integrity and authentication of the agency's information systems. The ISO is instrumental in incident handling and incident response, and in security-event monitoring. The ISO also leads the security training for the agency's staff and provides security guidance on all IT projects, including the evaluation and recommendation of technical controls.

In 2018 the ISO undertook several activities in order to enhance the security posture of the agency:

- an updated risk assessment with a focus on business continuity.
- regular vulnerability scans of ENISA important portals and assets.
- awareness raising for ENISA staff
- updated policies.
- continuous monitoring.

Throughout 2018, several technical activities were carried out in relation to information security, in particular updating of security and information, the creation of an and event management platform with enhanced logging capabilities, and updating of the incident repository was brought up to date. Another comprehensive security posture assessment was carried out with a focus on business continuity.

1.5.2 Objective 5.2. Engagement with stakeholders and strong international activities

Under this objective are grouped some of the tasks and activities of the agencies carried out in collaboration with stakeholders.

- National Liaison Officers' (NLOs') Network.
- Permanent Stakeholders Group
- Stakeholders' communication and dissemination activities.
- Outreach and image building activities.

National Liaison Officers Network

NLOs are key to the agency's daily work. They are the liaison between ENISA and the community of network and information security experts and relevant organisations in their respective Member State acting as 'ambassadors' and 'facilitators' of ENISA's work.

The current Permanent Stakeholders Group is composed of three nominated members who represent NRAs, DPAs and law enforcement authorities (Europol,the Office of the Body of European Regulators for Electronic Communications and one advisory body, the European Data Protection Board).

In 2018, ENISA enhanced its cooperation with the NLO Network as the first point of contact for ENISA in the Member States by implementing the 'guidelines on missions, principles and functioning of the NLO network' that were adopted at the Management Board meeting of October 2017.

The annual NLO meeting took place in January 2018, to better align the NLO activities to the ENISA Work Programme, studies and events from early on.

Particular emphasis was placed on ENISA outputs, expert groups and procurement for 2018 in view of

the enhanced role for NLOs decided at Management Board level.

The agency maintained, and shared with the NLO Network, information on all relevant ENISA projects and activities. Information was sent to the members of the NLO Network at regular intervals on upcoming ENISA project-related tenders, vacancy notices, events organised or contributed to by ENISA, etc.

Permanent Stakeholders Group

The Permanent Stakeholders Group was established by the ENISA regulation (Regulation (EU) No 526/2013). The Management Board, acting on a proposal by the Executive Director, sets up a Permanent Stakeholders Group for a term of office of 2.5 years.

The current Permanent Stakeholders Group is composed of three nominated members who represent NRAs, DPAs and law enforcement authorities (Europol,the Office of the Body of European Regulators for Electronic Communications and one advisory body, the European Data Protection Board). The remaining members are appointed *ad personam*, from Industry, Academia and Consumer Organisations amounting to 34 members from all over the European Union. These members constitute a multidisciplinary group and are selected upon the basis of their own specific expertise and personal merits.

The role of the Permanent Stakeholders Group is to advise the Executive Director on the development of the agency's work programme and on ensuring communication with the relevant stakeholders on all related issues. For this purpose two annual meetings were held in 2018, one in March and one in November.

Stakeholders' communication and dissemination activities

In 2018 ENISA sought to improve its focus on key activities and engage with the highest possible number of stakeholders. This includes the institutional stakeholders (e.g. EU Institutions) and other various groups such as national authorities, academia, industry, citizens, etc.

The agency continued to develop various communication tools and channels, including the website, with a strong emphasis on social media and news.

Dissemination activities are the responsibility of the Policy Office and Public Affairs Team, which will seek the appropriate level of outreach activities to take ENISA's work to all interested parties and to provide added value to the European Union.

Outreach and image-building activities

ENISA´s image of quality and trust is paramount for all stakeholders. It is essential that EU citizens can trust ENISA's work.

Cybersecurity threats are increasing all over the world, and Europe is no exception. With this in mind, ENISA's profile needs to be continuously strengthened.

The dissemination of the agency work is essential in creating an NIS culture across the various actors in Europe. ENISA is aware of this fact, and will aim to reach all stakeholders who require information about the work developed by the agency.

Several activities that will strengthen cybersecurity awareness across Europe are planned in different Member States, fulfilling ENISA's mandate, mission and strategy.

PART II

ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL

This section explains how ENISA delivered the achievements described in the previous section. It is divided into two subsections: 1) financial management and internal control and 2) declaration of assurance.

2.1 FINANCIAL MANAGEMENT AND INTERNAL CONTROL

2.1.1 Financial management

2.1.1.1 Budget execution of European Union subsidy (current year 2018 - C1 funds)

The excellent budget execution can be translated into the following figures: the expenditure appropriations for ENISA's 2018 budget of EUR 10 786 374 were committed at a rate of 99.9 % as at 31 December 2018.

The overall performance demonstrates the already proven ability of the agency to use the entrusted funds efficiently in order to implement its annual work programme and to manage its operational and administrative expenditure.

The respective payment rate on expenditure appropriations was 89.29 % in 2018. This payment rate is high and demonstrates that the agency's ability to finalise its annual activities and to execute the relevant payments within the year of reference was maintained. The procurement planning, which was moved forward to the end of the preceding year (2017) and enabled the agency to launch projects related to the work programme in early 2018, contributed significantly to the improvement of the payment rate of appropriations of the year (C1).

2.1.1.2 Amending budgets and budgetary transfers

The following table summarises the impact of budgetary transfers applied to the approved budget distribution in the 2018 budget (C1).

Table — Summary of budgetary transfers 1 to 6 impact on budget

	Initial budget allocation	2018 budget transfers approved by the Executive Director	Appropriations after budget transfers
Title 1	6 386 500.00	608 493.46	6 994 993.46
Title 2	1 047 500.00	– 131 408.52	916 091.48
Title 3	3 375 000.00	– 477 084.94	2 897 915.06
Total	**10 809 000.00**	**0.00**	**10 809 000.00**

The following table summarises the subsequent impact of the amending budget 1/2018 (approved by the Management Board).

Table — Summary of amending budget 1/2018 impact on budget

	Appropriations after transfers	Amending budget 1/2018	New appropriations 2018 (after amending budget 1/2018)
Title 1	6 994 993.46	758 573.59	6 402 617.30
Title 2	916 091.48	– 219 546.66	1 593 129.99
Title 3	2 897 915.06	– 562 321.23	3 179 478.20
Total	**10 809 000.00**	**– 23 294.30**	**10 785 705.70**

The table below summarises the impact of budget transfers (approved by the Executive Director after the adoption of amending budget 1/2018) on the final budget execution (C1).

Table — Summary of the budgetary transfers and impact on budget

	New appropriations 2018 (amending budget 1/2018)	2018 budget transfers 8-12 approved by the Executive Director	Final budget execution 2018
Title 1	6 402 617.30	– 8 800.39	7 744 766.66
Title 2	1 593 129.99	118 505.68	815 050.50
Title 3	3 179 478.20	– 109 705.28	2 225 888.54
Total	**10 785 705.70**	**0.00**	**10 785 705.70**

ENISA's budget does include the rent subsidy granted by Hellenic Authorities to ENISA representing a maximum amount of 640.000 euro per annum to cover its premises' lease requirements in Greece.

2.1.1.3 Carry forward of commitment appropriations

The commitment appropriations corresponding to the EU subsidy (C1 appropriations) that were not consumed by payments at the end of 2018 were carried forward to 2019 (C8 appropriations).

The commitment appropriations corresponding to the assigned revenues that were not consumed by payments at the end of 2018 were carried forward to 2019 (R0 appropriations).

The funds carried forward to 2019 (C8 appropriations) are detailed below:

Table — Summary of carry forwards 2018 to 2019

Title	Total C1 appropriations carried forward to 2019	Total R0 appropriations carried forward to 2019	Total amount carried forward from 2018 to 2019
Title 1. Staff	527 606.30	97 920.00	527 606.30
Title 2. Administration	323 627.64	18 473.73	323 627.64
Title 3. Operations	381 029.46	0.00	381 029.46
Total	**1 232 263.40**	**116 393.73**	**1 348 657.13**

The total of cancelled appropriations carried forward from 2017 to 2018 (C8 appropriations of 2018) but finally not paid in 2018 was EUR 110 505.47.

2.1.2 Controls

2.1.2.1 Internal Controls

Risk management

The agency has implemented an organisational structure and internal control systems suited to the achievement of policy and control objectives, in accordance with the standards and having due regard to the risks associated with the environment in which it operates.

The analysis of the register of exception and of the ex-post report combined with the result of the independent auditors (ECA and IAS) provide adequate and sufficient assurance as to the completeness and reliability of the information reported.

Control effectiveness as regards legality and regularity

The agency has set up internal control processes to ensure the management of risks related to the legality and regularity of underlying transactions. These control processes take into account the multiannual character of programmes, as well as the nature and complexity of the related financial transactions. To mitigate the risks of errors, the agency implements ex-ante verification to all its financial transactions.

In line with internal control standard (ICS) 8 ('processes and procedures'), the agency has produced the *ex post* control report for the financial year 2017. The recommendations issued in the report were addressed during the year to prevent future reoccurrence of these exceptions.

Compliance and effectiveness of internal control standards

ENISA has adopted a set of ICSs, based on international good practices, that aim to ensure the achievement of policy and operational objectives.

As regards financial management, compliance with these standards is compulsory.

In 2010 the Management Board of the agency adopted a set of 16 ICSs laying down the minimum requirements with which its internal control systems need to comply. Previously developed internal procedures were grouped together, prioritised and implemented in the daily workflows of the agency, as deemed appropriate.

The agency is planning to adopt the new internal control framework in 2019.

Ex-post audit control and exception

In 2018, ENISA performed ex-post controls as part of the internal control framework, for the financial year 2017. A total of 269 financial transactions were selected and checked, representing 13,82 % of all of the agency's financial transactions and 69,70 % of the agency's 2017 budget. As a result, five recommendations were issued.

Four of them are observations on administrative procedures for which corrective measures have already been taken. The last observation is related to the late payment of the rent subsidy by the Hellenic Authorities, which created a delay of payment from the agency to its landlord.

In 2018 the agency recorded 33 exceptions of which 26 are under the materiality levels and are of minor administrative nature with no financial impact.

The seven remaining, exceptions were due to a posteriori commitments. Reminders have been communicated to the respective project managers on the legality of carry forward commitments. Controls for the 2019 carry forward will be reinforced by increasing the sample check.

Moreover, the ECA is in charge of the annual audit of the agency, which concludes with 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.

Compliance regarding transparency, accountability and integrity

The agency is committed to constantly being vigilant and improving openness and transparency, with the goal of helping EU citizens and any other stakeholders understand how the agency is managed and being held accountable. With this objective ENISA publishes a wide range of documents and other relevant information on its website (https://www.enisa.europa.eu).

In accordance with the ENISA regulation (Regulation (EU) No 526/2013), the Management Board is the governing body of the agency. It is composed of representatives of the EU Member States and the European Commission. Its main role is to ensure that the agency carries out its tasks in accordance

with its operational and strategic objectives, as adopted by the agency's annual and multiannual work programme. It also supervises all budgetary and administrative matters.

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

The Management Board also 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, the executive director has the duty, among others, to provide an annual activity report addressed to the Management Board in order to assess ENISA's activities. The Management Board then, in turn, has to analyse and assess this report.

Once approved, and no later than 30 June of the year following the year under review, the annual activity report, which outlines the achievements for the year and the resources used, is formally adopted and communicated to the relevant stakeholders (namely the European Parliament, the European Council, the European Commission and the ECA). Once approved it is made publicly available through ENISA's website. For further financial transparency, the annual accounts (including the budgetary execution report) and the annual adopted budget are also disclosed 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 to the European Parliament all the information necessary for the discharge procedure. The discharge procedure is a tool for the Members of the European Parliament to check how and to what end public funds have been spent. The European Parliament can then decide to grant, postpone or refuse a discharge for a specific year.

To help the European Parliament in the discharge procedure, independent reviews of the agency take place. On an annual basis, the ECA gives assurance on the reliability of the annual financial statements and on the legality and regularity of the transactions conducted by the agency for the year under review. The IAS conducts periodic audits on specific topics, which are selected based on a risk assessment.

The results and follow-ups 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 the long-term impact of the agency's operations.

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, Permanent Stakeholder's Group, Executive Director and officials seconded by 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 has adopted an anti-fraud strategy and action plan. It achieved a significant result in terms of awareness-raising by preparing and delivering internal training on fraud prevention to its entire staff. Periodic training is planned to ensure that staff are continuously reminded of fraud prevention. As of 2018 fraud awareness training is included in yearly ethics and integrity training, which is compulsory for all staff.

In addition to the staff regulations, the agency is developing a code of conduct for all staff that offers comprehensive information and advice on a variety of issues, ranging from ethics to compliance with legal obligations. The aim 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 behaviour issued by the European Ombudsman, ENISA aims a 2-week deadline to answer requests from citizens.

2.1.2.2 Audit observations and recommendations

This section discloses and assesses the observations, opinions and conclusions published by auditors in their reports as well as the limited conclusion of the Internal Auditor on the state of internal control, which could 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 stakeholders' involvement in deliverables was issued in June 2018. Five non-critical audit findings and related recommendations were identified during this audit. ENISA has set up a specific

Main observations by the discharge authority	ENISA's replies and measures
Inclusion of a standard chapter on transparency, accountability and integrity in 2016 annual report.	As from the 2017 annual activity report a standard chapter on transparency, accountability and integrity is included (see previous section).
Considerable delay in the payment of rent for the offices in Athens by the Greek authorities.	Regarding the payments from the Hellenic Authorities, improvements have been made from the second semester of 2018.
Difficulty in recruiting, attracting and retaining suitably qualified staff	The agency has implemented social measures (e.g. a schooling programme) to improve attractiveness and retain qualified staff.
Absence of publication on the website of the CVs and declarations of interests of the agency's Management Board and Executive Board members.	Declarations of interest, declarations of commitment and CVs of ENISA Management Board representatives can be found here: https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/mb2019
Notes that a whistleblowing policy is being discussed between the EU's decentralised agencies and that a common policy and guidelines will be adopted in 2018; calls on the agency to report to the discharge authority on the implementation of that policy	The whistleblowing policy was adopted by the agency's Management Board in August 2018
Points out that the agency has not yet provided any specific initiative to improve transparency in its contacts with lobbyists and stakeholders; calls on the agency to enact a proactive lobby transparency policy without further delay and to report to the discharge authority on any measures taken addressing this issue; notes from the agency's reply that they are in the process of writing a policy addressing the issue	The agency will adopt in 2019 specific processes to improve transparency in its contacts with lobbyists and stakeholders

task force to ensure the adequate implementation of the action plan agreed with the IAS. As of the end of 2018, two recommendations have been closed, while processes and procedures still need to be revised and updated to address the three remaining recommendations.

European Court of Auditors

Issued in 2018, the ECA report on the 2017 annual accounts does not contain any critical audit findings.

Follow-up of audit plans, audits and recommendations

The agency will continue to improve its internal systems and remain vigilant with regard to possible risks of its activity within the internal legal and financial framework, in order to strive for the current situation of non-compliance issues attested by the IAS and the ECA.

Follow-up of observations from the discharge authority

2016 discharge

Regarding the European Parliament decision of 18 April 2018, the Executive Director of the agency was granted discharge in respect of the implementation of the agency's budget for the financial year 2016. The closure of the accounts of the agency for the financial year 2016 was also approved [14].

Measures implemented in response to the observations of the discharge authority

The table above presents a summary of the main observations and comments by the discharge authority on the implementation of the 2016 budget and the measures taken by ENISA.

14 http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2018-0153&format=XML&language=EN

2.1.3 Assessment of the effectiveness of the internal control systems

ENISA has adopted an internal control framework based on international good practice, aimed at ensuring the achievement of policy and operational objectives. In addition, as regards financial management, compliance with the internal control framework is a compulsory requirement.

ENISA has put in place the organisational structure and the internal control systems suited to the achievement of the policy and internal control objectives, in accordance with the standards and having due regard to the risks associated with the environment in which it operates.

Based on the most relevant key indicators and control results, ENISA has assessed the effectiveness, efficiency and economy of the control system and reached a positive conclusion on the cost-effectiveness of controls.

In conclusion, management has reasonable assurance that, overall, suitable controls are in place and working as intended; risks are being appropriately monitored and mitigated; and necessary improvements and reinforcements are being implemented.

2.2 DECLARATION OF ASSURANCE

I, the undersigned,

Udo Helmbrecht

Executive Director of the European Union Agency for Network and Information Security,

in my capacity as authorising officer,

declare that the information contained in this report gives a true and fair view [15].

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.

Heraklion, 30. 6. 2019

[signed]

Udo Helmbrecht

Executive Director

15 True and fair in this context means a reliable, complete and accurate view on the state of ENISA's affairs.

2.2.1 Review of the elements supporting assurance

The risk framework is used as a common means of classifying and communicating risk across the agency. It provides a common understanding and language regarding risk, along with a structure for the assessment, reporting and monitoring of risk. The risk framework defines the categories, subcategories and business risks applicable at the organisational level for ENISA as a whole. It includes:

- risk categories and subcategories;
- risks specific to each category (business risks);
- risk definition.

The agency's operations are channelled through the following activity areas that belong to administrative functions.

- Own resources (staff) that carry out tasks in line with ENISA's programming document in terms of operational and administrative activities.
- Contractors that support operational activities and other support activities that cannot be insourced by the agency. External agents are appointed either through a procurement procedure or through a call for expressions of interest for funding related to the shared organisation of events. Alternatively, in the case of working group members, they may be chosen by means of a selection procedure.

To mitigate compliance risks with regard to its administrative activities, the agency has carried out the activities presented in the table below.

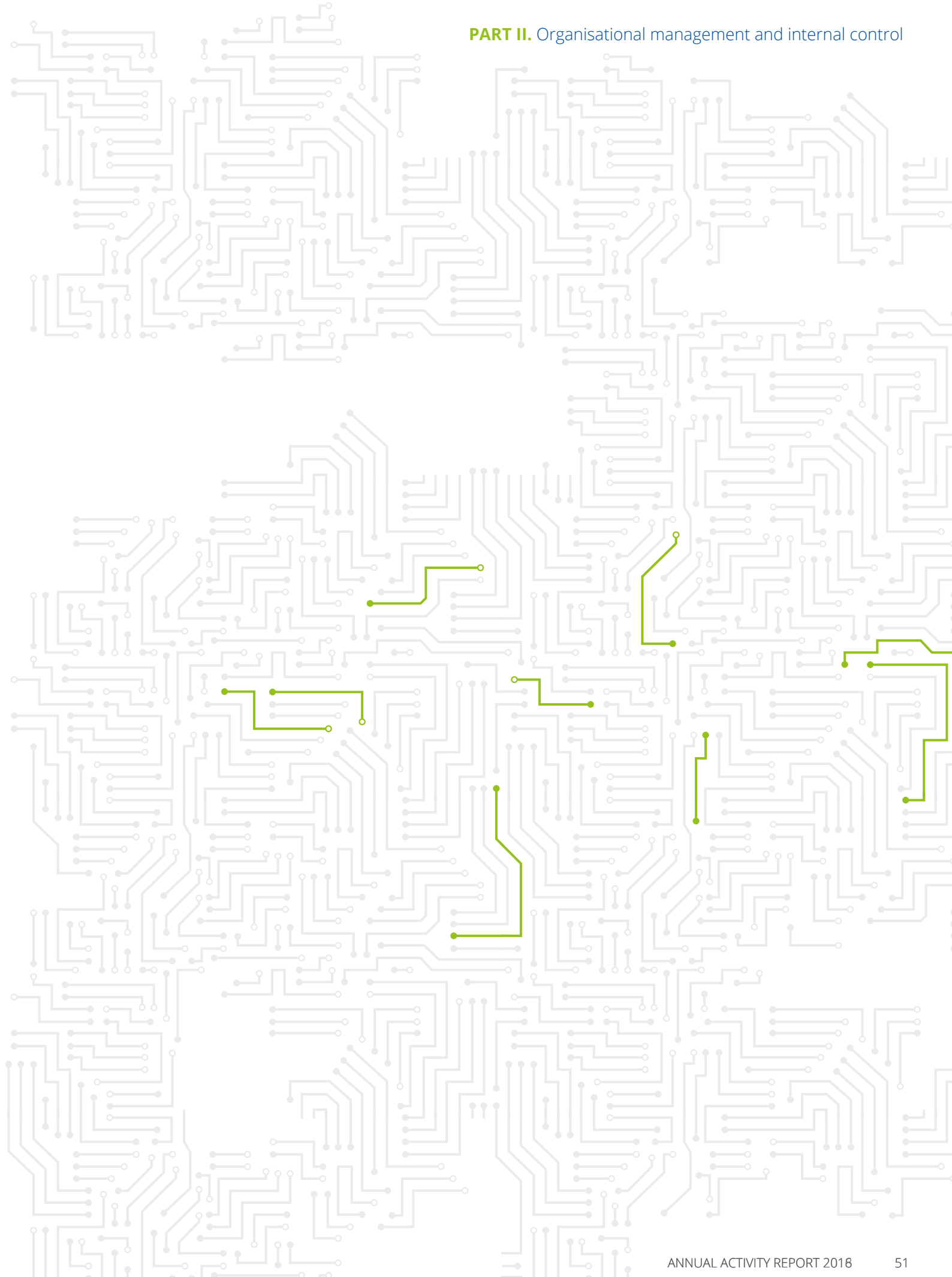
2.2.2 Human resources management

As at 31 December 2018, 74 statutory staff were employed by the agency (44 temporary agents (TAs), 27 contract agents (CAs) and three seconded national experts (SNEs)) . Despite the great efforts made in the selection procedures the agency's attraction and retention capability is still suffering from a low country coefficient factor and the fact that contract agent posts are not financially competitive in the cybersecurity job market.

In relation to schooling in Athens, where no European Schools are based, several service-level agreements have been concluded with each of the private schools being used by the children of ENISA staff members. Several children of staff members at ENISA Heraklion attended the European School in Heraklion in 2018, which offers education at nursery, primary and secondary levels. ENISA has a service-level agreement with the Commission's Directorate-General for Human Resources and Security for the provision of these services. In total five pupils attended the European School in Heraklion and 49 pupils attended crèche and schools in Athens.

The organisational chart, establishment plan and statistics for ENISA staff are included in Annex A.1.

Nr	Systemic process	Activity	Performance indicator
1	Follow up on auditor's comments and recommendations regarding administrative practices and procedures as they are implemented in line with financial regulation, implementing rules and the Staff Regulations.	Updating of documents and activity reporting.	Feedback by auditors in the next application period and overall improvement of performance.
2	Opening and closing of the annual budget and preparation of budgetary statements.	Approved set of budget lines for the period. Ensure financial appropriations are posted properly.	Annual budget lines open and running by the end of the year with the anticipated budget, economic out-turn account and supporting operations completed in time.
3	Implementation and consolidation of internal controls, as appropriate.	Annual review of internal controls.	Guidelines and checklists reviewed, annual risk assessment done. Controls updated accordingly. Staff participation and information.
4	Performance management exercise	Organise annual performance evaluation. Administer appeals	Number of appraisals concluded on time
5	Annual Learning and Development policy including training plan	Draft the learning and development policy including training plan.	Implementation of the learning and development policy and number of training courses delivered.
6	Talent Management strategy including annual recruitment plan	Execute the agency recruitment plan in line with the establishment plan.	Number of staff hired to cover new posts or make up for resignations
7	Internal ICT networks and systems.	Secure ICT networks and systems in place.	Results of external security assessment or audit.
8	Public procurement.	Regular, consistent observation of public-procurement practices and appropriate assistance provided to all departments.	Clear mandate of the procurement function established, staff informed, forms available, number and type of procurement processes handled, files of procurement processes organised and files for audit available. List of number of purchase orders per supplier, number of complaints processed.
9	Contract management.	General support on contract management.	Number of contracts prepared and signed by the agency, number of requests for support received from departments, number of claims processed.
10	*Ex ante* controls.	Well developed at the procedural, operational and financial levels.	Number of transactions as compared to number of erroneous transactions.
11	*Ex post* controls.	Well developed and done on annual basis.	Number of transactions as compared to number of erroneous transactions.



A

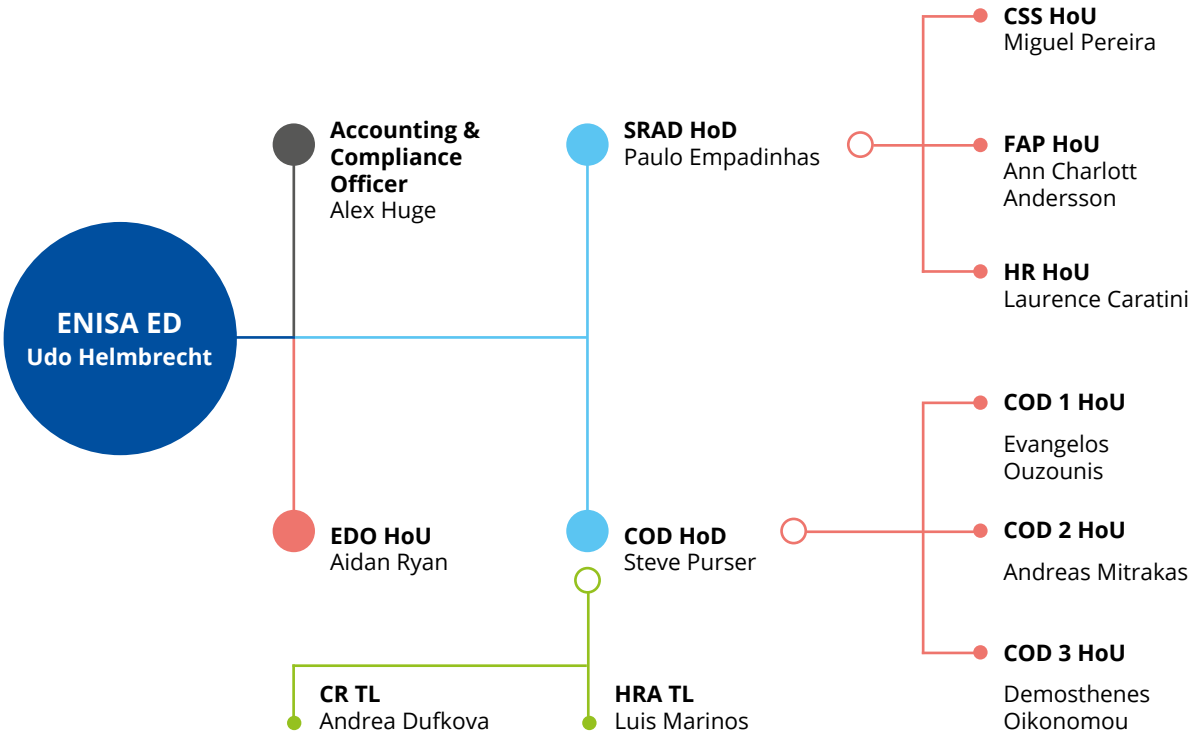
ANNEX 1
HUMAN RESOURCES

A.1.1 ORGANISATIONAL CHART

As provided for by the ENISA regulation (Regulation (EU) No 526/2013), the bodies of the agency comprise the following.

- A Management Board. The Management Board ensures that the agency carries out its tasks under conditions that enable it to serve in accordance with the founding regulation.
- An Executive Board. The Executive Board prepares decisions to be adopted by the Management Board on administrative and budgetary matters.
- A Permanent Stakeholders Group. The Permanent Stakeholders Group advises the Executive Director in the performance of his/her duties under this regulation.
- An Executive Director. The Executive Director is responsible for managing the agency and performs his/her duties independently.

Internally, ENISA is organised as follows (staffing as of 31.12.2017).



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

ED – Executive Director
SRAD – Stakeholders relations and administration department
HR – Human Resources
FAP – Finance and Procurement
CSS – Corporate Services and Stakeholders
EDO – Executive Director Office
COD – Core operations department
COD 1 – Secure Infrastructure & Services
COD 2 - Data Security & Standardisation
COD 3 - Operational Security
CR – CSIRT Relations
HRA - Horizontal Support & Analysis
TL – Team leader

A.1.2 ESTABLISHMENT PLAN 2018

Function group and grade (TA/AST)	2018 posts: Authorised under the EU budget	
	Permanent	Temporary
AD 16		
AD 15		1
AD 14		
AD 13		
AD 12		3
AD 11		
AD 10		5
AD 9		10
AD 8		15
AD 7		
AD 6		
AD 5		
AD total:		**34**
AST 11		
AST 10		
AST 9		
AST 8		
AST 7		2
AST 6		5
AST 5		5
AST 4		1
AST 3		
AST 2		
AST 1		
AST total:		**13**
Total staff:		**47**

A.1.3 INFORMATION ON ENTRY LEVEL FOR EACH TYPE OF POST

Nr	Job title	Type of contract (Official, TA, CA or SNE)	Function group/ Grade of recruitment	Indication of function dedicated to administrative, support or operations
1	Executive Director	TA	AD 14	Top Operations
2	Head of Department	TA	AD 11	Administrative
3	Head of Unit	TA	AD 9	Administrative/ Operations
4	Team Leader	TA	AD 7	Administrative/ Operations
5	Team Leader	CA	FGIV	Administrative/ Operations
6	Expert in Network and Information Security	TA	AD5	Operations
7	Officer in Network and Information Security	CA	FGIV	Operations
8	Assistant	AST	2	Administrative/ Operations
9	Assistant	CA	FGI	Administrative/ Operations
10	Senior Assistant	AST	4	Administrative/ Operations
11	Senior Assistant	CA	FGIII	Administrative/ Operations
12	Lead Expert Network and Information Security	AD	8	Operations
13	Advisor Expert Network and Information Security	AD	9	Operations

A.1.4 INFORMATION ON BENCHMARKING EXERCISE

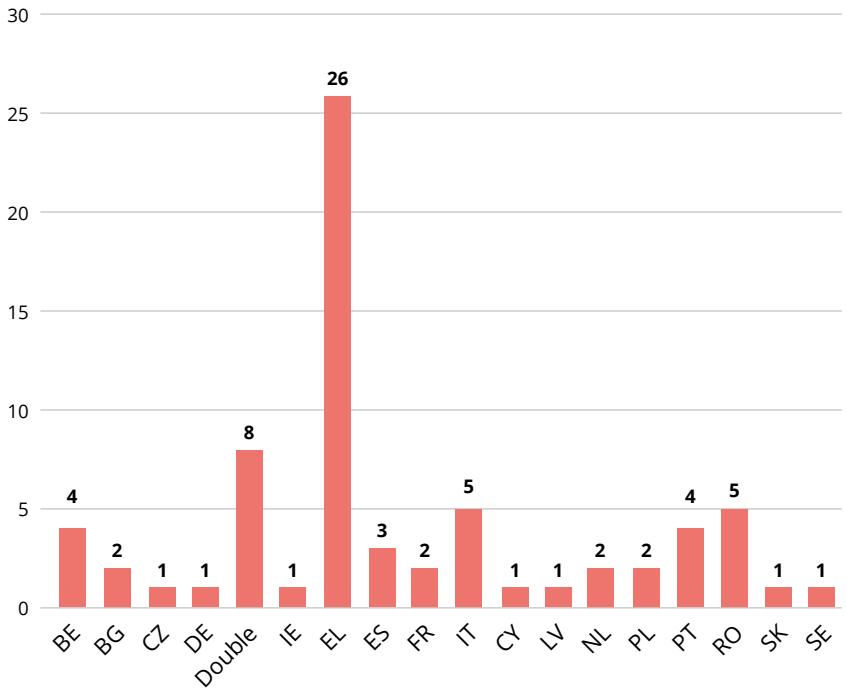
Job type	2018	2017	2016
Total administrative support and coordination	**22.89%**	**19.28 %**	**19.04 %**
Administrative support	19.28%	15.66 %	15.47 %
Coordination	3.61%	3.61 %	3.57 %
Total operational	**62.65%**	**66.27 %**	**66.66 %**
Top operational coordination	7.23%	7.23 %	7.14 %
General operational	55.42%	59.04 %	59.52 %
Total neutral	**14.46**	**14.46 %**	**14.29 %**
Finance and control	14.46%	14.46 %	14.29 %

The benchmarking exercise followed the European Commission's methodology. All the values are within the acceptable values for an agency of ENISA's size (i.e. overhead (administrative support and coordination) is below 25 %).

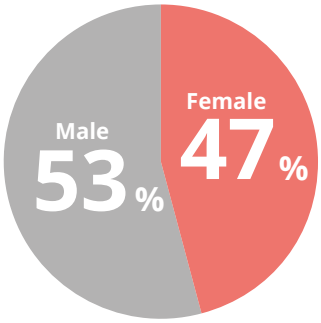
A.1.5 HUMAN RESOURCES STATISTICS

As at 31 December of 2018 the agency comprised of 70 in-house statutory staff.

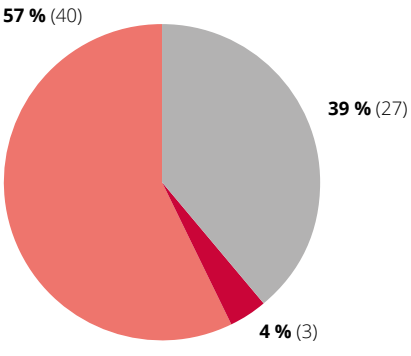
Employees by nationality



Gender distribution – all departments



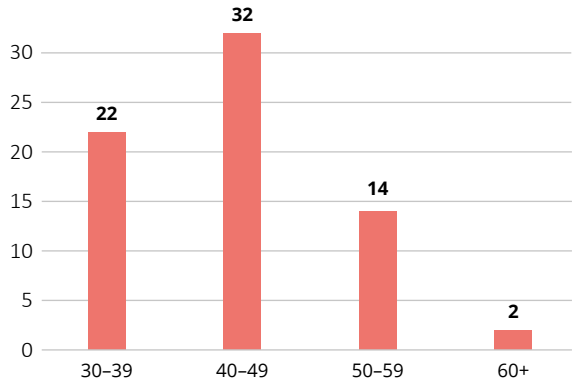
Employees by contract type



Contract type

- Contractual agent
- Seconded national expert
- Temporary agent

Employees by age range



A.1.6 HUMAN RESOURCES BY ACTIVITY

Activities	Planned Full Time Equivalents	Actual Full Time Equivalents
Activity 1 — Expertise: anticipate and support Europe in facing emerging network and information security challenges	14.47	12.55
Activity 2 — Policy: promote network and information security as an EU policy priority	21.58	23.83
Activity 3 — Capacity: support Europe in maintaining state-of-the-art network and information security capacities	14.34	9.97
Activity 4 — Community: foster the emerging European network and information security community	14.22	10.60
Activity 5 — Enabling: reinforce ENISA's impact	19.39	26.30
Total A1-A5	**84.00**	**83.25**

Note: The figures in the table above provide an estimate of the human resources attributed to each of the activities of the agency.

ANNEX 2
FINANCIAL RESOURCES

A.2.1 PROVISIONAL ANNUAL ACCOUNTS 2018

Balance sheet 2017 (in EUR)	2017	2018
NON-CURRENT ASSETS	**657 489**	**672 006**
Intangible assets	107 537	79 844
Tangible assets	549 952	575 662
Guarantee for leased building	–	16 500
CURRENT ASSETS	**1 808 377**	**1 595 549**
Short-term receivables	230 128	62 589
Cash and cash equivalents	1 578 249	1 532 960
ASSETS	**2 465 866**	**2 267 555**
NON-CURRENT LIABILITIES	**–**	**–**
Provisions (long term)	–	–
CURRENT LIABILITIES	**610 130**	**570 855**
European Commission pre-financing received	85 535	110 505
Accounts payable	110 195	54 603
Accrued liabilities	414 400	405 747
LIABILITIES	**670 842**	**679 135**
Accumulated result	1 691 055	1 855 736
Surplus/(Deficit) for the year	164 681	– 159 036
NET ASSETS	**1 855 736**	**1 696 700**

Statement of financial performance 2017 (in EUR)	2017	2018
OPERATING REVENUES	**11 187 610**	**11 420 540**
Revenue from the European Union subsidy	10 489 442	10 667 121
Revenue from administrative operations	698 168	753 419
OPERATING EXPENSES	**– 11 019 518**	**– 11 577 774**
Administrative expenses	– 8 808 548	– 9 430 560
Operational expenses	– 2 210 970	– 2 147 214
OTHER EXPENSES	**– 3 411**	**– 1 802**
Financial expenses	– 3 399	– 1 113
Exchange-rate loss	– 12	– 689
ECONOMIC RESULT FOR THE YEAR	**164 681**	**-159 036**

Remark: The figures included in the tables **Balance sheet** and **Statement of financial performance** are provisional, since they are, as of the date of the preparation of the annual activity report, still subject to audit by the ECA. It is thus possible that amounts included in these tables may have to be adjusted before the final accounts are adopted (deadline 1 July 2018).

A.2.2 FINANCIAL REPORTS 2018

Out-turn on commitment appropriations in 2018				
Chapter		**Commitment appropriations authorised ***	**Commitments made**	**%**
		1	**2**	**3=2/1**
Title A-1 STAFF				
A-11	Staff in active employment	5 443 399.01	5 443 399.01	100.00 %
A-12	Recruitment expenditure	384 922.68	384 922.68	100.00 %
A-13	Socio-medical services and training	74 541.43	74 541.43	100.00 %
A-14	Temporary assistance	1 331 330.08	1 331 330.08	99.87 %
Total Title A-1		**7 234 193.20**	**7 234 193.20**	**99.98 %**
Title A-2 FUNCTIONING OF THE AGENCY				
A-20	Buildings and associated costs	882 096.06	882 096.06	100.00 %
A-21	Movable property and associated costs	29 882.44	29 882.44	100.00 %
A-22	Current administrative expenditure	75 932.02	75 932.02	100.00 %
A-23	Information and communication technologies	600 632.19	600 519.62	99.98 %
Total Title A-2		**1 588 542.71**	**1 588 430.14**	**99.99 %**
Title B-3 OPERATING EXPENDITURE				
B-30	Group activities	672 587.53	672 570.00	99.99 %
B-32	Horizontal operational activities	367 322.84	367 256.58	99.98 %
B-36	Core operational activities	1 663 063.11	1 663 063.11	100.00 %
Total Title B-3		**2 702 973.48**	**2 702 889.69**	**99.99 %**
TOTAL ENISA		**11 525 709.39**	**11 523 957.73**	**99.98 %**

* Commitment appropriations authorised include, in addition to the budget voted by the budgetary authority, appropriations carried over from the previous exercise, budget amendments and miscellaneous commitment appropriations for the period (e.g. internal and external assigned revenue).

Out-turn on payment appropriations in 2018				
Chapter		**Payment appropriations authorised ***	**Payments made**	**%**
		1	**2**	**3=2/1**
Title A-1 STAFF				
A-11	Staff in active employment	5 443 399.01	5 443 399.01	100.00 %
A-12	Recruitment expenditure	384 922.68	347 843.96	90.37 %
A-13	Socio-medical services and training	74 541.43	42 122.81	56.51 %
A-14	Temporary assistance	1 331 330.08	871 665.82	65.47 %
Total Title A-1		**7 234 193.20**	**6 705 031.60**	**92.69 %**
Title A-2 FUNCTIONING OF THE AGENCY				
A-20	Buildings and associated costs	882 096.06	821 404.65	93.12 %
A-21	Movable property and associated costs	29 882.44	20 100.36	67.26 %
A-22	Current administrative expenditure	75 932.02	66 718.69	87.87 %
A-23	Information and communication technologies	600 632.19	356 578.80	59.37 %
Total Title A-2		**1 588 542.71**	**1 264 802.50**	**79.62 %**
Title B-3 OPERATING EXPENDITURE				
B-30	Group activities	672 587.53	589 817.36	87.69 %
B-32	Horizontal operational activities	367 322.84	212 521.71	57.86 %
B-36	Core operational activities	1 663 063.11	1 519 521.16	91.37 %
Total Title B-3		**2 702 973.48**	**2 321 860.23**	**85.90 %**
TOTAL ENISA		**11 525 709.39**	**10 291 694.33**	**89.29 %**

* Payment appropriations authorised include, in addition to the budget voted by the budgetary authority, appropriations carried over from the previous exercise, budget amendments and miscellaneous payment appropriations for the period (e.g. internal and external assigned revenue).

Breakdown of commitments to be settled on 31. 12. 2018					
Chapter		2018 commitments to be settled			
		Commitments in 2018	Payments in 2018	RAL 2018	% to be settled
		1	2	3 = 1 – 2	4 = 3/1
Title A-1 STAFF					
A-11	Staff in active employment	5 443 399.01	– 5 443 399.01	0.00	0.00 %
A-12	Recruitment expenditure	384 922.68	– 347 843.96	37 078.72	9.63 %
A-13	Socio-medical services and training	74 541.43	– 42 122.81	32 418.62	43.49 %
A-14	Temporary assistance	1 331 330.08	– 871 665.82	458 108.96	34.45 %
Total Title A-1		**7 234 193.20**	**– 6 705 031.60**	**527 606.30**	**7.29 %**
Title A-2 FUNCTIONING OF THE AGENCY					
A-20	Buildings and associated costs	882 096.06	– 821 404.65	60 691.41	6.88 %
A-21	Movable property and associated costs	29 882.44	– 20 100.36	9 782.08	32.74 %
A-22	Current administrative expenditure	75 932.02	– 66 718.69	9 213.33	12.13 %
A-23	Information and communication technologies	600 632.19	– 356 578.80	243 940.82	40.62 %
Total Title A-2		**1 588 542.71**	**– 1 264 802.50**	**323 627.64**	**20.37 %**
Title B-3 OPERATING EXPENDITURE					
B-30	Group activities	672 587.53	– 589 817.36	82 752.64	12.30 %
B-32	Horizontal operational activities	367 322.84	– 212 521.71	154 734.87	42.13 %
B-36	Core operational activities	1 663 063.11	– 1 519 521.16	143 541.95	8.63 %
Total Title B-3		**2 702 973.48**	**– 2 321 860.23**	**381 029.46**	**14.10 %**
TOTAL ENISA		**11 525 709.39**	**– 10 291 694.33**	**1 232 263.40**	**10.69 %**

* Commitment and payment appropriations authorised include, in addition to the budget voted by the budgetary authority, appropriations carried over from the previous exercise, budget amendments and miscellaneous payment appropriations for the period (e.g. internal and external assigned revenue).

Situation on revenue and income in 2018					
Title	**Description**	**Year of origin**	**Revenue and income recognised**	**Revenue and income cashed in 2018**	**Outstanding balance**
9000	SUBSIDY FROM THE EU GENERAL BUDGET	2018	10 777 626.00	10 777 626.00	0.00
9200	Subsidy from the Ministry of Transports of Greece	2018	685 661.79	685 661.79	0.00
9300	REVENUE FROM ADMINISTRATIVE OPERATIONS	2018	115 307.40	115 307.40	0.00
TOTAL ENISA			**11 578 595.19**	**11 129 227.09**	**45 998.40**

Average payment time for 2018							
Average payment time for 2018	**Total number of payments**	**Within time limit**	**Percentage**	**Average payment time**	**Late payment**	**Percentage**	**Average late-payment time**
14.11 days	2 021	1 862	92.13 %	14.11 days	159	7.87 %	41.12 days

ANNEX 3
OTHER ANNEXES

A.3.1 LIST OF ACRONYMS AND INITIALISMS

AD: administrator

AST: assistant

CA: contract agent

CEP: cyber exercise platform

CERT-EU: Computer Emergency Response Team for the EU institutions, bodies and agencies

CIIP: critical information infrastructure protection

CSIRT: computer security incident response team

DPA: data protection authority

DSP: digital service provider

ECA: European Court of Auditors

ECSC: European Cyber Security Challenge

ECSM: European Cyber Security Month

EDPS: European Data Protection Supervisor

EFTA: European Free Trade Association

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

ENISA: European Union Agency for Network and Information Security

ETL: ENISA threat landscape

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

FI-ISAC: Financial Institutes — Information Sharing and Analysis Centre

FIRST: Forum of Incident Response and Security Teams

GDPR: general data protection regulation

HoD: head of department

HoU: head of unit

IAS: Internal Audit Service

ICS: internal control standard

ICT: information and communications technology

IoT: internet of things

ISAC: information sharing and analysis centre

ISO: information security officer

IT: information technology

LEA: law enforcement agency

NCA: national competent authority

NCSS: national cybersecurity strategy

NIS: network and information security

NIS CG: NIS Cooperation Group

NLO: national liaison officer

NRA: national regulatory authority

OES: operator of essential services

PETs: privacy-enhancing technologies

PSD2: second payment services directive

SNE: seconded national expert

SOG-IS MRA: Senior Officials Group Information Systems Security Mutual Recognition Agreement

RD: Resources Department

TA: temporary agent

TF-CSIRT: Task Force on Computer Security Incident Response Teams

TRANSITS: computer-security and incident-response team personnel training

A.3.2 LIST OF POLICY REFERENCES

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

Reference	Policy/legislation reference — Complete title and link
2018	
Work programme 2017	ENISA Programming Document 2018-2020 Including multiannual planning, 2018 work programme and multiannual staff planning, available at: https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2018-2020
2017	
Work programme 2017	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), available at: https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2017-2019-with-amendments
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
Cybersecurity act, 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
2016	
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, pp. 1-30, 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 July 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 at (including link to the Annex): 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, pp. 1-88, available at: http://data.europa.eu/eli/reg/2016/679/oj

Reference	Policy/legislation reference — Complete title and link
LEA 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, pp. 89-131, 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, pp. 132-149, 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, 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, pp. 35-127, 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, pp. 73-114, available at: http://data.europa.eu/eli/reg/2014/910/oj
Communication on 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
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, 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, pp. 41-58, 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, pp. 8-14, 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, pp. 42-68, http://data.europa.eu/eli/reg_del/2013/1271/oj

Reference	Policy/legislation reference — Complete title and link
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, pp. 2-8, 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 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), available at: 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, pp. 1-17, (consolidated version, after amendments), available at: http://data.europa.eu/eli/reg/2011/1077/2015-07-20
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
Telecom Ministerial Conference on CIIP	Telecom Ministerial Conference on CIIP organised by the Presidency in Balatonfüred, Hungary, 14 and 15 April 2011
2010	
Internal security strategy for the European Union	An internal security strategy for the European Union (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

Reference	Policy/legislation reference — Complete title and link
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, pp. 1-4, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex %3A32009G1229(01)
2002	
Framework directive 2002/21/EC as amended	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, pp. 33-50 (consolidated version, after amendments), available at: http://data.europa.eu/eli/dir/2002/21/2009-12-19
E-privacy directive 2002/58/EC as amended	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, pp. 37-47, (consolidated version, after amendments), available at: http://data.europa.eu/eli/dir/2002/58/2009-12-19

TP-AB-19-001-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at 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 978-92-9204-297-4