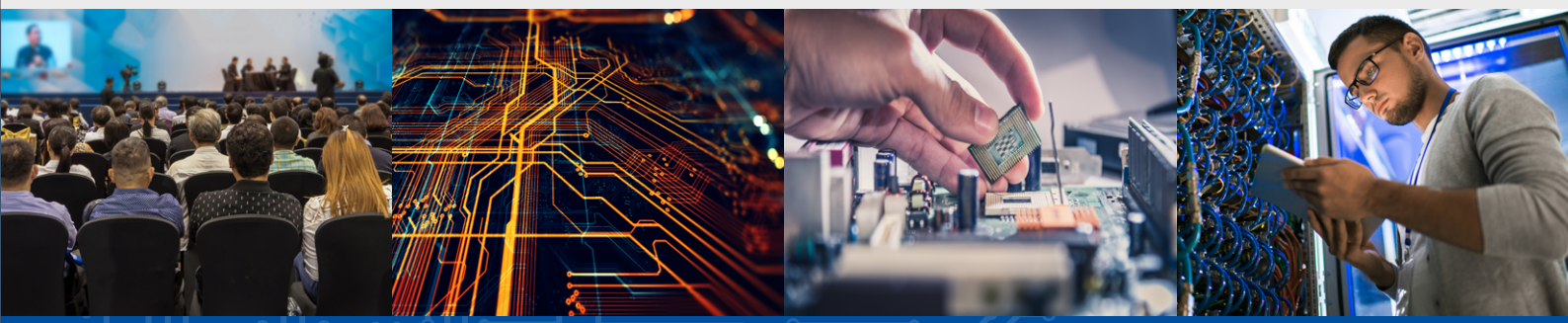
enisa

THE EU CYBERSECURITY AGENCY

ANNUAL ACTIVITY REPORT



2017

CONTACT

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

Luxembourg: Publications Office of the European Union, 2018

Print	ISBN 978-92-9204-254-7	ISSN 1830-981X	doi:10.2824/010905	TP-AB-18-001-EN-C
PDF	ISBN 978-92-9204-220-2	ISSN 2314-9434	doi:10.2824/558297	TP-AB-17-001-EN-N

ANNUAL ACTIVITY REPORT 2017

EUROPEAN UNION AGENCY FOR
NETWORK AND INFORMATION SECURITY

ENISA MANAGEMENT BOARD ASSESSMENT

THE ANALYSES AND ASSESSMENT BY THE MANAGEMENT BOARD OF ENISA OF THE CONSOLIDATED ANNUAL ACTIVITY REPORT FOR THE YEAR 2017 OF THE AUTHORISING OFFICER OF ENISA

The Management Board takes note of the Annual Activity Report (AAR) for the financial year 2017, submitted by the Executive Director of the European Union Agency for Network and Information Security (ENISA) in accordance with Article 47 of the Financial Regulation applicable to ENISA.

The Management Board received a copy of the 207 Annual Activity Report produced by the Executive Director of ENISA in his quality of Authorising Officer for the implementation of the annual budget on 13 June 2018.

In analysing and assessing the AAR 2017, the Management Board makes the following observations:

- The AAR presents key results of the implementation of the ENISA Work programme 2017 and leads to conclusion that the Agency completed all deliverables agreed with the Management Board both within time and within budget.

- ENISA produced 43 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 2017, against the framework of the ENISA Strategy 2016–2020.

- At the same time, the benefits of ENISA's work in the context of the security of network and information systems directive (NIS directive) [1] was observed even before the deadline for its transposition into national law of May 2018. In 2017, ENISA delivered important results in the context of activities regarding the implementation of the NIS directive. An important element of the NIS directive and of capacity building across the EU is the 'Reference security incident classification taxonomy', which was agreed upon by ENISA and the European CSIRT community.

- 2017 was a year in which the previous work and impact of ENISA was reviewed by external consultants. The successful outcome of this review was presented in the Cybersecurity package [2], which includes a communication renewing the EU cybersecurity strategy and the draft cybersecurity act. The draft cybersecurity act covers (i) a proposal for a renewed mandate for a stronger ENISA to serve the cybersecurity needs of Europe and (ii) a cybersecurity certification framework proposal.

- In 2017 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 and regional organisations. Following on from last year's tradition, ENISA organised several high-profile events such as the workshop during the 2017 EU Cybersecurity Conference in Tallinn, in collaboration with the Estonian Presidency, two editions of the ENISA Industry Event and the Annual Privacy Forum. ENISA also hosted 14 important thematic workshops and sessions, gathering together experts in the field to discuss cybersecurity topics.

1 Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union.

2 https://ec.europa.eu/digital-single-market/en/policies/cybersecurity#usefullinks

- 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 and school pupils from different Member States.

- In 2017 ENISA received the EU Ombudsman Award for Good Administration for Excellence in Innovation – Transformation.

- Overall, the AAR is in line with the ENISA Work Programme 2017 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 2017 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 99.99 %. The respective payment rate on expenditure appropriations was 88.19 % in 2017. This section also describes that the agency performed the 'job screening' benchmarking exercise for 2017. Support functions represents 19.28 % of the total statutory staff count, which is below the 25 % maximum value accepted for the European Union agencies.

- The AAR also provides a follow up of the 2015 Discharge, and control results. The agency had no open recommendations from the Internal Audit Service in 2017. This section also notes the main categories of deviation that led to exceptions reported. In 2017 the agency recorded 31 exceptions. 25 of them are under the materiality levels and are minor administrative mistakes. Of the six remaining, three a posteriori commitments were reported, two were late payments to the European Commission and the last was a purchase order on which the amount exceeded the limit.

- 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 2017. In the view of the Management Board, the overall performance and quality of the outputs was high. The Management Board notes with satisfaction that ENISA could deliver work programme 2017 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 2017 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

A MESSAGE FROM THE EXECUTIVE DIRECTOR

I am pleased to report another successful year for the European Union Agency for Network and Information Security (ENISA); 2017 brought good news for our future.

On 13 September 2017 the Commission adopted a cybersecurity package [3], which includes a communication renewing the EU cybersecurity strategy and the draft cybersecurity act. The package builds upon existing instruments and presents new initiatives to further improve EU cyber resilience and response. The draft cybersecurity act covers (i) a proposal for a renewed mandate for a stronger ENISA to serve the cybersecurity needs of Europe and (ii) a cybersecurity certification framework proposal. The proposed act promotes a permanent and updated mandate for the agency, which has now been given political support at the highest level with the adoption of the Council conclusions.

2017 was also a year in which the previous work and impact of ENISA was reviewed by external consultants. The successful outcome of this review supports and is evidence of what we all believed, namely that ENISA has made a positive contribution to cybersecurity in Europe over the last several years.

The success of our agency is built on the efforts, dedication and commitment of all staff members, on the stimulating collaboration with its stakeholders and on the effective strategic cooperation with the Management Board. I would like to take this opportunity to thank all of them for their significant contributions and efforts in 2017.

ENISA reached its main objective in 2017: it successfully completed the work programme in a timely manner and within the constraints of its budget. Please find in the introduction section a summary with highlights of ENISA activities during 2017, and in the next sections details on how they were carried out.

In the broader context, more work is required to secure cyberspace and guarantee a safe and secure digital economy for EU citizens.

3 https://ec.europa.eu/digital-single-market/en/policies/cybersecurity#usefullinks

During 2017 we witnessed several large-scale ransomware attacks that affected critical functions of our society such as hospitals and transportation. At the same time, the materialisation of internet of things (IoT) attacks has given a further demonstration of the potential damage that can result from malevolent manipulation of this technology.

More work is required to address these new challenges. At the same time, we are also seeing the benefits of the work in the context of the security of network and information systems directive (NIS directive) [4] emerging even before the deadline for its transposition into national law of May 2018. In 2017 ENISA delivered important results in the context of activities regarding the implementation of the NIS directive. For instance, ENISA produced a number of deliverables supporting the work streams established in the Cooperation Group [5], namely incident notification, baseline security measures and identification of operators of essential service provides.

As we look towards the future, there is no doubt that 2018 will be a challenging year. With our staff and our stakeholders we will support the implementation of the renewed EU cybersecurity strategy while looking forward to the adoption of the proposed cybersecurity act.

I believe in the future of ENISA, and I am looking forward to the proposed new stronger ENISA and to the agency playing its role in the safe EU cyberspace of tomorrow.

Udo Helmbrecht
Executive Director, European Union Agency for Network and Information Security

4 Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union.

5 The official body providing guidance on the EU-wide efforts related to the implementation of the NIS directive.

INTRODUCTION

THE EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY IN BRIEF

The European Union Agency for Network and Information Security (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.

In 2017 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 and regional organisations. Regular meetings with various Commission services, and with the Directorate-General for Communications Networks, Content and Technology in particular, took place during the year.

THE YEAR IN BRIEF

The key achievements of 2017 are as follows.

- ENISA produced 43 reports on different aspects of NIS. These include the latest version of the ENISA threat landscape, guidelines and best-practice recommendations regarding privacy-enhancing technologies. Additionally, ENISA reports focused on issues including but not limited to security and privacy in mobile environments, standardisation (including aspects of the eIDAS regulation [6] and the emerging area of certification of products.

6 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.

- ENISA initiated the process of assisting Member States in implementing the security of network and information systems directive (NIS directive), the first piece of EU-wide legislation on cybersecurity that provides legal measures to boost the overall level of cybersecurity in the EU.

- As defined by the NIS directive, in its role as secretariat of the computer security incident response teams (CSIRTs) network, ENISA has engaged all 28 EU Member States and their designated CSIRTs, together with EU institutions, in the development of rules and procedures on implementing the NIS directive by supporting operational cooperation among EU Member States during cyber crises such as WannaCry and NotPetya, supporting working groups and dedicated meetings.

- ENISA supported the organisation of CSIRTs network meetings, including the first meeting in Malta, the second in Estonia and the third in Greece. The third meeting took place at the campus of ENISA's headquarters in Heraklion, Greece, and saw the participation of CSIRT representatives from all EU Member States, the European Commission and the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU).

- An important element of the NIS directive and of capacity building across the EU is the 'Reference security incident classification taxonomy', which was agreed upon by ENISA and the European CSIRT community.

- Following on from last year's tradition, ENISA organised several high-profile events such as the workshop during the 2017 EU Cybersecurity Conference in Tallinn, in collaboration with the Estonian Presidency, two editions of the ENISA Industry Event and the Annual Privacy Forum. ENISA also hosted 14 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 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 and school pupils from different Member States.

- Finally, ENISA compiled a data breach severity assessment tool, in close collaboration with several Member States' data protection authorities, with the aim of setting up a coherent framework at EU level.

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 2017 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), incident reporting, eIDAS regulation, privacy and trust. 2017 was a year that saw ENISA supporting the implementation of the NIS directive in regard to baseline security measures, incident reporting and the identification of criteria for operators of essential services (OES). The agency also supported the Member States and the European Commission on the NIS directive provisions related to digital service providers.

Key achievements include the following.

- In the context of the NIS directive, the agency produced a number of deliverables supporting the work of the respective working streams established within the Cooperation Group, namely incident notification, baseline security measures and the identification of OES (see performance indicator for outputs O.1.1.1, O.2.2.2 and O.2.2.6).

- In supporting the implementation of the NIS directive ENISA also engaged 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 is 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).

- As part of its activities to develop baseline security recommendations for the IoT in the context of critical information infrastructure, ENISA organised together with Europol an IoT Security conference that was attended by over 250 participants and achieved significant visibility in the community. Also, more than 30 IoT stakeholders and experts were involved in the relevant study, including the ENISA IoT Security Experts Group and the European Commission's DG Communications Networks, Content and Technology (see performance indicator for output O.1.1.2).

- ENISA published a study to promote the uptake of cyber insurance by assessing the level of harmonisation of the risk assessment language in cyber insurance and supporting further convergence in the industry. The study has been widely referenced and the recommendations have been adopted by associations promoting harmonised wordings. The respective validation workshop received significant visibility and was attended by over 50 participants, including 24 insurance companies and 41 companies from 14 Member States overall, while a total of 51 insurance carriers, brokers and reinsurers from 12 Member States participated in the study (see performance indicator for output O.3.3.2).

- ENISA supported the Member States in the development and assessment of national cybersecurity strategies (NCSS) and updated the EU NCSS map. The new version of the map was built on the work performed in previous years and presents the Member States' strategic objectives and good practices in a simple and user-friendly manner. In addition, ENISA, in cooperation with the Dutch National Cyber Security Centre, organised a workshop in The Hague attended by more than 40 public and private stakeholders. Overall, 18 Member States participated in the activities of the agency regarding this output (see performance indicator for output O.3.1.3).

- For the sixth year, ENISA published its annual report on significant outage 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 authorities (NRAs) of the different EU Member States (see performance indicator for output O.1.2.2).

- Based on the significant incidents reported by the supervisory bodies of the different EU Member States, ENISA produced the first annual incident analysis report for trust service providers in the EU under Article 19 of the eIDAS regulation (Regulation (EU) No 910/2014). This report also placed emphasis on the analysis of the recently established incident-reporting procedure itself in an effort to highlight its peculiarities.

- More than 100 participants in the 2017 Annual Privacy Forum: (researchers, policymakers and industry participants).

Key conclusions on the effectiveness of the internal control systems and financial management

ENISA has consolidated internal control standards (ICS), based on international good practice, that aim to ensure that policy and operational objectives are achieved within the applicable legal and financial framework.

As regards financial management, compliance with these standards is compulsory and the agency consistently meets its goals in full.

The agency has put in place an organisational structure and a set of internal controls that are suited to the achievement of policy and control objectives, are in accordance with the standards and are suitable for mitigating risks associated with the environment in which it operates.

The current set of 16 ICS lays 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.

In 2017 the agency focused on compliance with the standards that were identified as areas of concern during the risk assessment exercise and on the recommendations raised by the auditing bodies (the Internal Audit Service of the European Commission (IAS) and the European Court of Auditors (ECA)). The agency continues to enjoy full compliance without audit observation and/or audit qualifications.

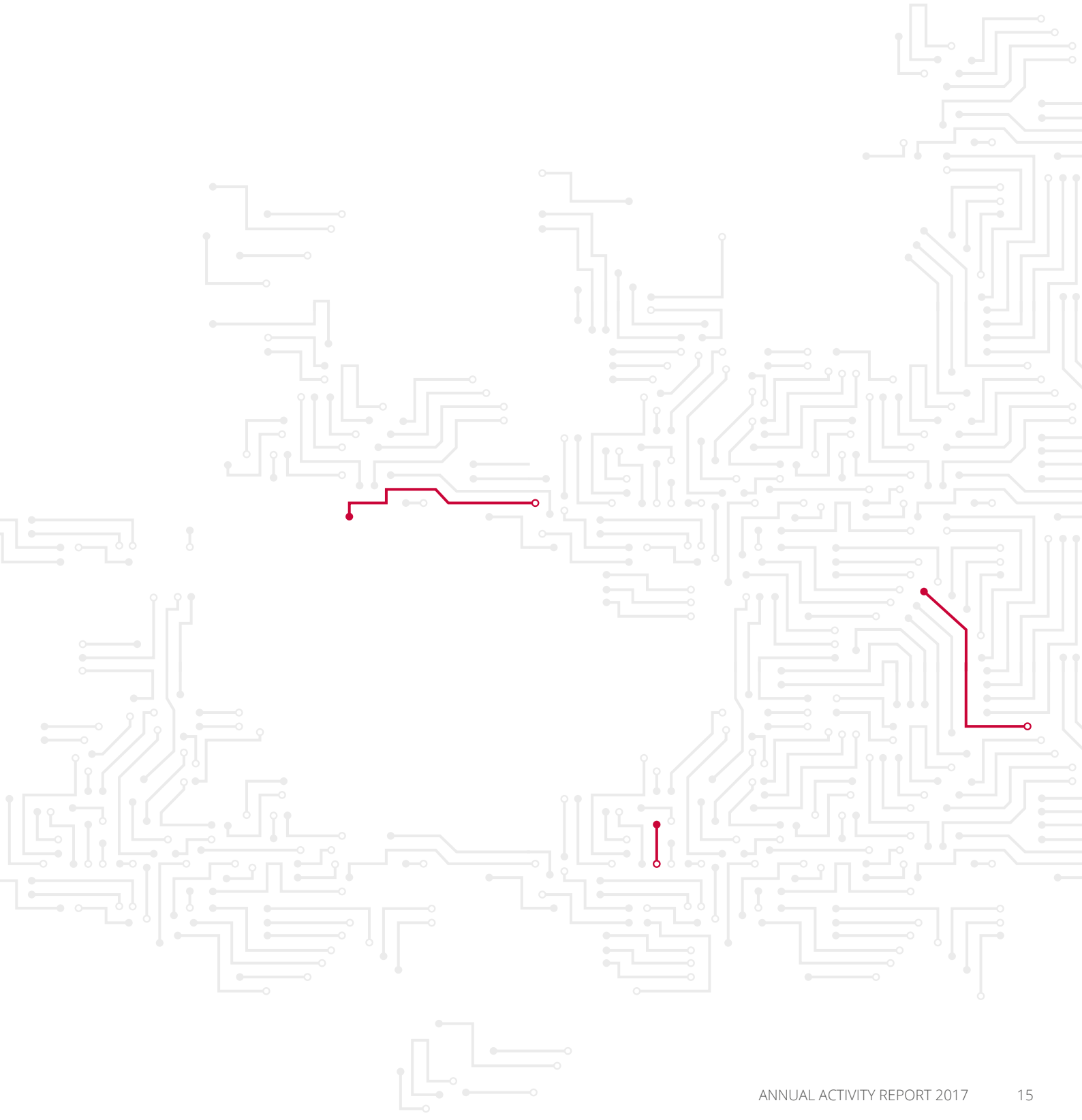
Notable internal and external events

2017 will stay in cybersecurity history as the year of ransomware: the year saw large-scale ransomware attacks that affected critical functions of our society such as hospitals and transportation. At the same time, the materialisation of IoT attacks gave a further demonstration of the potential resulting from manipulation of this technology. Some further highlights of the year related to cybersecurity were as follows.

- 2017 was a pivotal year regarding the implementation of NIS directive. Member States used the platform offered by the Cooperation Group to discuss good practices relevant to the transposition of the directive into national law with a view to achieving a higher level of convergence as the transposition deadline of May 2018 draws closer.
- The year witnessed several highly publicised IoT security attacks on both commercial products and critical infrastructure, thus raising relevant concerns and leading to calls for action towards stronger cybersecurity for connected objects, as clearly indicated in the mid-term review of the digital single market.
- 2017 was a year in which the operational cooperation of the CSIRTs network was tested during cyber crises such as WannaCry and NotPetya. The CSIRTs network proved its readiness and ability to cooperate during large-scale security incidents in the EU.

As underlined by the latest ENISA threat landscape, 2017 was the year in which incidents in the cyberthreat landscape led to the definitive recognition of some omnipresent facts. The agency gained specific evidence regarding monetisation methods, attacks on democracies, cyberwar, the transformation of malicious infrastructure and the dynamics within threat-agent groups. At the same time a lot of successful operations against cybercriminals were launched. Law enforcement, governments and vendors managed to shut down illegal dark markets, deanonymise the darknet and arrest prominent cybercriminals. Moreover, state-sponsored campaigns were revealed and details of technologies deployed by nation states were leaked.

Nonetheless, despite law enforcement activities and capability building, the cybersecurity market is failing: implemented measures and increased investment have not yet brought a decline in successful incidents. The cybersecurity community — with the support of ENISA — has to continue its fight against cybercrime in a coordinated manner. Cybersecurity skill shortage is aggravating the race towards inverting current cyber-incident trends.



PART I

ACHIEVEMENTS IN THE IMPLEMENTATION OF THE 2017 WORK PROGRAMME

This *Consolidated annual activity report 2017* follows the structure of the amended [7] 2017 ENISA work programme to assist the reader in understanding the achievements of the year. The 2017 work programme was aligned with the structure of the ENISA strategy document [8], 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 [9]. This strategy defines five strategic objectives that form the basis of future multiannual plans [10].

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 Union 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 2017 work programme are presented for each of the abovementioned activities.

7 The work programme was amended in September 2017 to address the changes in ENISA's activities linked to the agency's new role as defined in the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) regulation.

8 *ENISA strategy 2016-2020*, available at: https://www.enisa.europa.eu/publications/corporate/enisa-strategy

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

10 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. Annual specific 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.

After the description of the specific results for each activity and output, the achievements against indicators and the detailed results for each output are presented in tables.

Furthermore, the 2016 work programme impact indicators for which a target value was set for 2017 or 2018 have been included in Section 2.6 to follow up their result and impact. These can only be measured in the medium and long term.

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 critical information infrastructure

1.1.1.1 Output O.1.1.1 — Baseline security recommendations for the operators of essential services sectors

The key objective of this output was to assist the Member States by providing guidance and supporting material on the implementation of Articles 14(1) and (2) of the NIS directive, which refer to measures with a view to achieving a high common level of NIS security within the EU. ENISA achieved this objective by engaging with the NIS directive Cooperation Group and private stakeholders and by leveraging its existing knowledge and expertise in the area of standards and good practices on security measures and risk assessment.

Specifically, the agency supported the Cooperation Group by collecting and analysing the current and often common approaches to the security measures of OES. The outcome of these activities significantly helped the Cooperation Group to produce a reference document with security measures for public and private actors to improve their cybersecurity. All 28 Member States and 17 OES from various essential sectors were engaged in the development of baseline security requirements for OES. A workshop for the energy sector was held in Athens in September and was attended by representatives of 14 Member States and 21 OES.

Finally, ENISA provided detailed examples of implementation, lists and mapping tables of standards and good practices on risk-assessment and risk-management methodologies relevant to these security measures.

1.1.1.2 Output O.1.1.2 — Baseline security recommendations for IoT in the context of critical information infrastructure

ENISA defines the IoT as a cyber-physical ecosystem of interconnected sensors and actuators, which enables intelligent decision-making. With a great impact on citizens' safety, security and privacy, the IoT threat landscape is extremely complex. Therefore, it is important to understand what exactly needs to be secured and to implement specific security measures to protect the IoT from cyberthreats. The 2017 ENISA report on IoT cybersecurity provides experts, developers, manufacturers, decision-makers and security personnel with a guide to good practices and recommendations on preventing and mitigating cyberattacks against the IoT. This report lists the sensitive assets present in the IoT, as well as the corresponding threats, risks, attack scenarios, mitigation factors and possible security measures to implement. More than 30 IoT stakeholders and experts from more than 10 Member States were involved in the study, including the ENISA IoT Security Experts Group and DG Communications Networks, Content and Technology. Moreover, more than 250 participants attended the IoT Security conference that ENISA organised together with Europol in October. The deployment of baseline security recommendations into the IoT ecosystem will be critical to the proper functioning of these devices by mitigating and preventing cyberattacks. The March 2018 UK government report *Secure by design: improving the cybersecurity of consumer internet of things* took stock of the ENISA study on baseline security recommendations, along with several other ENISA studies, for example on smart cars, airports and hospitals. ENISA received an invitation to and presented the *Baseline security recommendations for IoT* study at the Mobile World Congress 2018 in Barcelona, an event that attracted more than 107 000 participants.

1.1.2 Objective 1.2. NIS threat landscape and analysis

1.1.2.1 Output O.1.2.1 — Annual ENISA threat landscape

The ENISA threat landscape (ETL) report enjoys major attention within Member States and the Commission, and also among experts and lay communities. This objective follows up on past achievements to deliver an overview of the cyberthreat landscape, along with a series of related information. This material seeks to be very comprehensive.

In 2017 the ETL was further developed to include more interactive elements both in the presentation and in the dissemination of related information.

The impact of the ENISA TL is varied.

- It is used as a consolidated summary of existing material in the area of cyberthreats.
- It provides strategic and tactical information that can be used within security-management tasks.
- It can be imported into risk-management methods.
- It can be used as basis for building up threat intelligence.
- It can be used for training purposes.
- The ENISA collection and analysis process can be used by other organisations to create their own threat landscapes.

In 2017 the team developing the ETL organised the first European event in the area of cyberthreat intelligence to address challenges and open issues in the related community. The success of the event has exceeded expectations by having some 150 participants who delivered vivid discussions and a comprehensive exchange of knowledge and ideas.

The ETL provides information regarding reduction of threat exposure. This information consists of available controls that can reduce the exposure and consequently mitigate the resulting risks. In addition to the report the agency made available to the public all relevant material as it was collected during the year.

In carrying out this work, synergies with related experts (i.e. the ENISA TL Stakeholder Group) and vendors have been exploited. The agency will invest in visualisation and quick availability of the resulting material.

In 2017 the ENISA threat landscape was accompanied by an end-user application (a web application available at https://etl.enisa.europa.eu) that will provide available information online. In this manner ETL users will be in the position to access ENISA threat information on a permanent basis. This platform may be used to integrate additional relevant information.

The ETL continues to be a key deliverable. It has been referenced by stakeholders from all Member States. Several thousand downloads and several hundred references have been made. Moreover, various articles have reported on ENISA TL findings.

As an indicator, the ETL has achieved following impact.

- ENISA threat landscape is cited in the UK cybersecurity strategy.
- ENISA threat landscape is mentioned in a Commission fact sheet about cybersecurity.
- ENISA threat landscape delivers input for topics under the Horizon 2020 programme.
- ENISA threat landscape information is being used by the Council to raise awareness.
- ENISA threat landscape is used as material for cybersecurity courses in universities.
- ENISA threat landscape is cited on Wikipedia.

The ETL continues to be a key deliverable. It has been referenced by stakeholders from all Member States. Several thousand downloads and several hundred references have been made.

1.1.2.2 Output O.1.2.2 — Annual incident analysis report for the telecom sector (Article 13a)

For the sixth year, ENISA published its annual report on significant outage 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 NRAs of the different EU Member States. The 2017 report covers the incidents that occurred in the previous year and gives an aggregated analysis of the incident reports about severe outages across the EU.

Some key findings from the 158 major incidents reported include the identification of mobile internet as the service most affected by such outages and system failures as the dominant root cause of incidents.

The annual incident analysis report is compiled based on the data provided by Member States. In order to facilitate collection and strengthen the relationship

with NRAs, ENISA organised three meetings during the year, attended by almost all EU NRAs. The agency also developed an online tool so Member States can submit their incidents online.

1.1.2.3 Output O.1.2.3 — Annual incident analysis report for trust service providers (Article 19)

This report provides an analysis and evaluation of the incident-reporting procedure in the EU under Article 19 of the eIDAS regulation. Considering the fact that incident reporting was only implemented as from the second half of 2016, and moreover that this was the first time that supervisory bodies had performed this exercise, only one incident was notified to ENISA. Future incidents reported under the provisions of Article 19, especially those with cross-border impact, could potentially have a highly damaging impact. Therefore, ENISA is paying a lot of attention to the particularities of Article 19-related incidents, as even apparently non-critical incidents can create significant impact across multiple Member States.

In order to facilitate this process ENISA manages a subject-matter expert group from the authorities from most of the Member States. The group meets twice a year to debate the incidents, along with other topics.

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 ICT security

This activity provided an assessment of the situation of European standardisation in the area of ICT security, taking into account the new requirements and priorities associated with the NIS directive (and with the Commission's communication on the Cybersecurity Public–Private Partnership (cPPP). In addition, the output of European standardisation in the area of trust services was analysed with a view to establishing suitability and coherence with policy goals.

While carrying out this work, ENISA consulted with industry and standards organisations (e.g. the European Telecommunications Standards Institute (ETSI), the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec)) as appropriate, mainly through expertise that was mobilised to produce reports, and standardisation conferences (e.g. ETSI Security Week).

1.1.3.2 Output O.1.3.2 — Priorities for EU research and development

In 2017 ENISA worked closely with the European Cyber Security Organisation and the cPPP on cybersecurity in order to align the work being carried out with the ENISA work programme. In addition, the agency offered support to the National Public Authority Representatives Committee by offering a secretariat function.

Also during the year ENISA looked into current best practices and guidelines for protecting EU systems and networks, and put in place an analysis of areas covered by the NIS directive, such the general data protection regulation and the Commission's decision on the cPPP, and provided guidance on where research and development activities funded in the context of the Horizon 2020 programme, the Connecting Europe Facility (CEF), Training of Network Security Incident Teams Staff and the Gigabit European Academic Network would achieve the greatest impact.

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

The outcomes of the Article 14 requests under policy activity for 2017 are as follows.

- Following a request from the green parties of the European Parliament, a briefing note about artificial intelligence was provided covering different aspects of the impact of this technology, including economic, social and privacy issues. The discussion was continued at the Annual Privacy Forum in Vienna and in subsequent meetings.
- ENISA received a request from the European Commission to study and measure the impact of key reinstallation attack vulnerability in order to provide further advice to citizens. An info note was created giving detailed information about the issue and providing different lines of actuation in order to prevent and mitigate the impact of the vulnerability.

1.1.5 General results: achievement of performance indicators for Activity 1

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 critical information infrastructure		
Output O.1.1.1 — Baseline security requirements for the OES sectors	Engage at least 20 Member States in the development of baseline security requirements for OES. Engage at least 15 private-sector stakeholders in the development of baseline security requirements for OES. More than 10 Member States and 15 OES to participate in the workshops.	28 Member States were engaged in the development of baseline security requirements for OES. 17 private-sector operators from various NIS directive sectors were engaged in the development of baseline security requirements for OES. A workshop for the energy sector was held in Athens in September and was attended by representatives of 14 Member States and 21 OES.
Output O.1.1.2 — Baseline security recommendations for IoT in the context of critical information infrastructure	Engage five leading IoT developers and five leading critical information infrastructure operators from five Member States in the preparation of the study.	12 leading IoT developers and eight leading critical information infrastructure operators from six Member States were engaged in the preparation of the study. Moreover, 32 stakeholders from 10 Member States were involved in the study. More than 250 participants attended the IoT conference that took place in October.
Objective 1.2. NIS threat landscape and analysis		
Output O.1.2.1 — Annual ENISA threat landscape (ENISA TL)	Involvement of at least five representatives from different bodies/Member States in the stakeholder group supporting the preparation of the annual ENISA TL.	12 representatives from different bodies/Member States in the supporting stakeholder group have been involved the preparation of the annual ENISA threat landscape.
Output O.1.2.2 — Annual incident analysis report for the telecom sector (Article 13a)	More than 20 NRAs/Member States to contribute to the preparation of the report.	28 NRAs/Member States contributed to the preparation of the report.
Output O.1.2.3 — Annual incident analysis report for trust service providers (Article 19)	More than 10 supervisory bodies/ Member States to contribute to the preparation of the report.	28 supervisory bodies/Member States contributed to the preparation of the report.
Objective 1.3. Research and development, innovation		
Output O.1.3.1 — Guidelines for European standardisation in the field of ICT security	Participation of at least five representatives of European standards-developing organisations and relevant services of the European Commission in drafting and reviewing the guidelines.	Eight representatives of European standards-developing organisations and relevant services of the European Commission, e.g. DG Communications Networks, Content and Technology, have been actively involved in drafting and reviewing the relevant guidelines.
Output O.1.3.2 — Priorities for EU research and development in the context of the Horizon 2020 programme	Involve at least five representatives from different stakeholders — research, industry, government.	Five representatives from different domains (research, industry, etc.) provided input and the final deliverable had a positive impact.
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/

1.1.6 Specific results: mapping of outputs into papers/publications/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 infrastructure
Output O.1.1.1 — Baseline security recommendations for the OES sectors **Baseline security requirements for OES** The report was published to the Cooperation Group. **Mapping of OES security requirements to specific sectors** https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors
Output O.1.1.2 — Baseline security recommendations for IoT in the context of critical information infrastructure **Baseline security recommendations for IoT** https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
Objective 1.2. NIS threat landscape and analysis
Output O.1.2.1 — Annual ENISA threat landscape **ENISA threat landscape report 2017** https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017
Output O.1.2.2 — Annual incident analysis report for the telecom sector (Article 13a) **Annual incident reports 2016** https://www.enisa.europa.eu/publications/annual-incident-reports-2016
Output O.1.2.3 — Annual incident analysis report for trust service providers (Article 19) **Annual incident analysis report for the trust service providers** https://www.enisa.europa.eu/publications/annual-incident-analysis-report-for-the-trust-service-providers
Objective 1.3. Research and development, innovation
Output O.1.3.1 — Guidelines for European standardisation in the field of ICT security **Improving recognition of ICT security standards** https://www.enisa.europa.eu/publications/improving-recognition-of-ict-security-standards
Output O.1.3.2 — Priorities for EU research and development **Priorities for EU research** https://www.enisa.europa.eu/publications/priorities-for-eu-research
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** 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 AN EU POLICY PRIORITY

1.2.1 Objective 2.1. Supporting EU policy development

ENISA continued to provide the Commission and the Member States with high-quality information, data and advice to support policymaking with an EU dimension.

In the policy development area the agency cooperated with public- and private-sector stakeholders to develop insights, consolidate views and provide recommendations in areas in which the EU takes action to further develop its policy. Examples of such cooperation included the domains of 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 IT security certification

The work of ENISA gained new impetus through the proposed cybersecurity act, which also includes an important component on the EU cybersecurity certification framework. This proposal complements other recent legislative and policy initiatives, such as the NIS directive and the Commission position on the cPPP. The agency is gradually becoming more empowered to continue supporting the Commission and the Member States in identifying a certification framework for ICT security products and services that on the one hand boost competition, and on the

other promote mutual recognition or harmonisation of certification practices up to a certain level. The way conformity assessment is carried out in European certification laboratories was an area of specific policy activity; it complemented involvement with stakeholders in two different certification workshops throughout 2017.

ENISA also reached out, with the discussion on certification, to standardisation organisations (ETSI etc.), ICT certification stakeholders (test labs, certification and accreditation bodies, the Senior Officials Group Information Systems Security, Common Criteria Recognition Arrangement, etc.) and ICT security product users (the European Smart Metering Industry Group, Eurosmart, etc.) as forums to enhance the dialogue around security certification and build upon the existing results these initiatives have developed in the past.

1.2.1.2 Output O.2.1.2 — Restricted: towards a digital single market for high-quality NIS products and services

ENISA conducted a study to perform a thorough mapping of the EU NIS start-up ecosystem in the EU using a multifaceted approach that addressed technology and innovation aspects, the policy and regulatory context and the funding side from a Member State, EU and private-sector perspective in light of the digital single market strategy. The study focused on identifying the opportunities available to EU NIS start-ups and the obstacles potentially hindering their growth prospects. Twenty-four individual start-ups and 10 funding-side organisations (including key venture capitalists and business accelerators) covering 10 sectors participated in the study, either via interviews or by attending the validation workshop.

This report helped ENISA to advise the Commission and Member States in better identifying where efforts should be focused in order to further support NIS innovation within the EU and allow start-ups to reach their full potential by leveraging the opportunities that arise from the digital single market. Start-up Europe, the Commission's initiative designed to connect start-ups, investors, accelerators, entrepreneurs etc., expressed significant interest in the findings and recommendations and has adopted a number of them as guidelines for future activities.

The report proposed guidelines and recommendations to strengthen NIS innovation within the EU, while a workshop was organised and co-hosted by DG Communications Networks, Content and Technology's Start-ups and Innovation Unit to bring together different stakeholders from the NIS start-up ecosystem and present the main findings.

1.2.2 Objective 2.2. Supporting EU policy implementation

1.2.2.1 Output O.2.2.1 — Contribute to EU policy in the area of the electronic communications sector

Since 2011 ENISA has supported work in the area of the electronic communication sector. In this respect, three meetings were organised with the Article 13a Expert Group and one technical project was developed (interconnect security dealing with SS7/Diameter) in 2017. Overall, 38 electronic communications providers and 28 national bodies (NRAs) participated in the study. Since the results of the study are still being debated and validated with the industry and national authorities, the study will be published later in 2018.

A strong relationship has been developed with the Commission and multiple inputs have been provided as regards the development of the new EU Electronic Communications Code. Every year ENISA tackles at least one technical topic, as recommended by Article 13a (e.g. a topic that represents a concern to many authorities across the EU).

In 2017 ENISA also continued its work in the area of privacy in electronic communications (e-privacy) and provided relevant technical opinions on online tracking and relevant user protection mechanisms.

1.2.2.2 Output O.2.2.2 — Develop guidelines for the implementation of mandatory incident reporting

ENISA is an active member of the Cooperation Group, the official body providing guidance on EU-wide efforts related to implementing the NIS directive.

Within the incident notification working stream established within the Cooperation Group, ENISA produced the deliverable *Reference document on incident notification for operators of essential services*, which serves as a main guideline for Member States when addressing the topic of incident notification. The document provides insights on how incident-notification provisions can be implemented at national level, highlights potential discrepancies in terms of incident reporting across different industries and further contributes to EU-wide harmonisation. The work represents a landmark in the work on incident reporting within the NIS directive, as more documents remain to be produced in the next years.

It sets the baseline on further developing incident reporting policies across the Member States.

The document was produced based on input from the Member States and taking into account the previous work done by the agency in the area of telecom and trust service providers. The work in this working stream was coordinated by the Dutch representation in the Cooperation Group. Overall, 49 private stakeholders and 20 public stakeholders contributed to the study.

1.2.2.3 Output O.2.2.3 — Recommendations supporting implementation of the eIDAS regulation

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

Furthermore, ENISA developed a set of recommendations and guidelines addressed to the all the involved stakeholders: trust service providers, supervisory bodies and conformity assessment bodies. More than 20 experts in the area of trust services stakeholders were involved in preparing and validating the reports. The reports were disseminated through different communication channels, with the European Commission's distribution channels being the DG Informatics–Communication and Information Resource Centre for Administrations, Businesses and Citizens mailing list, the Article 19 ENISA Expert Group mailing list and ENISA contacts through 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 Trust Services compliance info day on eIDAS. Moreover, a survey was carried out to examine the implementation and uptake of trust services under the eIDAS regulation.

1.2.2.4 Output O.2.2.4 — Recommendations for technical implementation of the general data protection regulation

Technical measures in the area 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. ENISA made available a set of recommendations that allow data controllers and data processors to properly support such aspects as consent, right to erasure, data portability, data breaches, accountability, anonymisation versus pseudonymisation, etc. ENISA also continued its work on privacy-enhancing technologies, apps and methods, along with certification for data protection to provide stakeholders with the necessary support.

1.2.2.5 Output O.2.2.5 — Privacy-enhancing technologies

ENISA has delivered practical guidelines on how to implement privacy and data protection by design and default. In 2017 the agency developed a community building tool prototype that aims to create and maintain a repository of best available techniques for privacy-enhancing technologies, further building on evaluating new techniques and keeping lists of techniques available. The practical functionalities of this tool were tested.

In this fifth edition, the Annual Privacy Forum was used to bring together key communities across research, policy and the industry to disseminate work in this area.

1.2.2.6 Output O.2.2.6 — Supporting the implementation of the NIS directive

In 2017 ENISA built on the work performed during the previous years with the aim of supporting the NIS Directive Cooperation Group by providing guidance and supplemental material on the implementation of Articles 5 and 6 of the NIS directive, which refer to the identification of OES.

In this respect ENISA collected the well-established approaches different Member States use to identify their OES. In total, 19 Member States participated in this study. The agency analysed the collected information and identified common features that could constitute a basis for a harmonised approach. The outcome of this work was the key feedback into the activities of the NIS Directive Cooperation Group work stream on the identification of OES.

This work was not concluded in 2017 but will continue in 2018. During this period ENISA will continue helping Member States to develop more knowledge and expertise on this topic and will contribute by providing input to the activities of the Cooperation Group work stream.

Furthermore, ENISA, in its activities to support the implementation of the NIS directive, engaged stakeholders from the air transport, finance and healthcare sectors to understand the respective sectorial specificities. A set of recommendations and good practices, related to incident reporting for instance, has already been provided to the Cooperation Group to enhance its knowledge of

the cybersecurity situation in each of the sectors of the NIS directive. Additional recommendations and good practices will be provided to the Cooperation Group if requested as the focus shifts from the horizontal aspects of the NIS directive to sectorial implementation in 2018.

Under these activities ENISA organised two very successful workshops, contributing to the discussions on the implementation of the NIS directive. The first one was the annual meeting of the ENISA expert group on finance, where the need to streamline the requirements of the NIS directive and the payment services directive II was raised. The second workshop was the third edition of the eHealth security workshop, which was this year co-hosted with the Portuguese Ministry of Health. The workshop reached a large number of relevant stakeholders. Furthermore, ENISA has raised awareness of the NIS directive by participating in workshops with hospital representatives in Belgium, Greece, Latvia and Portugal. In the air transport sector the request for cybersecurity training in collaboration with the European Aviation Safety Agency was the highlight of a very successful year. ENISA will continue to support these sectors in implementing the NIS directive in the coming years.

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

The 2017 outcomes of the Article 14 requests under policy activity are as follows.

- ENISA supported the establishment of the NIS directive Cooperation Group work stream on the dependency of OES and digital service providers on operators that function across borders in EU. In particular, after a formal request (cf. Article 14 of the agency's regulation) from Estonia, ENISA drafted the proof-of-concept paper for this area of activity. The paper demonstrates the need for such a work stream, in the context of the NIS Cooperation Group, by illustrating the complexity and the challenges around this subject matter.

- Following a request from the European Central Bank, ENISA has started providing expertise in the development of a Eurosystem red team testing framework for financial market infrastructures. ENISA is involved in validating and enriching the red teaming framework, which involves the Bank and all 28 Member States' central financial authorities. ENISA's contribution consists of meetings at the Bank's premises and providing comments and input on follow-up documents. The work is ongoing as the request will require activities through the first and second quarters of 2018.

- Following a request from the Greek Ministry of Health, ENISA prepared a full-day workshop focusing on the NIS directive and the healthcare sector. The workshop served the purpose of raising awareness regarding the NIS directive among key stakeholders from the sector in Greece. To that end ENISA gave a detailed presentation of the directive and the relevant provisions to an audience of over 80 representatives of Greek hospitals and other healthcare organisations, and coordinated a discussion on cybersecurity in healthcare focusing on the main challenges and the exchange of good practices.

- 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 will be carried out within the joint action on eHealth (health programme 2017). Specifically, ENISA has been asked to actively participate in Task 7.3, 'Data and system security', of work package 7, which addresses the issues on 'Implementation challenges and impact'. Activities related to this request will begin in 2018.

- Following a request from the European Aviation Safety Agency, ENISA has been assisting that agency on the subjects of sectorial implementation of the NIS directive and cybersecurity in aviation. In this context ENISA is currently supporting the creation of the European Aviation's information sharing and analysis centres (ISACs), which will provide a platform for cybersecurity information exchange across Europe. Moreover, ENISA is organising dedicated cybersecurity training courses for the aviation sector. A first training course for air carriers took place in 2017 in collaboration with the European Aviation Safety Agency. Due to the high demand a second one will be organised in the second quarter of 2018. Topics also include cybersecurity for avionics (training led by the European Aviation Safety Agency) and artefact analysis (forensics led by ENISA).

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 IT security certification	More than 10 private companies and 10 Member State representatives contribute to/ participate in the activity.	29 private companies and 12 Member State representatives have participated in the support activity.
Output O.2.1.2 — Restricted: towards a digital single market for high-quality NIS products and services	More than 10 leading private companies from two sectors take part in the study.	24 individual start-ups and 10 funding-side organisations covering 10 sectors participated in the study. The validation workshop was held in November in Brussels and was hosted by DG Communications Networks, Content and Technology's Startups and Innovation Unit.
Objective 2.2. Supporting EU policy implementation		
Output O.2.2.1 — Contribute to EU policy in the area of the electronic communications sector	Engage 20 sector providers and 20 national bodies in the activity.	38 sector providers and 28 national bodies (NRAs) participated in the study.
Output O.2.2.2 — Develop guidelines for the implementation of mandatory incident reporting	More than 15 private stakeholders and more than 15 public stakeholders contribute to the study.	49 private stakeholders and 20 public stakeholders contributed to the study.
Output O.2.2.3 — Recommendations for technical implementation of the eIDAS regulation	Engaging at least five representatives from different bodies/Member States in the preparation of the recommendations. Review and acceptance by at least 10 stakeholders (trust service providers, conformity assessment bodies and supervisory authorities) from at least five Member States.	15 representatives from different bodies/Member States were engaged in the preparation and validation of the recommendations. 26 stakeholders from 10 Member States have reviewed and validated the recommendations.
Output O.2.2.4 — Recommendations for technical implementation of the general data protection regulation	At least five representatives from different bodies/Member States participate in the preparation of the recommendations.	Six representatives from different bodies/Member States participated in the drafting and validation of the recommendations.
Output O.2.2.5 — Privacy-enhancing technologies	At least five experts in the area contribute to the report. The event should have at least 80 participants from the relevant communities.	Six experts contributed to the drafting and the review of the report and the relevant prototype. The Annual Privacy Forum was attended by more than 100 participants.
Output O.2.2.6 — Supporting the implementation of the NIS directive	Engaging at least 15 Member States and 15 private stakeholders in the ENISA contributions to the implementation of the NIS directive. 10 Member States participate in the activity. ENISA provides contributions as requested. 10 OES participate in the workshops.	19 Member States were engaged in the ENISA contributions and in the relevant activities. The Cooperation Group decided not to engage the private sector in this activity, which was done by the Member States at national level.
Objective 2.3. Response to Article 14 requests under policy		
Output O.2.3.1. — Response to requests under policy activity	Answers to requests.	Answer provided. See https://www.enisa.europa.eu/publications/enisa-article-14-requests

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

Activity 2 — Policy: promote network and information security as an EU policy priority
Objective 1.1. Improving the expertise related to critical information infrastructure
Output O.2.1.1 — Support the policy discussions in the area of IT security certification **Recommendations on European data protection certification** https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification **Considerations on ICT security certification in EU** https://www.enisa.europa.eu/publications/certification_survey **Overview of the practices of ICT certification laboratories in Europe** https://www.enisa.europa.eu/publications/overview-of-the-practices-of-ict-certification-laboratories-in-europe
Output O.2.1.2 — Restricted: towards a digital single market for high-quality NIS products and services **Effective models for startups in NIS** The report was disseminated to the ENISA Management Board
Objective 2.2. Supporting EU policy implementation
Output O.2.2.1 — Contribute to EU policy in the area of the electronic communications sector **Online tracking and user protection mechanisms** https://www.enisa.europa.eu/publications/online-tracking-and-user-protection-mechanisms
Output O.2.2.2 — Develop guidelines for the implementation of mandatory incident reporting **Guidelines on mandatory incident reporting in the context of the NIS directive** Dissemination of the report by the European Commission only within the Cooperation Group.
Output O.2.2.3 — Recommendations supporting implementation of the eIDAS regulation **Technical guidance on qualified trust services (six reports)** https://www.enisa.europa.eu/topics/trust-services/technical-guidance-on-qualified-trust-services **Qwacs plugin** https://www.enisa.europa.eu/publications/qwacs-plugin **eIDAS: overview on the implementation and uptake of trust services** https://www.enisa.europa.eu/publications/eidas-overview-on-the-implementation-and-uptake-of-trust-services
Output O.2.2.4 — Recommendations for technical implementation of the general data protection regulation **Privacy and data protection in mobile applications**

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

One of the main goals of this objective was to develop and improve activities related to the operational security capacity-support programme. In 2017 ENISA continued to build upon its work in the operational security area by providing technical training materials for CSIRTs to support the improvement of technical skills across Europe. The goal is to support Member States through a dialogue with relevant stakeholders in order to be ready for the technical challenges of the coming years. Another main goal of this objective was to help the EU Member States and other ENISA stakeholders, such as the EU institutions, bodies and agencies, to develop and extend the necessary capabilities in order to meet the ever-growing challenges of securing their networks.

1.3.1.1 Output O.3.1.1 — Support national and governmental CSIRTs capabilities

In 2017 ENISA concentrated its efforts on assisting CSIRTs by, for example, leveraging its role as secretariat of the CSIRTs network as defined in the NIS directive. In close cooperation with CSIRTs, the agency supported the development of Member States' national incident response capabilities by providing recommendations on key dimensions of NIS capacity building with a focus on the development and efficient functioning of national and governmental CSIRTs.

The main objective of this output in 2017 was to help Member States and other ENISA stakeholders, such as EU institutions, bodies and agencies, to develop and extend their incident response capabilities and services in order to meet the ever-growing challenges to secure their networks. Currently all Member States connected to the internet have CSIRT capabilities, but the level of maturity among them still varies dramatically. It is ENISA's mission to continue to help minimise those differences.

In 2017 ENISA published a study on the maturity aspects of CSIRTs, tailored to the national teams expected to join the CSIRTs network. The study takes all relevant information sources into account, with a special emphasis on the NIS directive, the various ENISA reports on CSIRT capabilities, maturity and metrics, and on the security incident management maturity model for CSIRTs, which is a good practice that has been widely used in Europe for several years. Additionally, ENISA has organised research to establish a readily implementable and useable self-assessment survey and peer review methodology. More than five Member States that had already experienced the CSIRT certification process supported this research. The primary target audience for the report is the EU CSIRTs network teams and their management. However, the report, and especially the maturity self-assessment that it contains, will be of use to all CSIRTs all over the world.

As part of a continuous effort, ENISA maintains and regularly updates its online European CSIRT Inventory. In 2017, in light of the implementation of the NIS directive, ENISA concluded a major usability makeover of the tool, which now has new features and is more user friendly. The new features of the tool include very detailed graphics and statistics on the participation of CSIRTs in different communities, membership status and contact details. The listing features 342 teams from 45 countries, a major increase that shows the continuous expansion of CSIRTs globally. This tool now allows the reader to filter the displayed teams by NIS directive CSIRTs network membership.

1.3.1.2 Output O.3.1.2 — Update and provide technical training for Member States and EU bodies

In 2017most of the activities in this area aimed at maintaining and extending the collection of good-practice guidelines and training courses 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 in order to improve the skills of CSIRT teams and their personnel. Over the past several years ENISA has developed a wide range of cybersecurity training courses, and delivered the training content to several national and governmental CSIRTs and their constituents. In detail, with the emphasis that the NIS directive places on the importance of the seven critical sectors, the agency aimed to identify the current situation in these sectors with regard to the available cybersecurity training courses, and whether there are any training needs specific to each of the sectors, beyond the generic needs for such training. In this regard, ENISA produced a set of deliverables providing:

- stocktaking results on the current situation for each of the NIS directive critical sectors with regard to the available cybersecurity training courses; and
- recommendations on what could be done with ENISA's training portfolio in order to improve the suitability of that portfolio for the existing training needs.

In 2017 ENISA also delivered, for the first time, sector-specific training for technical specialists in the aviation sector. The training media campaign led to 110 requests for participation from different organisations in both the private and the public sector in all Member States. Due to the enormous amount of applications, priority was given to the target audience (airports, air carriers and air traffic control personnel), coverage of Member States and relevance to the training.

Moreover, regarding good practices for CSIRT services, ENISA and the CSIRT community jointly set up a task force with the goal of reaching a consensus on a reference security incident classification taxonomy. The task force is composed of representatives of 41 CSIRTs from 16 Member States. Thanks to the task force's efforts, ENISA consolidated the results into a document that was published in January 2018 and paved the road towards efforts to build a common language to face future incidents, also in light of the implementation of the NIS directive.

1.3.1.3 Output O.3.1.3 — Support EU Member States in the development and assessment of national cybersecurity strategies

In 2017 ENISA supported the Member States in the development and assessment of NCSS by updating the EU NCSS map. The new version of the map was created on the basis of the work performed in previous years and presents the Member States' strategic objectives and good practices in an easy and user-friendly manner.

In addition, ENISA, in cooperation with the Dutch National Cyber Security Centre, organised a workshop in the Hague. The focus of the workshop was on collaboration, a topic not only fundamental to the objectives of a strategy but also highlighted in several pieces of legislation, such as the NIS directive and the new cybersecurity act. In this workshop ENISA validated the results of two reports created to provide guidelines and support the output of this activity: one for cooperative models on public–private partnerships (PPPs) and one for cooperative models on ISACs. The documents depict the status of ISACs and PPPs with regard to cybersecurity in Europe through well-informed maps.

In total, 18 Member States participated in the activities of ENISA regarding this output. Representatives from 14 Member States attended the workshop.

1.3.2 Objective 3.2. Support EU institutions' capacity building

1.3.2.1 Output O.3.2.1 — Restricted and public info notes on NIS

ENISA provides guidance on important NIS events and developments through info notes. Info notes are explanatory notes, regarding, for example, events that reach a certain level of public and media attention. Relevant NIS events might cover incidents, significant developments and announcements in the field of cybersecurity.

ENISA has provided balanced and neutral information regarding such events, covering issues, points of action, mitigation measures, summaries, related practices, etc.

In 2017 ENISA fulfilled its intention to continue providing info notes in a timely manner as a reliable and continuous service to its stakeholders.

Output O.3.2.2 — Restricted: upon request, support the assessment of existing policies/procedures/ practices on NIS within EU institutions

In 2017 a report was drafted as a joint effort between DG Communications Networks, Content and Technology and ENISA, who were tasked with presenting an overview of relevant sectorial initiatives at the EU and international levels in the field of cybersecurity. The information included in the document was presented to the Cooperation Group to ensure that both the members of the Cooperation Group and the relevant actors at Member State level involved in the transposition process for the NIS directive have a clear picture of the work that has already been conducted in the field.

This document builds on the work conducted by ENISA in 2016, validated by multiple directorates-general, and maps the main stakeholders at EU level, along with the relevant policy framework in the field of cybersecurity across key sectors covered by the NIS directive: energy, transport, banking and finance, health and drinking water.

The resulting document is conceived as a 'living' document, and will be regularly updated by the Commission services and ENISA to inform the Cooperation Group about any developments that might be relevant for the transposition process.

Considering the sensitive nature of the information that ENISA received from the EU institutions, this deliverable was restricted in distribution.

1.3.2.2 Output O.3.2.3 — Representation of ENISA on the Steering Board of CERT-EU and representation of the EU agencies using CERT-EU services

In 2017 a new service agreement with CERT-EU was put in place for ENISA. For the aforementioned agreement, ENISA has the formal task of representing the EU's decentralised agencies.

In this context ENISA participated in the Steering Board of CERT-EU, representing itself and the EU's decentralised agencies to ensure that the needs of these bodies are adequately represented.

1.3.3 Objective 3.3. Assist private-sector capacity building

1.3.3.1 Output O.3.3.1 — Cybersecurity culture: from identifying the issues to providing working scenarios for management level

ENISA has conducted a study that contains guidance and practical tools for organisations on developing and maintaining an internal cybersecurity culture.

The *Cyber security culture in organisations* report is the product of multidisciplinary research undertaken in order to better understand the dynamics of how cybersecurity culture can be developed and shaped within organisations. This research draws from disciplines that include organisational sciences, psychology, law and cybersecurity, along with the knowledge and experiences gathered from some of Europe's largest organisations. The report itself contains good practices, methodological tools and step-by-step guidance for those seeking to commence or enhance their organisation's own cybersecurity culture programme.

1.3.3.2 Output O.3.3.2 — Recommendations on cyber insurance

ENISA conducted a study to assess the level of harmonisation of the risk assessment language in cyber insurance. The lack of harmonisation/ standardisation was found to have a significant negative impact on the broad adoption of cyber-insurance products and several recommendations were developed to support the cyber-insurance market in achieving a higher level of language commonality. The report was based on input provided by stakeholders covering the full supply spectrum of the cyber-insurance market, focusing on carriers, underwriters and brokers. In all, 51 insurance carriers, underwriters, brokers and reinsurers and 58 companies in total from 12 Member States participated in drafting the recommendations via interviews and an online survey.

A very successful workshop was held in Brussels, with over 90 registrations for participation from multiple stakeholders from the fields of industry, academia and policy. In all, 24 insurance companies and 41 companies in total from 14 Member States participated in the workshop on validating the recommendations. The workshop contributed to the discussions on the maturity and standardisation of the cyber-insurance market. The report has been widely referenced in the community. Its recommendations were very well received and are being carefully considered by key stakeholders, including the OECD, which cites the report in a relevant publication on the current state of the cyber-insurance market [11]. Some have in fact already been adopted by associations proposing non-binding wording models to promote harmonisation in the market, such as the German Insurance Association.

11 http://www.oecd.org/daf/fin/insurance/2018-oecd-conference-cyber-insurance-market.htm

1.3.4 Objective 3.4. Assist in improving general awareness

1.3.4.1 Output O.3.4.1 — Cyber security challenges

In 2017 ENISA maintained its involvement in the area of cybersecurity challenges and advised the Member States on running national Cyber Security Challenge competitions. The agency has also continued its own annual European Cyber Security Challenge.

ENISA's support for national and European activities targeted university students from technical schools and young talent, including security practitioners from the industry. The goals in 2017 were to increase interest and future opportunities in NIS for these communities by promoting excellence in the form of competitions and to gather feedback on the areas of interest from these stakeholders.

The success of ENISA's Cyber Security Challenge is evidenced by the participation in the event, held in Malaga, Spain, of more than 150 contestants from 15 different EU and European Free Trade Association (EFTA) countries.

1.3.4.2 Output O.3.4.2 — European Cyber Security Month deployment

European Cyber Security Month has continued to outperform original expectations, as evidenced by the increased number of participants and activities, and the increased engagement year on year. In 2017 ENISA focused on providing guidance to Member States' campaigns and techniques to better evaluate the impact of awareness raising.

1.3.5 Objective 3.5. Response to Article 14 requests under capacity activity

1.3.5.1 Output O.3.5.1 — Response to requests under capacity activity

During 2017 ENISA delivered training to the European Parliament, the European Aviation Safety Agency, Latvia, Romania and Sweden on topics such mobile malware, artefact analysis, and incident handling and response. The feedback was highly positive, with only minor comments on possible course improvements.

1.3.6 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 — Support national and governmental CSIRTs capabilities	Updated material on CSIRT baseline capability report based on input from at least five Member States. Two updates (Q2, Q4) for the overview of existing CSIRTs and their constituencies in Europe for different type of stakeholders (e.g. business sector). During 2017, support provided for at least two Member States to enhance their 'national and governmental CSIRT baseline capabilities' and for two EU institutions, bodies or agencies to develop or enhance their incident response capabilities. At least 15 Member States participating in the technical CSIRT workshop.	More than five Member States provided input to the CSIRT capabilities and maturity report (study on CSIRT maturity). CSIRT Inventory; two update releases (Q2, Q4). • Over 50 team updates. • Full alignment with TF-CSIRT-TI [10], Forum of Incident Response and Security Teams (FIRST) list and governmental CSIRTs lists. • Major usability makeover, with new features and more user friendly. • The current listing features 342 teams from 45 countries, a major increase that shows the continual expansion of CSIRTs globally. • New filter that can display which national CSIRTs are participating in the CSIRTs network under the NIS directive (there are currently 35 such teams). Support was provided for five Member States (Belgium, France, Latvia, Netherlands, and Portugal) via the CSIRTs network working group on maturity assessment piloting initiatives. EU bodies such as the European Aviation Safety Agency and CERT-EU also received training support. 24 representatives from 16 Member States participated in a technical CSIRT training workshop.
Output O.3.1.2 — Update and provide technical training for Member States and EU bodies	At least 15 Member States covered during the survey for stocktaking in NIS directive training schemes. Continued CSIRT services training provided to a minimum of 20 participants from different organisations in five Member States. At least one piece of training material updated to support improved operational practices of CSIRTs in at least 15 Member States. At least one new (or updated) good-practice guide on a particular CSIRT service. At least 70 % of participants in training courses (online or onsite) evaluate the experience as positive or very positive.	The training vendors that participated in the surveys provided 57 training records from 15 different organisations covering 16 Member States. CSIRT training delivered for 24 participants from 16 Member States in the aviation sector. Incident handling training material updated to support sector-specific training. A good-practice guide, Reference incident classification taxonomy, was released based on the input from 41 CSIRTs from 16 Member States. Feedback evidence that the training was well received: 75 % was positive or very positive while the remaining 25 % was medium.
Output O.3.1.3 — Support EU Member States in the development and assessment of NCSS	Engage at least 15 EU Member States in this activity/workshop.	18 Member States engaged in the ENISA activity.

12 http://www.oecd.org/daf/fin/insurance/2018-oecd-conference-cyber-insurance-market.htm
Trusted Introducer : https://www.trusted-introducer.org/

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 3.2. Support EU institutions' capacity building		
Output O.3.2.1 — Restricted and public info notes on NIS	In 2017, at least one additional key stakeholder group (e.g. ENISA Management Board members or the Permanent Stakeholders Group) receiving restricted info notes on a regular basis. At least six public info notes published on the ENISA website.	In 2017 one restricted cybersecurity info note was produced regarding ransomware. It was shared with an additional ENISA stakeholder group. In 2017 ENISA published 11 cybersecurity info notes on its website.
Output O.3.2.2 — Restricted: upon request, support the assessment of existing policies/procedures/ practices on NIS within EU institutions	At least three EU institutions and five Member States take part in the activity.	Eight EU institutions and agencies and all 28 Member States were involved in this activity. The initial findings of the report were presented to the Cooperation Group in February as a joint effort by ENISA and DG Communications Networks, Content and Technology.
Output O.3.2.3 — Representation of ENISA on the Steering Board of CERT-EU and representation of the EU agencies using the CERT-EU services	Attendance at CERT-EU Management Board meetings. Consultation with EU agencies and representing their views at Management Board level.	Actively kept the EU agencies informed about the CERT-EU activities and represented the EU agencies' views on the CERT-EU Steering Board. ENISA substantially contributed to the agreement that was reach between the EU agencies and CERT-EU.
Objective 3.3. Assist private-sector capacity building		
Output O.3.3.1 — Cybersecurity culture: from identifying the issues to providing working scenarios for management level	Involve at least five representatives from different bodies/Member States in the preparation of this study.	13 private companies [11] contributed to the survey across five Member States.
Output O.3.3.2 – Recommendations on cyber insurance	At least seven insurance companies and 10 companies from at least five Member States take part in the preparation of the recommendations.	51 insurance carriers, brokers and reinsurers and 58 companies in total from 12 Member States participated in drafting the recommendations (interviews and survey). 24 insurance companies and 41 companies in total from 14 Member States participated in the recommendations validation workshop, which was held in Brussels in October.
Objective 3.4. Assist in improving general awareness		
Output O.3.4.1 — Cyber security challenges	At least two additional Member States organise national cybersecurity challenges in 2017 and participate in the European Cyber Security Challenge.	Five new countries have joined the challenge in 2017: Cyprus, Czech Republic, Denmark, Italy, and Norway.
Output O.3.4.2 — European Cyber Security Month deployment	All 28 Member States and other partners and representatives from different bodies/Member States participate in/support European Cyber Security Month 2017.	Activities were registered in all 28 Member States and support for European Cyber Security Month 2017 from different bodies was realised.
Objective 3.5. Response to Article 14 requests under capacity activity		
Output O.3.5.1. — Response to requests under capacity activity	Answers to requests.	Answer provided. See https://www.enisa.europa.eu/publications/enisa-article-14-requests

13 Initial analysis directed the research towards private companies as they were the most likely to have implemented a cybersecurity culture programme.

1.3.7 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 — Support national and governmental CSIRTs capabilities **Update ENISA CSIRT Inventory** https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map **Update on CSIRT baseline capabilities** https://www.enisa.europa.eu/publications/study-on-csirt-maturity **Good-practice guide on how to improve CSIRT capabilities** https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process **Online CSIRT maturity self-assessment tool** https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey
Output O.3.1.2 — Update and provide technical training for Member States and EU bodies **Stock taking of information security training needs in critical sectors** https://www.enisa.europa.eu/publications/stock-taking-of-information-security-training-needs-in-critical-sectors **Reference incident classification taxonomy** https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy **Online training material update** https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material **Exploring the opportunities and limitations of current threat intelligence platforms** https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms
Output O.3.1.3 — Support Member States in the development and assessment of NCSS **Updated — EU NCSS map** https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map **Information sharing and analysis centres (ISACs) — Cooperative models** https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models **Public private partnerships (PPP) — Cooperative models** https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models
Objective 3.2. Support EU institutions' capacity building
Output O.3.2.1 — Restricted and public info notes on NIS **ENISA cybersecurity info notes** https://www.enisa.europa.eu/publications/info-notes
Output O.3.2.2 — Restricted: upon request, support the assessment of existing policies/procedures/practices on NIS within EU institutions **Mapping of cybersecurity sectorial initiatives at the EU and international level** The report was disseminated to the ENISA Management Board.
Output O.3.2.3 — Representation of ENISA on the Management Board of CERT-EU and representation of the EU agencies using the CERT-EU services CERT-EU interinstitutional agreement was reached with the participation of ENISA and the EU's decentralised agencies.
Objective 3.3. Assist private-sector capacity building
Output O.3.3.1 — Cybersecurity culture: from identifying the issues to providing working scenarios for management level **Cyber security culture in organisations** https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations
Output O.3.3.2 — Recommendations on cyber insurance **Commonality of risk assessment language in cyber insurance** https://www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance
Objective 3.4. Assist in improving general awareness
Output O.3.4.1 — Cyber security challenges **The European Cyber Security Challenge: lessons learned report** https://www.enisa.europa.eu/publications/the-european-cyber-security-challenge-lessons-learned-report
Output O.3.4.2 — European Cyber Security Month deployment **2017 European Cyber Security Month — Deployment report** https://www.enisa.europa.eu/publications/european-cyber-security-month-2017
Objective 3.5. Response to Article 14 requests under capacity activity
Output O.3.5.1. Response to requests under capacity activity **ENISA Article 14 requests** https://www.enisa.europa.eu/publications/enisa-article-14-requests

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 — Evaluation of Cyber Europe 2016 and report on exercise after-action activities from 2014 to 2016

In 2016 ENISA organised the fourth pan-European cyber-crisis exercise, Cyber Europe 2016 (CE2016). The pan-European exercises organised by ENISA are producing a number of significant recommendations and actions for all of the involved stakeholders. It is extremely important to ensure follow-up and to monitor the progress of all these actions. Otherwise, the added value from the lessons learned from the exercise is diminished.

In early 2017 ENISA performed an in-depth analysis of the evaluation data gathered from the exercise. This resulted in a detailed after-action report that was published together with a related video on ENISA's website [14] in summer 2017.

First, the exercise fostered cooperation between targets of simulated cybersecurity incidents, security providers and national authorities, shedding light on national-level public–private and private–private cooperation. Second, CE2016 helped participants understand how cybersecurity authorities would cooperate with each other and EU bodies in the event of a large-scale crisis. Undoubtedly, crisis cooperation at the EU level is maturing and improving greatly. Last, the exercise offered countless opportunities for participants to enhance their cybersecurity capabilities, from their technical and operational expertise to their capacity to handle crisis communication. Organisational and individual cybersecurity preparedness and capabilities in the EU were excellent overall.

The exercise offered countless opportunities for participants to enhance their cybersecurity capabilities, from their technical and operational expertise to their capacity to handle crisis communication.

1.4.1.2 Output O.4.1.2 — Planning of Cyber Europe 2018

In 2018 ENISA will organise the fifth pan-European cyber exercise, Cyber Europe 2018 (CE2018). This exercise will closely follow up and build upon the lessons learned and actions from previous exercises, such as CE2014 and CE2016.

CE2018 will focus on testing and training on large-scale incident management cooperation procedures at the EU and national levels. It will offer preparatory

14 https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/ce-2016

Cyber Europe 2016

training and cooperation opportunities, such as small exercises, to Member States and the EU institutions (e.g. Cyber SOPEx). The exercise's escalation and build-up will be realistic and focused in order to better capture how incidents are managed and how cooperation happens in real life. The exercise will include explicit scenarios for the CSIRTs network set up under the NIS directive.

In 2017 the agency, together with the cybersecurity authorities (planners) from the Member States, developed a comprehensive exercise plan for CE2018. A dedicated task force has developed an extensive scenario with over 10 different types of cybersecurity incidents relevant to the essential sector of aviation, affecting airports, air carriers, civil aviation authorities and internet service providers who provide services to the aviation industry.

The exercise will be held in summer 2018. A trailer for this exercise was produced in 2017 and published [15] early in 2018.

1.4.1.3 Output O.4.1.3 — Support activities for cyber exercise planning and cyber crisis management

Cyber Exercise Platform development and content management

In 2014 ENISA started to develop the Cyber Exercise Platform (CEP). CEP hosts a number of services that ENISA offers to the Member States and EU institutions, such as exercise organisation and management, an exercise playground with technical incidents, a map of exercises and hosting the exercise-development community. In 2017 ENISA maintained and enhanced the experience offered by CEP, including user support. It added support for the Virtual Exercise Universe, a set of online applications emulating real-life platforms such as social media, mainstream media, expert blogs, dedicated/specialised sites, the online presence of hackers, etc.

Also in 2017 ENISA developed a Cyber Incident Visualisation tool, which includes a map that visualises the occurrence of incidents. During the year ENISA also developed an online training and education platform to support exercise preparation and other related activities of the agency.

In addition, new content and exercise incident challenges and material were developed in order to maintain the interest of stakeholders and make CEP a central tool in cybersecurity exercising for all stakeholders, in the form of ad hoc on-demand exercises (Cybersecurity Technical Exercises — CTEx). The CTEx database of incidents includes over 40 incidents ranging from malware analysis, network forensics, mobile malware, steganography, offensive and defensive capture-the-flag games, etc.

If you are interested in organising such an exercise contact: c3@enisa.europa.eu

EU-level cyber-crisis and incident management procedures and Connecting Europe facility cybersecurity digital service infrastructure

During 2017 ENISA started activities for the future takeover of the management and operations for the centralised components of the MeliCERTes platform, formerly known as CEF CSP Cybersecurity DSI Core Service Platform. MeliCERTes is expected to be the

15 https://www.youtube.com/watch?v=hCDOp7_hsjY

key cooperation mechanism for computer emergency and response teams in the European Union, and will enhance EU-wide capability for preparedness, cooperation and information exchange, for better coordination and response to cyberthreats and crises.

As the body with final responsibility for MeliCERTes, and the body in charge of maintaining it, ENISA is currently following the development of the platform closely, and is actively supporting the Commission and the consortium of national CSIRTs in the various activities that are being carried out. At the same time the agency is building its capability to gradually take over the parts of the infrastructure as implemented.

ENISA is expected to implement some of the systems and functionalities for the management, maintenance and further development of the MeliCERTes platform, together with the development of some of the related internal and external operational process.

Blueprint

In 2017 ENISA supported DG Communications Networks, Content and Technology in its activities related to cyber-crisis management and in preparation for the release of the blueprint proposal [16] in parallel to the cybersecurity act.

16 Commission Recommendation on 'Coordinated Response to Large Scale Cybersecurity Incidents and Crises' consists of a Blueprint for Coordinated response to large-scale cross-border cybersecurity incidents and crises http://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-ANNEX-1-PART-1.PDF so that the EU has in place a well-rehearsed plan in case of a large scale cross-border cyber incident or crisis.

ENISA experts drafted papers, supported CSIRTs network working groups and represented the agency in crisis-management workshops in Brussels. Additionally, the specifications of a prototype aimed at supporting the production of EU cybersecurity technical situation reports, as defined in the blueprint proposal, were drafted with the assistance of an external expert in machine learning and natural-language processing. The specifications of this prototype were used as the foundations for a public tender worth EUR 80 000 released in January 2018.

1.4.2 Objective 4.2. CSIRT and other NIS community building

1.4.2.1 Output O.4.2.1 — Support the fight against cybercrime and collaboration between CSIRTs and law enforcement agencies

In 2017 the key goal for ENISA, of supporting the collaboration between CSIRT and law enforcement communities, was served by analysing the technical, legal and organisational aspects of this collaboration. In addition to the publication of two reports in this area, the annual workshop for national and governmental CSIRT and their law enforcement counterparts was organised together with Europol's European Cybercrime Centre and inter alia it demonstrated that full-circle policy should mean involving judiciary authorities.

CSIRT's Network meeting - October 2017

1.4.2.2 Output O.4.2.2 — EU CSIRT network secretariat and support for EU CSIRT network community building

In 2017 ENISA supported the Commission and Member States in the implementation of the NIS directive, in particular in the area of incident response. As part of this activity ENISA has an active role as CSIRTs network secretariat and actively supports cooperation among the CSIRTs. Moreover, ENISA provides expertise and assistance, as envisioned by the NIS directive, by developing guidance and good practices in the area of operational community efforts, such as on information exchange or CSIRTs maturity assessments.

As defined by the NIS directive in its role as CSIRTs network secretariat, ENISA has engaged all 28 EU Member States and their designated CSIRTs in developing rules and procedures. The CSIRTs network secretariat has engaged them in the implementation of the NIS directive through dedicated physical meetings (in Malta, Estonia and Greece) and working group activities, and, last but not least, by supporting operational cooperation during cyber crises such as WannaCry and NotPetya.

Furthermore, the agency contributed to the dialogue between NIS-related communities, including between CSIRTs and law enforcement and data-privacy communities, in order to support a consistent EU-wide approach to NIS.

Through the CSIRTs network working groups, more than 10 Member States CSIRT representatives actively participated in activities that improved operational cooperation and information sharing among CSIRTs in Europe.

In addition, ENISA took an active role in supporting the CSIRTs network in activities relevant to the CEF work programme. ENISA also successfully developed and managed the main communications infrastructure of the CSIRTs network that was assigned to the agency.

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-building activity

The outcomes of the Article 14 requests under policy activity for 2017 are as follows.

- Following the Article 14 request by another EU agency, the European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, ENISA supported the organisation, planning, conduct and evaluation of the exercise on the visa information system (VIS). In particular, ENISA trained that agency's personnel and exercise planners from the Member States on the exercise management methodology. In addition ENISA helped them to apply the methodology in the organisation of the VIS exercise by providing templates for all required documentation, supporting the development of the different products of the exercise and supporting the conduct and the evaluation process. ENISA also offered a dedicated space within the CEP for the VIS exercise and offered customer helpdesk support.

- Following a request from the Science and Technology Options Assessment of the European Parliament, ENISA conducted a study with the title *Cyber-security in the EU CSDP — Challenges and risks for the EU*. For this study, ENISA consulted external stakeholders within and beyond the EU (i.e. NATO, academia). The study concluded with a set of proposals from the political down to the tactical level. The study was subsequently presented in the European Parliament.

- Following a request from the Estonian Presidency, ENISA assisted the organisers of EU Cybrid 17 [17], the event organised by Estonian Presidency, in developing the exercise scenario. This exercise was the first of its kind at the level of ministers of defence. ENISA also supported and participated in the exercise during the execution.

- Following a request from the European External Action Service, ENISA provided assistance in developing the 2017 EU parallel and coordinated exercise by extending the EU Cybrid17 scenario to accommodate the needs of the exercise in 2017.

17 https://www.eu2017.ee/news/press-releases/EUCYBRID2017

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**	
Objective 4.1. Cyber crisis cooperation		
Output O.4.1.1 — Evaluation of Cyber Europe 2016. Report on exercise after-action activities from 2014 to 2016	At least 80 % of the countries actively involved in the exercise contribute to the evaluation and quality assurance processes of the report. At least 80 % of the countries actively involved in exercises agree with the conclusions of the report.	All EU Member States plus Switzerland and Norway participated in the exercise and contributed to the evaluation. The conclusions of the after-action report were approved by all countries involved in the exercise.
Output O.4.1.2 — Planning of Cyber Europe 2018	At least 24 EU Member States/EFTA countries confirm their support for CE2018.	All EU Member States plus Switzerland and Norway were involved in the planning of CE2018.
Output O.4.1.3 — Support activities for cyber exercise planning and cyber crisis management	At least 70 % of CEP users evaluate it positively. At least 90 % of the participating Member States agree to the operational procedures developed. Over 80 % of the countries on the Governance Board approve the implementation roadmap and deployment plan.	Over 95 % users evaluated CEP positively in the evaluation surveys for the different exercise activities. All Members of the CSIRTs network agreed the standard operational procedures. The CEF Governance Board unanimously approved the roadmap for ENISA to take over the central parts of the platform.
Objective 4.2. CSIRT and other NIS community building		
Output O.4.2.1 — Support the fight against cybercrime and collaboration between CSIRTs and law enforcement agencies	At least five Member States' CSIRT representatives and five Member States' law enforcement agency (LEA) representatives participate in the preparation of the report. At least five Member States' CSIRT representatives participate in the preparation of the guidelines. At least 15 Member States participate in the ENISA/Europol European Cybercrime Centre annual workshop.	13 respondents from the CSIRT community, 11 from the law enforcement community and one belonging to both participated in the preparation of the report through a survey. In addition there were 23 respondents originating from 19 Member States and two respondents from EFTA countries. For the preparation of the guidelines, interviews were carried out with: (a) eight experts from the CSIRTs community, six from the LEA community and two belonging to both communities (in all 16 experts originated from 11 Member States); (b) four CSIRT representatives from three Member States and five LEA representatives from three Member States. More than 70 participants attended the workshop. Participants were from 24 Member States and three EFTA countries.
Output O.4.2.2 — EU CSIRT network secretariat and support for EU CSIRT network community building	Engaging all 28 Member States' designated CSIRTs in the development of the rules of procedure and in general in the implementation of the NIS directive. Positive feedback regarding ENISA support from the majority of the participants in activities. Positive feedback from participants in the events/workshops organised by ENISA. ENISA's work successfully reflected by existing CSIRT communities (FIRST, Task Force CSIRT (TF-CSIRT), EU CSIRT network) and CSIRT network. At least five Member States' CSIRT representatives participate in preparing updates in the design of the inventory of services for improved cooperation and information sharing among CSIRTs in Europe.	ENISA has engaged all 28 Member States and their designated CSIRTs in the development of rules and procedures, and in general in the implementation of the NIS directive through dedicated physical meetings and working group activities (Malta, Estonia and Greece). Through the CSIRTs network working groups more than 10 Member States CSIRT representatives actively participated in activities that improved operational cooperation and information sharing among CSIRTs in Europe. ENISA's work is positively recognised in other CSIRT structures, e.g. reference incident classification taxonomy in TF-CSIRT, CSIRT maturity assessment framework in FIRST and the Global Forum on Cyber Expertise.

Summary of outputs in Activity 4 — Community: foster the emerging European network and information security community		
Outputs	**Performance indicator**	
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	Answer provided. See https://www.enisa.europa.eu/publications/enisa-article-14-requests/

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 — Evaluation of Cyber Europe 2016 and report on exercise after-action activities from 2014 to 2016 **Cyber Europe 2016 — After action report** https://www.enisa.europa.eu/publications/ce2016-after-action-report **Exercise after action activities 2014-2016** Published with restricted access
Output O.4.1.2 — Planning of Cyber Europe 2018 **CE2018 exercise plan** Published with restricted access
Output O.4.1.3 — Support activities for cyber exercise planning and cyber crisis management Services delivered.
Objective 4.2. CSIRT and other NIS community building
Output O.4.2.1 — Support the fight against cybercrime and collaboration between CSIRTs and law enforcement agencies **Improving cooperation between CSIRTs and law enforcement: legal and organisational aspects** https://www.enisa.europa.eu/publications/improving-cooperation-between-csirts-and-law-enforcement **Tools and methodologies to support cooperation between CSIRTs and law enforcement** https://www.enisa.europa.eu/publications/tools-and-methodologies-to-support-cooperation-between-csirts-and-law-enforcement
Output O.4.2.2 — EU CSIRT network secretariat and support for EU CSIRT network community building Status: work related to the CSIRTs network activities and support is restricted to CSIRTs network members only. **Maturity reference for CSIRTs — Executive summary** https://www.enisa.europa.eu/publications/maturity-reference-for-csirts-2013-executive-summary Status: Full report available only to CSIRTs network members via the CSIRTs network portal.
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

1.5 KEY RESULTS IN THE IMPLEMENTATION OF ACTIVITY 5 — ENABLING: REINFORCE ENISA'S IMPACT

Activity 5 covers the following four main objectives.

- Management.
- Engagement with stakeholders.
- International activities.
- Compliance and support.

1.5.1 Objective 5.1. Management

The Executive Director is responsible for the overall management of the agency. The Executive Director has one personal assistant.

To support the Executive Director an Executive Director's Office (EDO) has been set up. The tasks covered by EDO include policy advice, legal advice, Management Board secretariat, coordination of the work programme and press communications.

During 2017, policy and legal advice extended to all aspects of the agency's work and included advice in relation to both the operational and administrative departments of the agency.

In 2017 EDO continued to support the Management Board and the Executive Board in their functions by providing secretariat assistance.

In relation to the Management Board, one ordinary meeting was organised during 2017 and informal meetings were held as necessary. The Management Board portal was supported as well. Three meetings of the Executive Board were held.

1.5.2 Objective 5.2. Engagement with stakeholders

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

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

National Liaison Officers Network

ENISA has kicked off various activities aiming at strengthening the cooperation with its National Liaison Officers (NLO) Network. NLOs are key actors in the agency's daily work. They are the liaison between ENISA and the community of network and information security (NIS) experts and relevant organisations in their respective Member State acting as 'ambassadors' and 'facilitators' of ENISA's work.

In 2017 ENISA built upon these efforts and improved its cooperation with the NLO Network as the first point of contact for ENISA in the Member States.

ENISA has kicked off various activities aiming at strengthening the cooperation with its National Liaison Officers (NLO) Network. NLOs are key actors in the agency's daily work.

A meeting of NLOs took place in April 2017 to strengthen ENISA's cooperation with the NLO Network. Particular emphasis was placed on how to improve collaboration, in view of the enhanced role for NLOs discussed at Management Board level.

The agency maintained, and shared with the NLO Network, information on all relevant ENISA projects and activities (e.g. unit responsible for the project, relevant tender results, etc.), while maintaining available online resources and expanding them as appropriate.

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.

In 2017 the Management Board adopted guidelines on the missions, principles and functioning of the NLO Network, thus strengthening its role.

Permanent Stakeholders Group

In 2017 ENISA reinforced the contribution of the Permanent Stakeholders Group to the ENISA work programme. The current Permanent Stakeholders

Group consists of 33 top IT-security experts, who were appointed following an open call for expression of interest for membership in 2017.

The current group is composed of nominated members from two organisations (Europol and Office of the Body of European Regulators for Electronic Communications) and one advisory body (the Article 29 Working Party), and members appointed *ad personam*, amounting to 33 members from all over the European Union, compared with 23 members in the previous group.

These members constitute a multidisciplinary group derived from industry, academia and consumer organisations, and are selected upon the basis of their own specific expertise and personal merits. Three nominated members represent NRAs, data protection authorities and law enforcement authorities.

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 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.

Stakeholders' communication and dissemination activities

In 2017 ENISA sought improve its focus on key activities and engage the highest possible number of stakeholders. This includes the institutional stakeholders (e.g. EU Institutions) and other various groups of such as academia, industry, citizens, etc.

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

Dissemination activities are the responsibility of the Stakeholder Communication 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 image 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 are planned in different Member States that will strengthen cybersecurity awareness across Europe, fulfilling ENISA's mandate, mission and strategy.

1.5.3 Objective 5.3. International relations

In 2017 the Management Board adopted guidelines on international relations.

1.5.4 Objective 5.4. Compliance and support

The Stakeholder Relations and Administration Department (SRAD) strives to operate a cost-efficient, customer-oriented service.

SRAD has contributed to ENISA's strategy both internally and externally, seeking optimal solutions for delivering on ENISA's mandate.

SRAD seeks to enhance the functionality of the agency's administrative procedures, to provide administration-related services and strategic support and orientation for the agency's strategy.

SRAD oversees a variety of programmes, projects and services relating to personnel, finance, purchasing, technology, facilities management, health, safety, security and much more.

SRAD's aim is to provide high quality services to the whole organisation and external stakeholders to ensure the optimal use of the agency's resources to increase its overall efficiency. Coordination with the IAS, the European Anti-Fraud Office, the ECA, the European Ombudsman, etc. is one of the main tasks in this area. All internal policies related to transparency, the anti-fraud policy, protection of whistle-blowers, declarations of interests, etc. are addressed under this activity.

1.5.4.1 Information technology

IT at ENISA must support the organisation's business processes and provide the platforms and the tools needed by the Core Operations Department for the secure hosting and operation of its IT systems. The focus is on building formal procedures and processes, and outsourcing first-level IT support. Moreover, additional information security tools will be put in place, such as DMARC (Domain-based Message Authentication, Reporting and Conformance) for the agency's email and an intrusion-detection system in cooperation with CERT-EU.

Task	Objective	Target set for 2017	Achieved in 2017
Consolidate systems and applications on a maximum of two platforms	Efficiency	60 %	60 %
Maximise data sharing	Efficiency	60 %	60 %
Move the agency's IT infrastructure progressively to the cloud	Efficiency	50 %	50 %
Business applications will be securely available on the most widely used mobile devices	Availability	70 %	70 %
Continuous operations	Availability	99 %	99 %

1.5.4.2 Finance, accounting and procurement

The key objective here is to ensure the compliance of financial resource management with the applicable rules, and in particular with sound financial management (i.e. the effectiveness, efficiency and economy principles), as set down in the financial regulation. As the agency's resources are derived from the EU budget, management is required to comply with a set of regulations, rules and standards set down by the EU's competent institutions. The Finance, Accounting and Procurement Unit is responsible for high-quality reporting (annual accounts) and contribution to the audit and discharge procedures.

In 2017 preparations were made so that in 2018 the agency will benefit from the deployment of tools used to simplify and automate its work, automated applications (budget reporting, procurement planning), e-Prior (EU Commission platform for the management of the procurement lifecycle, from pre-award to post-award of a contract).

The deployment of tools, coupled with the outsourcing of certain low-value activities, improved the overall resource-management and reporting capacity of the agency.

The aim is to contribute to the agency's annual and multiannual programming, from inception to execution. Financial resources are allocated according to the needs expressed by the organisational units and according to the priorities set by the agency's management.

Key objectives for the year 2017 included high budget-commitment and payment rates, a low number of budget transfers during the year, planned and justified carry-overs and reduced average payment delay.

Task	Objective	Target set for 2017	Achieved in 2017
Deployment of new financial-information systems	Efficiency, better reporting, information quickly provided	80 %	80 %
Budget implementation (committed appropriations for the year)	Efficiency and sound financial management	100 %	99 %
Payments against appropriations for the year (C1 funds)	Efficiency and sound financial management	89 %	88 %
Payments against appropriations carried over from year n – 1 (C8 funds)	Efficiency and sound financial management	95 %	91 %
Payments made within financial regulation time frame	Efficiency and sound financial management	90 %	89 %

1.5.4.3 Human resources

In 2017 work to align ENISA's human resources processes and policies with the reform of the EU Staff Regulations continued with the adoption of implementing rules through the Management Board in line with Article 110 of the Staff Regulations. The agency also managed 11 recruitment procedures. ENISA furthermore adopted a new approach in terms of learning and development, moving towards a learning organisation with a number of activities including new learning opportunities, managerial workshops and an enhanced process to identify strategic learning needs. Various other measures were developed that contributed to a continuous organisational effort to build a high-performance culture (e.g. a new internal mobility policy). In addition, the agency offered several traineeship opportunities enabling young graduates to acquire practical experience and knowledge of EU administration and of the agency's day-to-day work.

Task	Objective	Target set for 2017	Achieved in 2017
Execution of the establishment plan (only temporary-agent posts)	Minimum 95 % as target execution	95 %	88 %
Efficient management of selection procedures	Reduction of time to hire (time between the closure date for applications and the signature of the reserve list by the Executive Director)	5 months	4 to 8 months depending the recruitment procedure
Turnover of staff	Reduction of statutory staff turnover (temporary agents and contract agents)	< 12 %	8 %

1.5.4.4 Internal communication, legal affairs, data protection and information security coordination

1.5.4.4.1 Internal communication

Internal communication activities aim to keep all those working within the agency informed and to enable both management and staff to fulfil their responsibilities effectively and efficiently. Staff members must be regularly informed of policy decisions taken by the Management Board and ENISA's senior management, enabling them to better understand their role and to acquire a broader knowledge of the agency's mission and activities. This should contribute to a common corporate culture, improve staff engagement and ultimately also improve the implementation of the work programme. Moreover, it is expected that a new internal communications strategy will be completed and implemented in 2018. Thereafter, it is envisaged that an annual review of this strategy will be carried out to ensure that it is kept up to date and appropriate for the agency.

Task	Objective	Target set for 2017	Achieved in 2017
Increase the level of awareness of ENISA's work and recent developments related to the agency	Develop internal communication strategy	80 %	70 %
Increase staff motivation	Bring all staff members and offices closer for better and more fruitful cooperation	80 %	70 % (this indicator will be revised after the staff-satisfaction survey planned for 2018)

1.5.4.4.2 Legal affairs

In 2017 EDO supported the legal aspects associated with the operations of the agency. These include dealing with matters such as contracts, procurement, employment related matters, data protection and corporate governance matters. The Legal Affairs service also managed complaints submitted pursuant to Article 90 of the Staff Regulations and complaints to the European Ombudsman, and represented the agency before the Court of Justice of the European Union.

1.5.4.4.3 Data protection compliance tasks and data protection officer

The main tasks of the data protection officer are as follows.

- Inform and advise ENISA of its obligations pursuant to Regulation (EC) No 45/2001 and document this activity and the responses received.
- Monitor the implementation and application of ENISA's policies in relation to the protection of personal data.
- Monitor the implementation and application of Regulation (EC) No 45/2001 at ENISA, including the requirements for data security, the provision of information to data subjects and their requests in relation to exercising their rights under the regulation, along with the requirements for prior checking or prior consultation with the European Data Protection Supervisor.
- Monitor the documentation, notification and communication of personal data in the context of ENISA's operations.
- Act as ENISA's contact point for the European Data Protection Supervisor on issues related to the processing of personal data.
- Inform and advise ENISA on the current status of the revision of Regulation (EC) No 45/2001 and relevant discussions at EU level.
- Support ENISA in preparing for the transition to the new data protection regulation (action plan).

1.5.4.4.4 Information security coordination

The information security officer (ISO) coordinates the information security management system on behalf of the authorising officer. In particular, the ISO advises the ICT 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 2017 the ISO contributed to such goals as:

- improving ENISA's security posture by planning penetration tests and vulnerability assessments;
- advising on security policies and updating existing ones in line with the evolution of threats and risks;
- improving internal security training for ENISA staff;
- implementing new systems and tools that can support improvements in IT security.

Throughout 2017 several penetration tests of ENISA main portals and platforms took place, together with a comprehensive security-posture assessment. Key priorities in terms of information security were identified for the medium/long term. During the corporate staff meeting the ISO delivered regular security-awareness-raising presentations. An important tool (Microsoft Advanced Threat Analytics) for detecting malicious activities was deployed internally.

1.6 FOLLOW-UP ON THE RESULT AND IMPACT OF ACTIVITIES CARRIED OUT BEFORE 2017

This section aims to summarise the result and impact of activities (work packages) carried out during the previous year, with indicators set to be evaluated in current and later years. Results and impacts can only be measured in the medium and long term.

The result and impact of activities described in the 2016 work programme [18] and reported in the *Annual activity report 2016* [19] for which an impact indicator was set for 2017 are listed in the table below. The table covers only those activities with impact indicators set for longer intervals, and follows the structure and terminology of the 2016 work programme.

18 https://www.enisa.europa.eu/publications/corporate/amending-work-programme-2016

19 https://www.enisa.europa.eu/publications/corporate/enisa-annual-report-2016

SO1 — To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security		
WPKs [20], impact indicators	**Results achieved by end of 2016**	**Results achieved by end of 2017**
WPK 1.1. Improving the expertise related to critical information infrastructure		
By 2017, national authorities in at least five Member States use ENISA's recommendations on smart cars.	Over the year, several authorities were involved in the study and the activities of the ENISA Cars Security Expert Group. The agency received valuable input and feedback from the French Ministry of Interior — Gendarmerie Nationale, the German Federal Office for Information Security, the Joint Research Centre, the French Network and Information Security Agency and Kuratorium Sicheres Österreich.	Based on feedback received by stakeholders from several authorities, six Member States use ENISA's recommendations. In addition to national authorities, the European Automobile Manufacturers' Association [21] published principles of automotive cybersecurity based on the work done in the ENISA study of 2016.
By 2017, national authorities in at least five Member States use ENISA's recommendations on smart health devices, services and infrastructure.	ENISA built this study based on healthcare organisations (hospitals) from across the EU, namely with representatives from Oulu University Hospital, Finland; Hospital Clinico San Carlos, Madrid, Spain; HUG Geneva Hospitals, Switzerland; the Association of Hospitals in Vienna, Austria; NHS Digital, United Kingdom; the National Oncology Hospital of Sofia, Bulgaria; Jena University Hospital, Sweden; and Munich Municipal Hospital, Germany.	Based on interviews and comments received by representatives of national authorities, 14 Member States used ENISA's recommendations either fully or partially by the end of 2017. In addition, other hospitals and national authorities used the ENISA recommendations, specifically SPMS, Portugal; UMC Sint Pieter, Belgium; the Belgian Federal Public Health Service; the General Hospital of Famagusta and General Hospital of Nicosia, Cyprus; the Federal Ministry of Health, Germany; Healthcare Innovation of Southern Denmark; the Centre de Seguretat de la Informació de Catalunya (Cesicat), Spain; Hopitaux du Leman, France; the Croatian Institute for Health Insurance; HSE Ireland; and Humanitas University Hospital Milan, Italy
By 2017, national authorities in at least five Member States use ENISA's recommendations on smart airports.	The study involved several major airports across Europe and related entities such as the European Commission, the European Aviation Safety Agency, the SESAR Joint Undertaking, Eurocontrol and Airports Council International Europe.	National authorities from six Member States have provided feedback to ENISA that they fully or partially use these recommendations. ENISA's recommendations have been validated by key stakeholders, including several national authorities and representatives of national authorities. The study was extended to other national authorities, such as Belgocontrol, Athens International Airport, Geneva Airport, Hungarocontrol, the International Air Transport Association, SITA, Schiphol Airport and Fraport.
WPK 1.2: Network and information security threat landscape analysis		
By 2017, results produced are referenced by at least 500 stakeholders in the area of threat/risk assessment.	ENISA threat landscape results have been reused by multiple stakeholders, both within and outside the EU. In various discussions, blogs and presentations, references to the ENISA threat landscape report 2016 have also been found widely referenced on different social networks. During the first week of dissemination, the ENISA threat landscape report 2016 was disseminated via social media at the following rates: around 200 views and 70 likes on LinkedIn, around 2 000 impressions on Twitter, around 15 retweets and around 50 engagements. This response from the community is considered successful. Additional analytics will be obtained after a sufficient window of time.	Following the trend of previous years, ENISA's threat landscape report has been referenced by a large number of stakeholders within and outside the EU. References are within expert presentations, reports and educational material used on university courses. It has been disseminated on social media with over 2 000 views and around 100 likes. Moreover, it has been used within business assessments, university courses and as a reference for risk assessments. In 2017 ENISA organised an event on cyberthreat intelligence that attracted around 140 participants and created a significant impact in the domain of cyberthreat intelligence. In 2017 ENISA also launched an ETL tool that has attracted the attention of the community.

20 WPK – Work Package in the WP 2016 corresponds to Objectives in Wp2017.

21 The association's members include all EU car manufacturers and its associated organisations cover all Member States.

SO1 — To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security

WPKs [20], impact indicators	Results achieved by end of 2016	Results achieved by end of 2017
WPK 1.2: Network and information security threat landscape analysis		
By 2017, results produced are downloaded by at least 10 000 individuals.	Various ENISA threat landscape reports (ENISA threat landscape and thematic landscapes) were downloaded by more than 20 000 individuals in 2016. These numbers refer to 2015 deliverables disseminated in 2016. For the time being, and after around 1 week of dissemination, the uptake of ENISA 2017 deliverables has seen around 2 500 downloads.	ENISA results in the area of cyberthreats and threat landscape have been downloaded several tens of thousands of times and were referenced in many reports and presentations, both in 2016 and in 2017.

SO2 — To assist the Member States and the Commission in enhancing capacity building throughout the EU

WPKs, impact indicators	Results achieved by end of 2016	Results achieved by end of 2017
WPK 2.1. Assist Member States' capacity building		
WPK 2.1.B. Assistance in the area of cybersecurity strategies		
By 2017, 10 Member States use ENISA's good practices on NCSS.	Experts from Belgium, Bulgaria, Denmark, Estonia, Ireland, Greece, Spain, France, Croatia, Luxembourg, Hungary, Malta, Austria, Slovenia, Finland and Sweden have provided information and are including ENISA's recommendations in their national strategies.	Austria, Belgium, Bulgaria, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Greece, Hungary, Ireland, Luxembourg, Latvia, Malta, Portugal, Slovakia, Slovenia, Spain, Romania, Sweden and Norway (EFTA) are using ENISA's recommendations in their national strategies.
By 2017, 15 private organisations use ENISA's good practices on NCSS.	Experts from 15 private organisations have provided information and are including ENISA's recommendations in their national strategies.	Experts from 16 private organisations have provided information and are including ENISA's recommendations in their national strategies.
By 2017, 10 Member States use ENISA's good practices on national PPPs.	Experts from Belgium, Bulgaria, Denmark, Estonia, Ireland, Greece, Spain, France, Croatia, Luxembourg, Hungary, Malta, Austria, Slovenia, Finland and Sweden have provided information and are including ENISA's recommendations in their national strategies.	In addition to those mentioned for 2016, experts from the Czech Republic, Germany, the Netherlands, Austria, Poland, Portugal, Slovakia and Finland also include ENISA's recommendations in their strategies. The total number of Member States using ENISA's recommendations by 2017 was 24.
By 2017, 15 private organisations use ENISA's good practices on national PPPs.	Experts from 15 private organisations have provided information and are including ENISA's recommendations in their national strategies.	15 private organisations in addition to those involved in 2016 provided information to the activities under national cybersecurity strategies in ENISA. Overall, 30 private organisations are using ENISA's good practices either fully or partially.
WPK 2.2. Support European Union institutions' capacity building		
WPK 2.2.A. Information notes on NIS: production and review mechanisms ('info notes')		
In 2017, improve information flows regarding NIS issues between the EU institutions.	In 2016 information and feedback from different EU institutions were used for the creation of and as reference within various info notes. In the same way, info notes for on-demand topics were created.	In 2016 and 2017 the ENISA cybersecurity info note was a frequently referenced source in the European and international community. Examples are the notes on WannaCry, supply chain attacks, Mirai, etc.
In 2017, improve the mechanism for producing and distributing info notes.	In 2017 info notes will be contextualised according to ENISA's threat landscape and their content will be updated as deemed necessary in order to provide a more coherent representation of NIS occurrences in the two work packages.	In 2016 and 2017 the cybersecurity info note was rebranded, introducing a better contextual link to other ENISA work, such as the ENISA threat landscape and its dedicated application.

SO3 — To assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security		
WPKs, impact indicators	**Results achieved by end of 2016 (Annual activity report 2016)**	**Results achieved by end of 2017**
WPK 3.1. Supporting European Union policy development		
WPK 3.1.A. Contribution to EU policy linked to secure infrastructure and services		
By 2017, 15 companies and five Member State competent authorities contribute to ENISA's efforts in the area of cloud computing.	ENISA involved more than 15 companies and five Member State competent authorities in the efforts under cloud security (Secure Cloud and the paper).	In total, more than 45 companies and a total of 14 Member States have been involved and have contributed to the efforts under cloud security. The 4th edition of Secure Cloud in Dublin, Ireland organised by ENISA together with CSA and Frauhofer FOKUS attracted an audience of over 150 participants from over 45 companies. 34 speakers in the conference represented private-sector organisations. Representatives from 14 Member States participated in the audience, while speakers from 7 Member States made up the conference agenda.
By 2017, 15 companies and five Member State competent authorities contribute to ENISA's efforts in the areas of smart grids or ICS [22]/ supervisory control and data acquisition.	ENISA involved more than 15 companies and five Member State competent authorities in the various activities of the ICS Stakeholder Group and EuroSCSIE over the course of the year, including the members-only meeting co-hosted with MSB in Sweden. Moreover ENISA organised open sessions on network attacks on ICS/supervisory control and data acquisition in Frankenthal, Germany in September 2016 and another one during the 4SICS Security in Industrial Control Systems summit in Stockholm in October 2016.	In addition to the results of 2016, the annual European Supervisory Control and Data Acquisition and Control System Information Exchange/ENISA Industry 4.0 Cyber Security Experts Group meeting was held in October 2017 in Sweden. Private-sector operators and experts from national authorities from France, Germany, the Netherlands, Sweden and Switzerland participated.
By 2017, 10 companies and five Member State competent authorities contribute to ENISA's efforts in the area of certification of components and systems.	There were almost 70 participants (six Member States and more than 30 private companies) at the certification workshop organised in March.	More than 30 stakeholders from private companies and Member State representatives have participated in the support activities.
By 2017, 10 companies and five Member State competent authorities contribute to ENISA's efforts in the area of finance.	ENISA's Expert Group on Finance grew to 35 members, all of whom contributed to the papers published in the finance area. ENISA was also involved in collaboration with the 28 Member States in the regulatory working groups on the implementation of payment services directive 2.	ENISA's Expert Group on Finance grew to 35 members, all of whom contributed to the papers published in the finance area. ENISA was also involved in collaboration with the 28 Member States in the regulatory working groups on the implementation of payment services directive 2.
WPK 3.2. Supporting European Union policy implementation		
WPK 3.2.A. Assist Member States and the Commission in the implementation of the NIS directive		
By 2017, 10 Member States contribute to ENISA's efforts for harmonised implementation of the NIS directive.	ENISA has engaged with almost all Member States in its effort to develop guidelines that can contribute to the proper implementation of the NIS directive across the EU. More than 20 Member States answered the surveys launched on the NIS directive.	In addition to the results from 2016, in 2017 ENISA supported the NIS Directive Cooperation Group by drafting and commenting upon the guidelines produced by the group. During these activities the agency engaged with almost all Member States. More than 20 Member States answered the surveys launched and commented on the draft guidelines of the Cooperation Group.

22 Industrial Control Systems

SO3 — To assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security

WPKs, impact indicators	Results achieved by end of 2016 (Annual activity report 2016)	Results achieved by end of 2017
By 2017, 20 major private organisations contribute to ENISA's efforts for harmonised implementation of the NIS directive.	The work developed by ENISA in the area of incident reporting and security measures engaged a lot of private companies that had a direct interest in providing useful information to ENISA. Although only 20 private organisations answered the online surveys launched by ENISA, the number was much bigger during workshops and other activities.	An additional 58 private organisations contributed to ENISA's efforts by answering online surveys related to the harmonised implementation of the NIS directive. Moreover, in 2017 a large number of private organisations contributed to ENISA's efforts via workshops and other activities.
By 2018, five Member States deploy ENISA's guidelines on the NIS directive in three sectors/ services.	To be determined in 2018.	Results to be assessed only in 2018 as the NIS directive transposition deadline is in May 2018.
By 2018, 10 private organisations deploy ENISA's guidelines on the NIS directive in three sectors/services.	To be determined in 2018.	Results to be assessed only in 2018 as the NIS directive transposition deadline is in May 2018.
WPK 3.2.C. Assistance in the implementation of mandatory incident-reporting schemes		
By 2017, 15 Member States make direct use of the outcomes of Article 13a work by explicitly referencing it or by adopting it at national level.	Almost all Member States take part in Article 13a workshops. All Member States have adopted the incident-reporting thresholds and made direct use of the Article 13a work.	Almost all Member States take part in Article 13a workshops. All Member States have adopted the incident-reporting thresholds and made direct use of the Article 13a work.
By 2017, 10 major e-communication providers across the EU comply with ENISA's minimum security measures.	More than 40 e-communication providers have taken part in the survey launched by ENISA in the area of security measures. All of them have declared a certain level of compliance with the general security measures proposed by ENISA.	More than 40 e-communication providers have taken part in the survey launched by ENISA in the area of security measures. All of them have declared a certain level of compliance with the general security measures proposed by ENISA. The SS7 survey had 39 respondents in 2017. The project checked EU level status as regards signalling security.
By 2017, 15 Member States contribute to ENISA's efforts on the harmonised implementation of Article 19 of the eIDAS regulation.	Three meetings of the eIDAS Article 19 expert group were organised in 2016. On average more than 15 Member States participated in each of them.	20 Member States contributed to ENISA's efforts on the harmonised implementation of Article 19 of the eIDAS regulation

SO4 — To enhance cooperation both between the Member States of the EU and between related NIS communities

WPKs, impact indicators	Results achieved by end of 2016 (Annual activity report 2016)	Results achieved by end of 2017
WPK 4.2: Network and information security community building		
In 2017, enhanced operational community efforts (e.g. operational cooperation, information exchange).	ENISA helped existing communities by participating in their governance structures (TF-CSIRT Steering Committee) or the FIRST Conference Programme Committee.	ENISA's work also positively recognised in other CSIRT structures, e.g. reference incident classification taxonomy in TF-CSIRT-TI, CSIRT maturity assessment framework in FIRST and the Global Forum on Cyber Expertise.

PART II
MANAGEMENT

2.1 BUDGETARY AND FINANCIAL MANAGEMENT

2.1.1 Budget execution of EU subsidy (C1 funds)

The excellent budget execution can be translated into the following figures: the expenditure appropriations for ENISA's 2017 budget of EUR 10 608 964 were committed at a rate of 99.99 % as at 31 December 2017.

ENISA did not cancel any C1 appropriations of the year (cancellation rate 0.00 %).

The overall performance demonstrates the already proven capacity 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 88.19 % in 2017. This payment rate is high and demonstrates that the agency's capacity 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 (2016) and enabled the agency to launch projects related to the work programme in early 2017, contributed significantly to the improvement of the payment rate of appropriations of the year (C1).

2.1.2 Amending budgets/budgetary transfers

The following table summarises the impact of budgetary transfers Nos 1 to 6 (approved by the Executive Director of ENISA) on the initial 2017 budget.

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

	Initial budget	2017 budget transfers 1 -6 approved by the Executive Director	Appropriations after transfer 1-6
Title 1	6 387 979.00	0.00	6 387 979.00
Title 2	1 770 700.00	– 45 070.00	1 725 630.00
Title 3	3 086 000.00	45 070.00	3 131 070.00
Total	**11 244 679.00**	**0.00**	**11 244 679.00**

The following table summarises the subsequent impact of the amending budget 1/2017 (approved by the Management Board).

Table — Summary of amending budget 1/2017 impact on budget

	Appropriations after transfer 1-6	Amending budget 1/2017	New appropriations 2017 (amending budget 1/2017)
Title 1	6 387 979.00	14 638.30	6 402 617.30
Title 2	1 725 630.00	– 132 500.01	1 593 129.99
Title 3	3 131 070.00	48 408.20	3 179 478.20
Total	**11 244 679.00**	**– 69 453.51**	**11 175 225.49**

The table below summarises the impact of budget transfers Nos 7 to 10 (approved by the Executive Director after the adoption of amending budget 1/2017) on the final budget execution.

Table — Summary of the budgetary transfers 7 to 10 impact on budget

	New appropriations 2017 (amending budget 1/2017)	2017 budget transfers 7-10 approved by the Executive Director	Final budget execution 2017
Title 1	6 402 617.30	– 4 188.09	6 398 429.21
Title 2	1 593 129.99	7 182.47	1 600 312.46
Title 3	3 179 478.20	– 2 994.38	3 176 483.82
Total	**11 175 225.49**	**0.00**	**11 175 225.49**

5.2.1 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 2017 were carried forward (automatic carry forward) to 2018 (C8 appropriations).

The commitment appropriations corresponding to the subsidy from the Greek authorities for the lease of the ENISA premises in Greece (external assigned revenue — R0 appropriations) that were not paid by 31 December 2017 were carried forward (automatic carry forward to R0 appropriations 2018).

The funds carried forward to 2018 (C8 appropriations) are detailed below:

Table — Summary of carry forwards 2017 to 2018

Title	Total C1 appropriations carried forward to 2018	Subsidy from Greek authorities carried forward (R0 2017 to R0 2018)	Total amount carried forward from 2017 to 2018
Title 1 — Staff	482 509,75	0,00	482 509,75
Title 2 — Administration	430 128,27	26 370,24	456 498,51
Title 3 — Operations	498 802,49	0,00	287 569,77
Total	**1 411 440,51**	**26 370,24**	**1 437 810,75**

The total of cancelled appropriations carried forward from 2016 to 2017 (C8 appropriations of 2017) but finally not paid in 2017 was EUR 90 916.34.

2.1.3 Types of procurement procedures

In 2017 a total of 40 procurement procedures were launched, resulting in 38 contracts being signed (nine framework contracts, 13 service contracts, one works contract and 15 specific contracts awarded under re-opening of competition). Also, 340 purchase orders (175 of which were issued under pre-existing framework contracts) were signed.

2.1.4 Interest charged by suppliers

During 2017 the agency had to pay EUR 2 393.93 of interest to its suppliers as result of exceeding the payment terms agreed with the suppliers.

2.2 MANAGEMENT OF HUMAN RESOURCES

2.2.1 Human resources

At the end of 2017, 74 statutory staff were employed by the agency (42 temporary agents, 29 contract agents and three seconded national experts). 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 the schooling for ENISA staff members 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 staff members. Several children of staff members at ENISA Heraklion attended the European School in Heraklion in 2017, which offers education at the following levels: nursery, primary and secondary education. ENISA has a service-level agreement with the Commission's DG Human Resources and Security for the provision of these services.

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

2.2.2 Results of screening

Following the European Commission's methodology, the agency performed the 'job screening' benchmarking exercise for 2017. The result of the exercise, which is a snapshot of the staffing situation as at the end of December 2017, appears in Annex A.4. It is relevant to mention that the 'Overhead', support functions, represents only 19.28 % of the total statutory staff count, which is below the 25 % maximum value accepted for the agencies. This is only possible due to very efficient resource management.

2.3 ASSESSMENT BY MANAGEMENT

2.3.1 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 of the payments concerned. In order to achieve the best control possible the agency has focused intensively on the verification of results before transactions are initiated (*ex ante* verification).

In line with ICS 8 (Processes and procedures), the agency has produced the *ex post* control report for the financial year 2016. The recommendations issued in the report were addressed during the year.

The *ex post* controls of the financial year 2016 were quite extensive. A total of 234 financial transactions were sampled and checked, representing 11.62 % of all of the agency's financial transactions and representing 65.15 % of the agency's 2016 budget. As a result, one recommendation was issued regarding a delay of payment that did not generate any interest to be paid.

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 the improvement in the agency's overall internal control environment and performance.

2.4 BUDGET IMPLEMENTATION TASKS ENTRUSTED TO OTHER SERVICES AND ENTITIES

The agency did not entrust budget implementation to other services and entities.

2.5 ASSESSMENT OF AUDIT RESULTS AND FOLLOW-UP OF AUDIT RECOMMENDATIONS

2.5.1 Internal Audit Service

The agency had no open recommendations from the IAS in 2017. In September 2016 the IAS performed the agency's risk assessment. The report showed the next three topics for auditing: stakeholders' involvement in the deliverables, human resources and IT. The agency will take immediate action to construct a quality management system and implement its risk-management policy. The audit on stakeholders' involvement in the deliverables was performed during the last week of September 2017. The draft report will be communicated to the agency in the second quarter of 2018.

2.5.2 European Court of Auditors

Issued in 2017, the 2016 ECA report on the annual accounts does not contain any recommendations.

2.5.3 Follow-up of audit plans, audits and recommendations

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

2.6 FOLLOW-UP OF OBSERVATIONS FROM THE DISCHARGE AUTHORITY

2.6.1 2015 discharge

Regarding the European Parliament decision of 27 April 2017, the Executive Director of the agency was granted discharge in respect of the implementation of the agency's budget for the financial year 2015. The closure of the accounts *of the agency for the financial year* 2015 was also approved [23].

2.6.2 Measures implemented in response to the observations of the discharge authority

The following table presents a summary of the main observations and comments by the discharge authority on the implementation of the 2015 budget and the measures taken by ENISA.

23 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0175+0+DOC+XML+V0//EN

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 next section).
Considerable delay in the payment of rent for the offices in Athens by the Greek authorities.	The agency made continued significant efforts in liaising with the Greek authorities in order to remedy the situation. However, ENISA is dependent on the good will of the Greek authorities.
Difficulty to recruit, attract and retain suitably qualified staff.	The agency has implemented social measures (e.g. food vouchers, increased education allowances) to attract and retain qualified staff.
Adoption of internal rules on whistleblowing during the first quarter of 2017.	Internal rules on whistleblowing have been drafted and are under discussion for formal validation by upper management.
Absence of publication on the website of the CVs and declarations of interests of the agency's Management Board members and of its Executive Board.	Declarations of interest and of commitment of ENISA Management Board representatives can be found here: https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/mb2017 Only the CV of the Chair of the Management Board is currently available on ENISA's website: https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/jean-baptiste-demaison-cv
Transparency to improve in contacts with lobbyists and stakeholders.	In accordance with its legal basis ENISA has to maintain regular dialogue with the private sector, consumer organisations and academic experts. Internal rules have been adopted to define and clarify the relationship between ENISA and its stakeholders to guarantee transparency. Furthermore, the members of the Management Board are only required to provide annual declarations of interest and annual declarations of commitments. These declarations have been published on ENISA's website.

2.7 COMPLIANCE REGARDING TRANSPARENCY, ACCOUNTABILITY AND INTEGRITY

The agency is committed to operating as an open and transparent organisation. To help citizens and other stakeholders understand how the agency is managed and held accountable, 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 highest governing body of the agency. It is composed of representatives of the Member States and the Commission. Its main role is to ensure that the agency carries out its tasks in accordance with its operational and strategic objectives, as adopted 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 and the minutes of the meetings and adopted decisions (including annual and multiannual work programmes) are published on ENISA's website.

The Management Board has also the responsibility to appoint 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 to 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 Council, the European Parliament, 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 the 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 aware about fraud prevention. As of 2018 fraud-awareness training is included in the yearly ethics and integrity training, which is compulsory for all staff.

In addition to the Staff Regulations the agency has introduced 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 is implementing a 2-week deadline to answer requests from citizens.

PART III

ASSESSMENT OF THE EFFECTIVENESS OF THE INTERNAL CONTROL SYSTEMS

3.1 RISK MANAGEMENT

The agency was previously using the risk assessment done by the IAS in 2012. In September 2016 the IAS produced a new risk assessment with an audit plan that started in 2017.

3.2 COMPLIANCE AND EFFECTIVENESS OF INTERNAL CONTROL STANDARDS

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

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

The agency has also put in place 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.

In 2010 the Management Board of the agency adopted a set of 16 ICS 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.

In 2014 the agency focused on compliance with the standards that were identified as areas of concern during the risk assessment exercise and on the recommendations raised by the auditing bodies (ECA and IAS). During 2017 the agency achieved compliance with the ICS listed below.

Mission (ICS 1)

The agency's mission and scope is described in the ENISA regulation. Mission statements for departments and units were established based on the evolution of the organisation in 2017. The roles and tasks of each department and unit are clearly defined.

Ethical and organisational values (ICS 2)

The agency has procedures in place — including updates and yearly reminders — to ensure that all staff are aware of relevant ethical and organisational values (e.g. ethical conduct, avoidance of conflicts of interest, fraud prevention, reporting of irregularities). Specific training is organised by the agency for its staff every year in order to reinforce professional behaviour, compliance with the expected behaviour, ethics and integrity, and in order to prevent workplace harassment.

Staff allocation and mobility (ICS 3)

In 2017 ENISA implemented some structural organisational adjustments with the objective of

increasing the agility of the organisation in adapting swiftly to new and diverse challenges. Additionally, two staff moved voluntary from Crete to Athens.

Staff evaluation and development (ICS 4)

In 2017 the performance-management exercise (annual appraisal and reclassification) took place successfully, with only one appeal on the annual appraisal, well below the rate of appeals in other EU organisations. Both exercises were conducted in line with the Staff Regulations and related implementing rules. Comprehensive and practical guidelines for staff and managers have been issued in order to the exercise to be a continuous process that improves employee engagement and drive business results.

The adopted 2017 learning and development plan offered further diversification of learning pathways with the use of the various Commission framework contracts, addressing learning at and through work, knowledge sharing, training modules, language courses, etc.

Objectives and performance indicators (ICS 5)

The 2017 work programme, part of the 2017-2019 programming document, was developed by the agency's services, with continuous input and guidance from its two governing bodies, the Management Board and the Permanent Stakeholders Group. The programming document clearly sets out how the planned activities at each management level contribute to the achievement of objectives, taking into account the resources allocated and the risks identified. The programming document's objectives are established on SMART (specific, measureable, achievable, relevant, time-bound) criteria and are updated or changed during the year in order to address significant changes in priorities and activities.

The role of the Executive Board is to assist in preparing decisions to be adopted by the Management Board on administrative and budgetary matters only.

The agency has based the measurement of its performance on key performance indicators that are applied to all areas of activity. Key performance indicators are more qualitative for the agency's operational goals, whereas they are more quantitative for the agency's administrative goals. The effectiveness of key controls is assessed using relevant key performance indicators, including self-assessments that have been carried out in the form of progress reports and follow-up actions that seek to realign divergences from the work programme.

ENISA installed the project management tool Matrix, which has streamlined and consolidated the planning, monitoring and reporting functions in a uniform and comprehensive way.

Finally, the agency again managed to optimise the budget execution for 5 consecutive years. The commitment rate of budget appropriations available for the year 2017 (C1) reached 99.99 %.

Risk-management process (ICS 6)

The agency did not have any open audit recommendations for 2017. The IAS performed a risk assessment of the agency in September 2016. The report showed the next three topics for auditing: stakeholders' involvement in the deliverables, human resources and IT. The agency will take immediate action to construct a quality management system and to implement its risk-management policy.

The first audit topic on involvement of stakeholders on ENISA deliverables was performed during the last week of September 2017. The draft report will be communicated to the agency in the first half of 2018.

The agency again managed to optimise the budget execution for 5 consecutive years. The commitment rate of budget appropriations available for the year 2017 (C1) reached 99.99 %.

Operational structure (ICS 7)

Delegation of authority is clearly defined, assigned and communicated by means of the Executive Director's decisions. It conforms to regulatory requirements and is appropriate to the level of importance of the decisions to be taken as well as the risks involved. All delegated authorising officers have received and acknowledged the charter of the role and responsibility of the authorising officer (by delegation), along with the individual delegation Executive Director's decision.

The agency's sensitive functions are clearly defined, recorded and kept up to date.

As regards sensitive functions, due care has been taken to avoid potential conflict-of-interest situations. However, due to the small size of the agency, the mobility of staff in sensitive functions is very limited and takes into account service needs and available resources. Proper back-ups are designated in order to ensure business continuity and adequate segregation of duties.

Processes and procedures (ICS 8)

Several policies were developed to strengthen the processes and procedures ICS. The agency created a policy on financial circuits. The roles and responsibilities of financial actors are described in this policy, along with existing workflows (see comment on the 'Paperless' application in ICS 11).

A code of professional conduct for *ex ante* financial verification was developed. The document emphasises the role and responsibilities of the financial verifying agent.

The agency proceeded in 2017 with the full 2016 *ex post* control exercise, and it will deliver the 2017 *ex post* control report in the first semester of 2018.

Management supervision (ICS 9)

Management at all levels supervises the activities for which they are responsible and tracks the main issues identified. The management team, which comprises the Executive Director and the heads of departments and units, meets on a monthly basis and sets priorities for the actions to be taken in order to achieve the short- and medium-term objectives of the agency. A list of action items is compiled. It contains all agreed actions as allocated to specific departments or units. The list is published on a dedicated intranet page and regularly reviewed by the management team. Besides the monthly management team meeting, a heads-of-unit meeting is organised every week. Management supervision covers both legality and regularity aspects (i.e. set-up and compliance with applicable rules) and operational performance (i.e. achievement of programming-document objectives).

Management also establishes action plans in order to address accepted ECA and IAS audit recommendations and monitors the implementation of these action plans throughout the year.

Business continuity (ICS 10)

Adequate measures — including handover files and deputising arrangements for relevant operational activities and financial transactions — are in place to ensure the continuity of all services during 'business-as-usual' interruptions (such as sick leave, staff mobility, migration to new IT systems, incidents, etc.).

An IT business continuity plan (BCP) has been developed and implemented. An agency-wide BCP, designed to cover crisis response and recovery arrangements with respect to major disruptions, has been developed and fully implemented. The agency BCP's identifies the functions, services and infrastructure that need to be restored within certain time limits and the resources necessary for this purpose. Electronic and hard-copy versions of both BCPs are stored in secure and easily accessible locations that are known to relevant staff.

Document management (ICS 11)

Document-management systems and their related procedures comply with: (1) relevant compulsory security measures; (2) provisions on document management; and (3) rules on the protection of personal data. Information security policy specific to data categorisation and labelling is in place. As regards the exchange of information classified at the 'Restreint UE/EU restricted' level, an administrative arrangement between the Security Directorate of the European Commission and the agency was signed on 27 May 2011.

An internal document-management guide sets out the conditions according to which documents need to be registered, filed and saved using the agency's registration and filing systems. A special, intranet-based tool was developed to capture the information needed to register and retrieve documents. In addition, an incoming- and outgoing-mail procedure was developed.

As regards the financial and administrative workflows, in January 2015 ENISA adopted a SharePoint-based application, 'Paperless', which routes documents to staff involved in the preparation, review and approval of all kinds of work-related documents and transactions. All financial and administrative workflows are well documented and all supporting documents are uploaded and stored in 'Paperless', including changes and comments by workflow actors. Approved workflows are permanently stored and an appropriate audit trail is produced.

Information and communication (ICS 12)

Internal communication measures and practices are in place for sharing information and monitoring activities. These include regular Management Team meetings during which issues relevant to

performance, audit results and financial information are discussed and actions are decided upon and assigned. Regular financial reporting is available to all staff on ENISA's intranet. All engagements in new projects are discussed during the implementation of the annual work programme and decisions are documented and communicated.

An external communication strategy is in place. ICT security policies are in place for main systems and subsystems and are described in procedures and policies. Internal communication is also supported through use of the intranet and through weekly staff meetings within units. External communication and dissemination procedures must be further developed and communicated to staff accordingly.

The weekly staff meeting is used as a platform for communication between all departments. Every week staff members can share their work with the rest of the agency.

Accounting and financial reporting (ICS 13)

All finance and accounting procedures are documented in the agency's internal control manual. The preparation, implementation, monitoring and reporting on budget implementation is centralised in the Finance, Accounting and Procurement Section, within the Stakeholders Relations and Administration Department. The European Commission's budget and accounting management system, ABAC, is the main tool used for financial management. It is compliant with applicable financial regulatory frameworks. The ABAC Assets module is used for the management of ENISA's inventory. Financial management information produced by the agency, including financial information provided in the annual activity report, complies with applicable financial and accounting rules.

Evaluation of activities (ICS 14)

Key performance indicators are used in order to measure the performance and assess the impact of the agency's projects as provided for in its annual work programmes. The general report and the annual activity report are the tools used by the agency to report on performance and impact. The feedback of relevant stakeholders is taken into account.

Assessment of internal control systems (ICS 15)

Each year ENISA's management assesses the compliance of annual activities and performance with the internal control systems in place, as part of preparation of the annual activity report.

Internal audit capability (ICS 16)

The head of the Stakeholder Relations and Administration Department assumes the internal control coordination function. He is responsible for implementing internal control systems in the agency and liaising with the IAS of the European Commission. Given the limited size of the agency, the role of internal audit capability cannot be performed. Since 2005 the agency has relied on the IAS to carry out internal audits. The IAS plays a key role in auditing bodies of the European Union.

Internal control tasks performed in ENISA include 100 % of *ex ante* verifications, annual *ex post* controls, hierarchical controls and outsourced engagements, coordinated by the internal control coordination. The role of internal control coordination was reinforced in order to comply with all the recommendations issued by the IAS and ECA.

Concerning the overall state of the internal control system, generally the agency complies with the three assessment criteria for effectiveness: (1) staff that have the required knowledge and skills; (2) systems and procedures designed and implemented to manage the key risks effectively; and (3) no instances of ineffective controls that have exposed the agency to substantial risk.

Enhancing the effectiveness of the agency's control arrangements is an ongoing effort, as part of the continuous improvement of management procedures. It includes taking into account any control weaknesses reported and exceptions recorded.

IV

PART IV
MANAGEMENT ASSURANCE

4.1 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 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 on the next page.

	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 budget lines opened and budget lines ownership, appropriations 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 evaluation.	Organise annual performance evaluation. Administer appeals.	Number of evaluations carried out.
5	Annual training programme.	Draft the generic training plan of the agency.	Document presentation and implementation of programme.
6	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/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.

4.2 EXCEPTIONS

In 2017 the agency recorded 31 exceptions.

Some of these 31 exceptions are ones that generated interest payments to suppliers. The others are administrative mistakes for which corrective measures have been implemented to prevent the repetition of these errors.

Twenty-five of them are under the materiality levels and are minor administrative mistakes.

Of the six remaining, three *a posteriori* commitments were reported, two were late payments to the European Commission and the last was a purchase order on which the amount exceeded the limit.

The information reported in Parts II and III stems from the results of auditing by management and auditors. These reports result from a systematic analysis of the evidence available. This approach provides sufficient guarantees as to the completeness and reliability of the information reported, and results in complete coverage of the budget delegated to the Executive Director of ENISA.

V

PART V
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.

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.

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

Heraklion, June 2018

Udo Helmbrecht
Executive Director

A

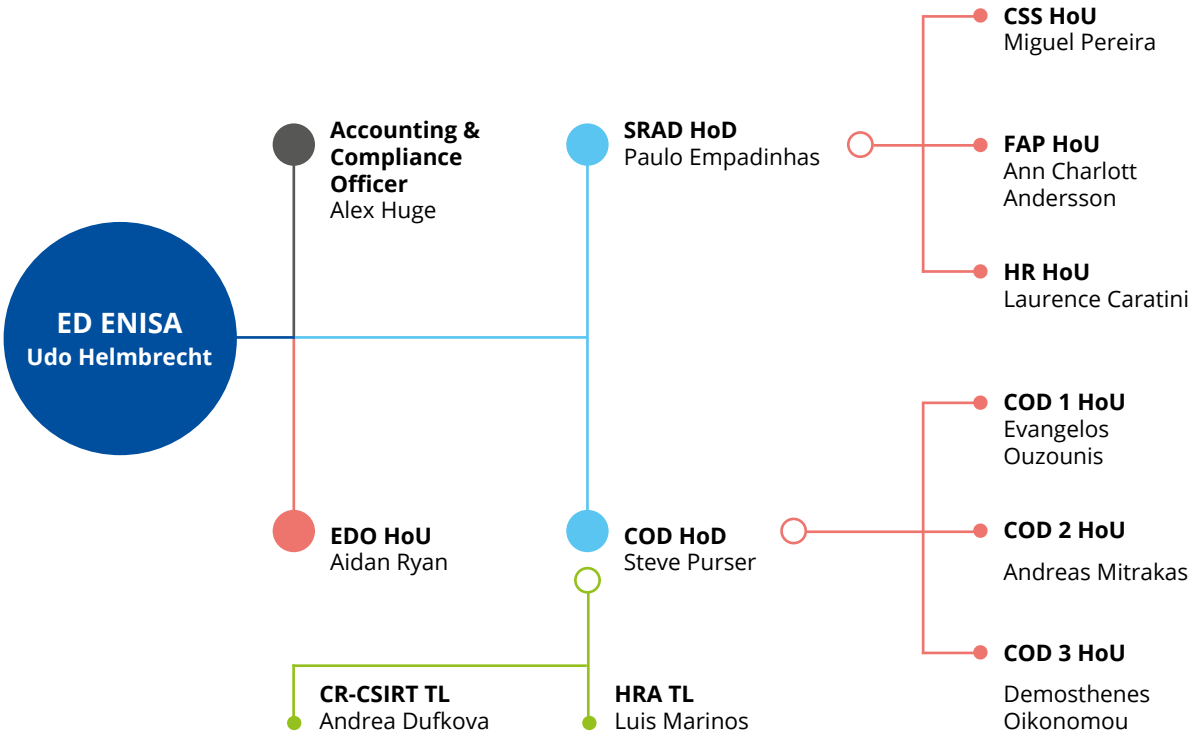
ANNEX 1
HUMAN RESOURCES

A.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 Programme Management
CR – CSIRT Relations
HRA - Horizontal Support & Analysis
TL – Team leader

A.3 ESTABLISHMENT PLAN 2017

Function group and grade (TA/AST)	Posts 2017: Authorised under the union 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		2
AST 3		
AST 2		
AST 1		
AST Total:		**14**
Total Staff:		**48**

A.4 INFORMATION ON ENTRY LEVEL FOR EACH TYPE OF POST

Nr	Key functions	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 Department	TA	AD 11	Top Operations
4	Head of Unit	TA	AD 9	Top Operations
5	NIS analyst	TA	AD 8	Operations
6	Head of Unit	TA	AD 9	Top Operations
7	Head of Unit	TA	AD 9	Neutral
8	Head of Unit	TA	AD 9	Top Operations
9	Head of Unit	TA	AD 9	Administrative
10	Head of Unit	TA	AD 9	Administrative
11	Legal Officer	TA	AD 8	Coordination
12	Network and Information Security — Research and Analysis Expert	TA	AD 8	Operations
13	Expert in Network and Information Security	TA	AD 8	Operations
14	Expert in Network and Information Security	TA	AD 8	Operations
15	Accounting and Compliance Officer	TA	AD 8	Neutral
16	Expert in Network and Information Security	TA	AD 7	Operations
17	Expert in Network and Information Security	TA	AD 7	Operations
18	Network and Information Security — Research and Analysis Expert	TA	AD 6	Operations
19	Expert in Network and Information Security	TA	AD 6	Operations
20	Expert in Network and Information Security	TA	AD 6	Operations
21	Expert in Network and Information Security	TA	AD 6	Operations
22	Expert in Network and Information Security	TA	AD 6	Operations
23	Expert in Network and Information Security	TA	AD 6	Operations
24	Expert in Network and Information Security	TA	AD 6	Operations
25	Expert in Network and Information Security	TA	AD 6	Operations
26	Expert in Network and Information Security	TA	AD 6	Operations
27	Expert in Network and Information Security	TA	AD 6	Operations
28	Expert in Network and Information Security	TA	AD 6	Operations
29	Expert in Network and Information Security	TA	AD 5	Operations
30	Expert in Network and Information Security	TA	AD 6	Operations
31	Expert in Network and Information Security	TA	AD 6	Operations
32	Expert in Network and Information Security	TA	AD 6	Operations
33	Administrative Officer	TA	AD 5	Operations
34	Team coordinator	TA	AD 8	Administrative

Nr	Key functions	Type of contract (Official, TA, CA or SNE)	Function group/ Grade of recruitment	Indication of function dedicated to administrative, support or operations
35	Team Leader	TA	AST 4	Neutral
36	Facilities officer	TA	AST 4	Administrative
37	Procurement Officer	TA	AST 4	Neutral
38	Administrative Assistant	TA	AST 3	Operations
39	HR Assistant	TA	AST 3	Administrative
40	IT Assistant	TA	AST 3	Administrative
41	Assistant	TA	AST 3	Operations
42	Financial Assistant	TA	AST 2	Neutral
43	Personal Assistant to the Executive Director	TA	AST 2	Operations
44	Internal Control and Reporting Officer	TA	AST 2	Neutral
45	Administrative Assistant	TA	AST 1	Operations
46	HR Assistant	TA	AST 1	Administrative
47	Assistant to the Head of Department	TA	AST 1	Operations
48	Team coordinator	TA	AST 4	Neutral
49	Officer in Network and Information Security	CA	FG IV	Operations
50	Officer in Network and Information Security	CA	FG IV	Operations
51	Officer in Network and Information Security	CA	FG IV	Operations
52	Officer in Network and Information Security	CA	FG IV	Operations
53	Officer in Network and Information Security	CA	FG IV	Operations
54	Officer in Network and Information Security	CA	FG IV	Operations
55	Officer in Network and Information Security	CA	FG IV	Operations
56	Officer in Network and Information Security	CA	FG IV	Operations
57	Procurement Support Officer	CA	FG IV	Neutral
58	HR Officer	CA	FG IV	Administrative
59	Team Leader	CA	FG IV	Administrative
60	Press Communication Officer	CA	FG IV	Administrative
61	HR Officer	CA	FG IV	Administrative
62	Financial Officer	CA	FG IV	Neutral
63	Administrative Assistant	CA	FG III	Neutral
64	Officer in Network and Information Security	CA	FG III	Operations
65	Officer in Network and Information Security	CA	FG III	Operations
66	Officer in Network and Information Security	CA	FG III	Operations
67	Officer in Network and Information Security	CA	FG III	Operations
68	Officer in Network and Information Security	CA	FG III	Operations
69	Officer in Network and Information Security	CA	FG III	Operations

Nr	Key functions	Type of contract (Official, TA, CA or SNE)	Function group/ Grade of recruitment	Indication of function dedicated to administrative, support or operations
70	Finance and Procurement Assistant	CA	FG III	Neutral
71	ICT Systems Officer	CA	FG III	Administrative
72	Corporate Communications Assistant	CA	FG III	Coordination
73	Project Assistant	CA	FG III	Operations
74	Financial Assistant	CA	FG III	Neutral
75	Software Developer Officer	CA	FG III	Administrative
76	Facilities Management Assistant	CA	FG I	Administrative
77	Officer in Network and Information Security	CA	FG IV	Operations
78	Officer in Network and Information Security	CA	FG IV	Operations
79	Officer in Network and Information Security	CA	FG IV	Operations
80	Officer in Network and Information Security	SNE	SNE	Operations
81	Officer in Network and Information Security	SNE	SNE	Operations
82	Officer in Network and Information Security	SNE	SNE	Operations
83	Officer in Network and Information Security	SNE	SNE	Operations
84	Officer in Network and Information Security	SNE	SNE	Operations

A.5 INFORMATION ON BENCHMARKING EXERCISE

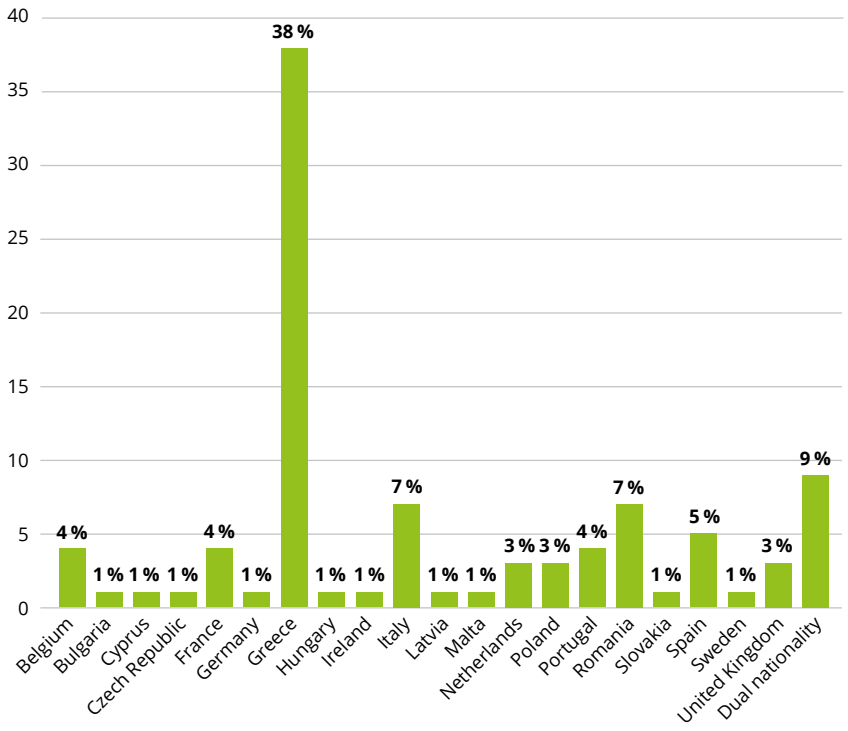
Job Type	2017	2016
Total administrative support and coordination	**19.28 %**	**19.04 %**
Administrative support	15.66 %	15.47 %
Coordination	3.61 %	3.57 %
Total operational	**66.27 %**	**66.66 %**
Top operational coordination	7.23 %	7.14 %
General operational	59.04 %	59.52 %
Total neutral	**14.46 %**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

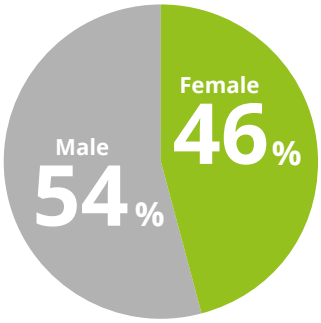
A.6 HUMAN RESOURCES STATISTICS

As of the end of 2017 the agency comprised 74 statutory staff (42 temporary agents, 29 contract agents and three seconded national experts).

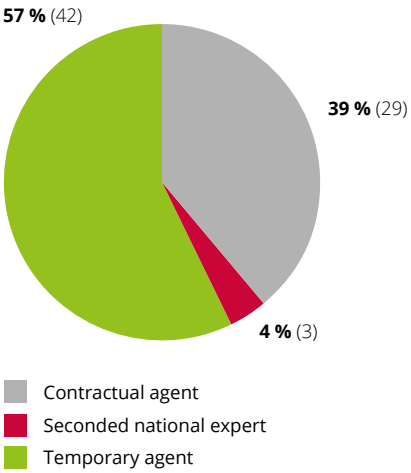
Staff members by Nationality (in percents)



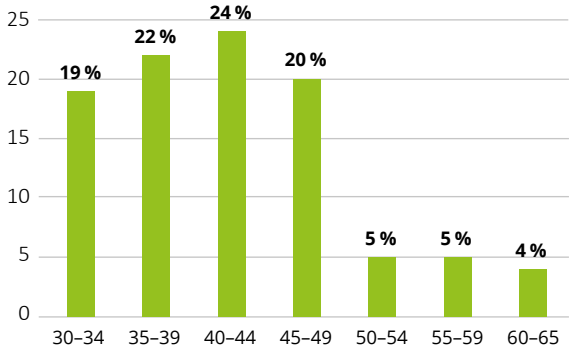
Gender Balance (in percents)



Staff members by Category (in percents)



Age Analysis (in percents)



A.7 HUMAN RESOURCES BY ACTIVITY

Activities	Planned FTEs	Actual FTEs
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**

ANNEX 2
FINANCIAL RESOURCES

B.1 PROVISIONAL ANNUAL ACCOUNTS 2017

Balance Sheet 2017 (in EUR)	2016	2017
NON-CURRENT ASSETS	**891 267**	**657 489**
Intangible assets	864	107 537
Tangible assets	890 403	549 952
CURRENT ASSETS	**1 470 630**	**1 808 377**
Short-term receivables	245 857	230 128
Cash and cash equivalents	1 224 773	1 578 249
ASSETS	**2 361 897**	**2 465 866**
NON-CURRENT LIABILITIES	**-**	**-**
Provisions (long term)	-	-
CURRENT LIABILITIES	**670 842**	**679 135**
European Commission pre-financing received	38 436	85 535
Accounts payable	232 730	110 195
Accrued liabilities	399 676	483 405
Accrued Liabilities	399 676	316 093
Short-term provisions	-	-
LIABILITIES	**670 842**	**679 135**
NET ASSETS	**1 691 055**	**1 786 731**

Statement of financial performance 2017 (in EUR)	2016	2017
OPERATING REVENUES	**10 995 538**	**11 187 610**
Revenue from the European Union subsidy	10 359 496	10 489 442
Other revenue	-	-
Revenue from administrative operations	635 129	698 168
OPERATING EXPENSES	**– 10 560 858**	**– 11 088 523**
Administrative expenses	– 8 260 628	– 8 877 553
Operational expenses	– 2 300 230	– 2 210 970
Adjustments to provisions	-	-
OTHER EXPENSES	**– 1 200**	**– 3 411**
Financial expenses	– 1 020	– 3 399
Exchange-rate loss	– 180	– 12
ECONOMIC RESULT FOR THE YEAR	**433 480**	**95 676**

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).

B.2 FINANCIAL REPORTS 2017

Out-turn on commitment appropriations in 2017				
Chapter		**Commitment appropriations authorised ***	**Commitments made**	**%**
		1	**2**	**3=2/1**
Title A-1 STAFF				
A-11	Staff in active employment	4 674 963.79	4 674 963.79	100.00 %
A-12	Recruitment expenditure	175 432.52	175 196.14	99.87 %
A-13	Socio-medical services and training	169 988.95	169 988.95	100.00 %
A-14	Temporary assistance	1 378 043.95	1 378 043.95	100.00 %
Total Title A-1		**6 398 429.21**	**6 398 192.83**	**99.99 %**
Title A-2 FUNCTIONING OF THE AGENCY				
A-20	Buildings and associated costs	868 135.15	868 135.15	100.00 %
A-21	Movable property and associated costs	25 435.15	25 435.15	100.00 %
A-22	Current administrative expenditure	83 026.87	83 026.87	100.00 %
A-23	Information and communication technologies	623 715.29	623 715.29	100.00 %
Total Title A-2		**1 600 312.46**	**1 600 312.46**	**100.00 %**
Title B-3 OPERATING EXPENDITURE				
B-30	Group activities	943 054.94	943 054.94	100.00 %
B-32	Horizontal operational activities	569 390.45	569 390.45	100.00 %
B-36	Core operational activities	1 664 038.43	1 664 038.43	100.00 %
Total Title B-3		**3 176 483.82**	**3 176 483.82**	**100.00 %**
TOTAL ENISA		**11 175 225.49**	**11 174 989.11**	**99.99 %**

* 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 2017				
Chapter		**Payment appropriations authorised ***	**Payments made**	**%**
		1	**2**	**3=2/1**
Title A-1 STAFF				
A-11	Staff in active employment	4 674 963.79	4 674 963.79	100.00 %
A-12	Recruitment expenditure	175 432.52	173 148.78	98.70 %
A-13	Socio-medical services and training	169 988.95	94 758.49	55.74 %
A-14	Temporary assistance	1 378 043.95	972 812.02	70.59 %
Total Title A-1		**6 398 429.21**	**5 915 683.08**	**92.46 %**
Title A-2 FUNCTIONING OF THE AGENCY				
A-20	Buildings and associated costs	868 135.15	775 783.39	89.36 %
A-21	Movable property and associated costs	25 435.15	20 632.81	81.12 %
A-22	Current administrative expenditure	83 026.87	69 728.86	83.98 %
A-23	Information and communication technologies	623 715.29	436 668.79	70.01 %
Total Title A-2		**1 600 312.46**	**1 302 813.85**	**81.41 %**
Title B-3 OPERATING EXPENDITURE				
B-30	Group activities	943 054.94	847 047.53	89.82 %
B-32	Horizontal operational activities	569 390.45	359 711.54	63.17 %
B-36	Core operational activities	1 664 038.43	1 470 922.26	88.39 %
Total Title B-3		**3 176 483.82**	**2 677 681.33**	**84.30 %**
TOTAL ENISA		**11 175 225.49**	**9 896 178.26**	**88.55 %**

* 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 31.12.2017

Chapter		2017 Commitments to be settled			
		Commitments 2017	Payments 2017	RAL 2017	% to be settled
		1	2	3=1-2	4=1-2/1
Title A-1 STAFF					
A-11	Staff in active employment	4 674 963.79	– 4 674 963.79	0.00	0.00 %
A-12	Recruitment expenditure	175 196.14	– 173 148.78	2 283.74	1.30 %
A-13	Socio-medical services and training	169 988.95	– 94 758.49	75 230.46	44.26 %
A-14	Temporary assistance	1 378 043.95	– 972 812.02	405 231.93	29.41 %
Total Title A-1		**6 398 192.83**	**– 5 915 683.08**	**482 746.13**	**7.54 %**
Title A-2 FUNCTIONING OF THE AGENCY					
A-20	Buildings and associated costs	873 501.64	– 775 783.39	92 351.76	10.64 %
A-21	Movable property and associated costs	25 435.15	– 20 632.81	4 802.34	18.88 %
A-22	Current administrative expenditure	83 026.87	– 69 728.86	13 298.01	16.02 %
A-23	Information and communication technologies	623 715,29	– 436 668.79	187 046.50	29.99 %
Total Title A-2		**1 605 678.95**	**– 1 302 813.85**	**297 498.61**	**18.59 %**
Title B-3 OPERATING EXPENDITURE					
B-30	Group activities	943 054.94	– 847 047.53	96 007.41	10.18 %
B-32	Horizontal operational activities	569 390.45	– 359 711.54	209 678.91	36.83 %
B-36	Core operational activities	1 664 038.43	– 1 470 922.26	193 116.17	11.61 %
Total Title B-3		**3 176 483.82**	**– 2 677 681.33**	**498 802.49**	**15.70 %**
TOTAL ENISA		**11 180 591.98**	**– 9 896 178.26**	**1 279 047.23**	**11.45 %**

* 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 2017

Title	Description	Year of Origin	Revenue and Income recognised	Revenue and Income cashed in 2017	Outstanding Balance
9000	SUBSIDY FROM THE EU GENERAL BUDGET	2017	10 574 977.00	10 574 977.00	0.00
9200	Subsidy from the Ministry of Transports of Greece	2017	566 261.74	520 263.34	45 998.40
9300	REVENUE FROM ADMINISTRATIVE OPERATIONS	2017	33 986.75	33 986.75	0.00
TOTAL ENISA			**11 175 225.49**	**11 129 227.09**	**45 998.40**

Average payment time for 2017

Average payment time for 2017	Total number of payments	Within time limit	Percentage	Average payment time	Late payment	Percentage	Average payment time
17.81 days	2 359	2 040	86.48 %	11.80 days	319	13.52 %	53.74 days

ANNEX 3
OTHER ANNEXES

C.1 LIST OF ACRONYMS

AD: administrator
AST: assistant
CA: contract agent
CE2016: Cyber Europe 2016
CE2018: Cyber Europe 2018
CEF: Connecting Europe Facility
CEN: European Committee for Standardisation
Cenelec: European Committee for Electrotechnical Standardisation
CEP: Cyber Exercise Platform
CERT-EU: Computer Emergency Response Team for the EU institutions, bodies and agencies
CIIP: critical information infrastructure protection
cPPP: Cybersecurity Public–Private Partnership
CSCG: ETSI CEN-Cenelec Cyber Security Coordination Group
CSIRT: computer security incident response teams
COD: Core Operational Department
CSS: Cyber Security Strategy
DG: European Commission directorate-general
ECA: European Court of Auditors
EDO: Executive Director's Office
EFTA: European Free Trade Association
eIDAS regulation: 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
ENISA: European Union Agency for Network and Information Security
ETL: ENISA threat landscape
ETSI: European Telecommunications Standards Institute
EU: European Union
FAP: Finance, Accounting and Procurement
FIRST: Forum of Incident Response and Security Teams
FTE: full-time equivalent
HoD: head of department
HoU: head of unit
HR: human resources
IAS: Internal Audit Service
ICS: internal control standards
ICT: information and communication technologies
IoT: internet of things
ISAC: information sharing and analysis centre
ISO: information security officer
LEA: law enforcement agency
NCSS: national cybersecurity strategies
NIS: network and information security
NLO: national liaison officer
NRA: national regulatory authority
O: output
OES: operators of essential services
PPP: public–private partnership
Q: quarter
SNE: seconded national expert
SRAD: Stakeholder Relations and Administration Department
TA: temporary agent
TF-CSIRT: Task Force of Computer Security Incident Response Teams
TL: threat landscape
VIS: visa information system, a database containing information on visa applications by non-EU nationals requiring a visa to enter the Schengen area
WPK: work package

C.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
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 — 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, 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	
NIS directive	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 cPPP	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 cPPP	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
General data protection regulation (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
LEA DP 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
PNR 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

Reference	Policy/legislation reference — Complete title and link
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
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, the European Economic and Social Committee and the Committee of the Regions — 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

Reference	Policy/legislation reference — Complete title and link
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 European 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), http://register.consilium.europa.eu/doc/srv?l=EN&f=ST 5842 2010 REV 2
Digital agenda	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions — A digital agenda for Europe, COM(2010) 245 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010DC0245&from=EN
2009	
Commission communication on IoT	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions — Internet of things — An action plan for Europe, COM(2009) 278 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2009:0278:FIN
Council Resolution of December 2009 on NIS	Council Resolution of 18 December 2009 on a collaborative European approach to network and information security, OJ C 321, 29.12.2009, 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

NOTES

NOTES

NOTES

TP-AB-18-001-EN-N

ABOUT ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the European Union, its Member States, its citizens and the private sector. ENISA works with these groups 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. More information about ENISA and its work can be found at https://www.enisa.europa.eu

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

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

enisa.europa.eu

Publications Office

ISBN 978-92-9204-256-1