enisa

THE EU
CYBER
SECURITY
AGENCY

ANNUAL ACTIVITY REPORT

2016

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

PRINT
Catalogue number: TP-AB-17-001-EN-C
ISBN: 978-92-9204-221-9
ISSN: 1830-981X
DOI: 10.2824/331949

PDF
Catalogue number: TP-AB-17-001-EN-N
ISBN: 978-92-9204-220-2
ISSN: 2314-9434
DOI: 10.2824/558297

enisa

ANNUAL ACTIVITY REPORT 2016

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 2016 OF THE AUTHORISING OFFICER OF ENISA

According to Article 47 of the Financial Regulation applicable to ENISA,

1. The authorising officer shall report to the Management Board on the performance of his duties in the form of an annual activity report […]. The consolidated annual activity report shall indicate the results of the operations by reference to the objectives set, the risks associated with the operations, the use made of the resources provided and the efficiency and effectiveness of the internal control systems, including an overall assessment of the costs and benefits of controls.

The consolidated annual report shall be submitted to the Management Board for assessment.

2. No later than 1 July each year the consolidated annual activity report together with its assessment shall be sent by the Management Board to the Court of Auditors, to the Commission, to the European Parliament and to the Council.

The Management Board received a copy of the 2016 Annual Activity Report produced by the Executive Director of ENISA in his quality of Authorising Officer for the implementation of the annual budget on 19 June 2017.

After the Executive Board scrutiny, the assessment by the Management Board of the consolidated annual activity report (hereinafter AAR) is as follows:

- The AAR presents key results in the implementation of the ENISA Work programme 2016 and leads to conclusion that the Agency completed all deliverables agreed with the Management Board both within time and within budget. 64 activities have been reported as completed in 2016. Among those activities, the support to implement key EU policy areas should be highlighted, notably the NIS directive[1], the General Data Protection regulation (GDPR)[2], eIDAS regulation[3] and the Payment Services directive 2 (PSD2)[4].

- 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 2016.

- Overall, the AAR is in line with the ENISA Work Programme 2016 in this regard 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 2016 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 100%. This section also reports on results of job screening benchmarking exercise. The support function is 20,24% of the total statuary staff count, which is below the maximum value (25%) accepted for the decentralized small size agencies.

- The AAR also provides a follow up of the 2014 Discharge, and control results. The Agency has followed up on recommendations of Internal Audit Service as well as of the Court of Auditors. In 2016 no new recommendations were issued. This section also notes the main categories of deviation that led to exceptions reported in the Register of Exceptions and mentions that there is one exception registered with high materiality (above 60.000,00 euros). This case is related to a posteriori commitment. A human error on a handover provided by a previous staff member created a delay in concluding the budgetary commitment.

- 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 2016. 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 increase the output 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.

- 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.

[1] 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: ELI: http://data.europa.eu/eli/dir/2016/1148/oj

[2] 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) (Text with EEA relevance), OJ L 119, 4.5.2016, pp. 1-88, available at: http://data.europa.eu/eli/reg/2016/679/oj

[3] 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

[4] 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 (Text with EEA relevance), OJ L 337, 23.12.2015, pp. 35-127, available at: http://data.europa.eu/eli/dir/2015/2366/oj

TABLE OF CONTENTS

A MESSAGE FROM THE EXECUTIVE DIRECTOR

I would like to take the opportunity to summarise key achievements of 2016, another successful year with ENISA.

I am pleased to report that, consistently with previous years, we have successfully completed our 2016 annual Work Programme, delivering all 64 reports on time and within budget. These reports cover a wide spectrum of NIS areas ranging from traditional activities such as incident reporting and baseline security controls to emerging areas such as smart hospitals, cars and airports, embedded systems and cyber insurance. The Agency also produced a number of practical studies supporting the implementation of key EU policy areas, notably the NIS directive, the general data protection regulation (GDPR), eIDAS and the payment services directive 2 (PSD2). All ENISA reports are structured in such a way as to bring the key issues to the foreground and to make concrete proposals on what needs to happen in order to strengthen our European common approach to cybersecurity.

The Agency continues to deliver operational, financial, legal and compliance requirements at similar efficiency levels as previous years. During 2016 the Agency began to put in place a quality management system (QMS), a 3-year project, supported by a quality policy, as well as large set of standard operation procedures and work instructions (WINs) that aim at the standardisation of the internal procedures, optimisation of processes, risk mitigation, and increase in efficiencies. The QMS aims for a constant performance improvement of the best possible use of the available appropriations for delivering the best results for EU citizens. In May 2016, the Agency carried out a reorganisation. We consider our colleagues to be the best asset of ENISA, and bearing this in mind the Agency will continue to promote the value of the people that contribute to the success of our work.

ENISA has coordinated another successful pan-European exercise, building on the achievements of past years and once again raising the bar in terms of both objectives and internal collaboration requirements. The 2016 exercise was a simulation of an EU-wide crisis triggered by cyber-attacks designed to test EU- and national-level cooperation and to improve technical and operational capabilities. This was the first exercise to be spread over 6 months and to incorporate a 2-day intensive operations exercise. The exercise benefited from exclusive on-site media coverage and was broadcast in 16 EU languages.

ENISA hosted several other successful events including two separate meetings of the ENISA Industry Group, the Annual Privacy Forum (APF) and a briefing session at the premises of the European Parliament on cryptography to MEPs. In the scope of the Work Programme we also hosted a range of high-level technical workshops in important areas. We have worked in close collaboration with others to support the EU Cybersecurity challenge, helping the EU to motivate and develop new talent, and the European Cyber Security Month (ECSM), the EU advocacy campaign promoting awareness on cybersecurity. Many other successful projects can be seen in this report.

The Agency's media outreach has improved and we are better prepared to meet the challenges for the renewal of the mandate in the next few years as the critical relevance of the Agency is attested by the daily cybersecurity challenges that the EU faces. During 2016, a new enhanced website with improved functionality, new content and dedicated sections was launched that allows the Agency to be closer to a larger number of stakeholders. We have further strengthened our relations with many different stakeholders and assisted them in making significant improvements to the state of cybersecurity throughout the EU.

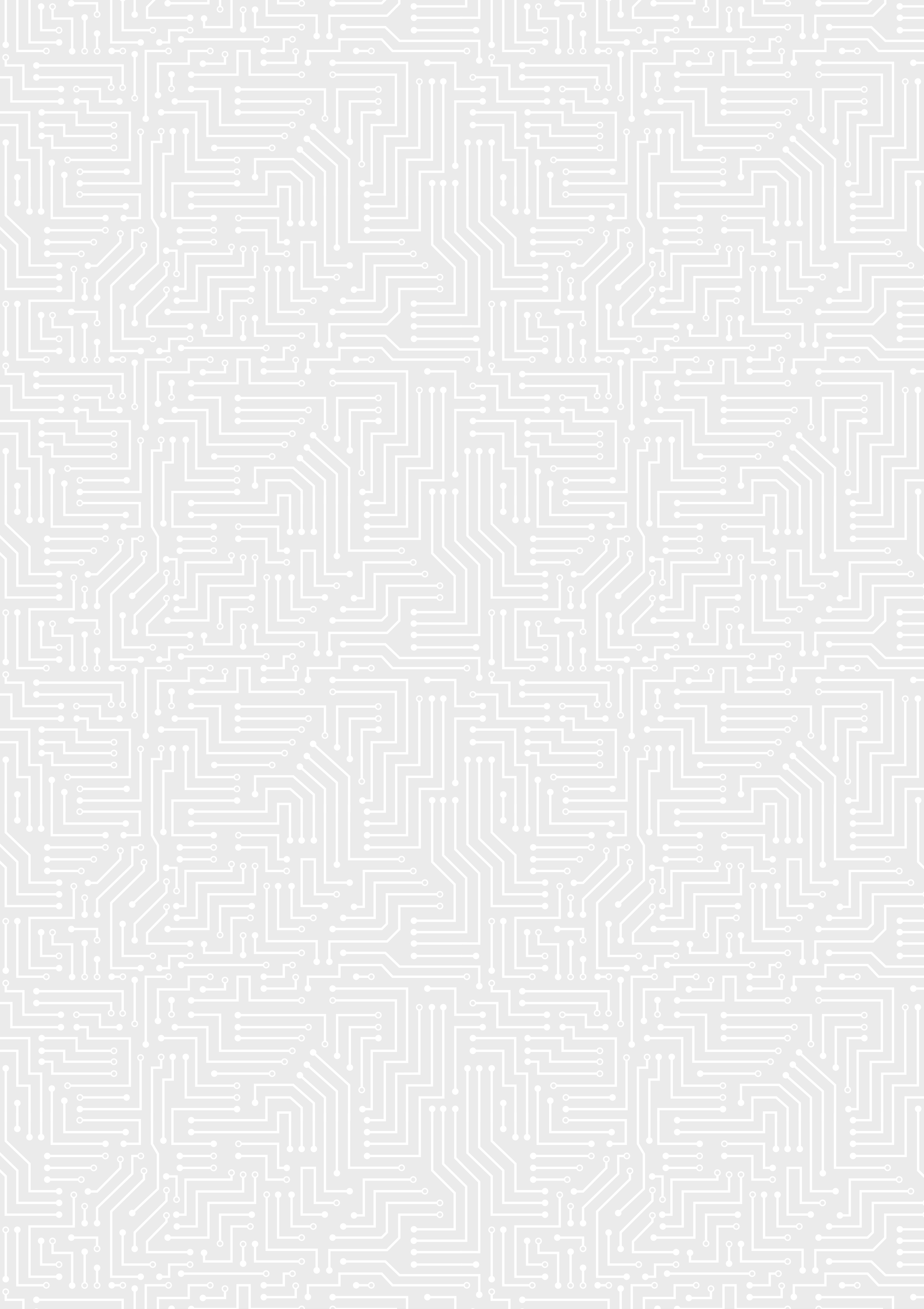
We continue to receive and respond to requests from the Member States and EU institutions. During 2016, we closed 23 such requests. Most of these requests were in the area of training, but we also received requests to assist the Commission regarding policy implementation and also regarding specific cyber vulnerabilities.

The above illustrates the capacity of ENISA staff to work together and deliver on time and in budget. I believe that our efforts are appreciated by all our stakeholders, which includes the EU Member States, the European Commission, the European Parliament, industry and ultimately the EU citizens.

Nowadays the need to optimise the available budget of the European Union as well as the need to do more with fewer resources is a reality across all the European Union organisations and bodies. ENISA is not an exception; the Agency continues to pursue efficiency and effectiveness.

I profit from this opportunity to thank all staff and stakeholders for their contributions and efforts during 2016, and look forward to delivering our new projects and studies in the following year and reinforce our support to keep EU cyberspace safe and prepared for the economic development aimed by all EU citizens.

Udo Helmbrecht
Executive Director, ENISA



INTRODUCTION

ENISA 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 extends ENISA's mandate until 19 June 2020.

ENISA is a centre of expertise for network and information security or cybersecurity in Europe. ENISA supports the EU and the Member States in enhancing and strengthening their capability 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 together with members of both the public and private sector, to deliver advice and guidelines that are based on solid operational experience. ENISA also supports the development of European Union (EU) policy and law on matters relating to network and information security (NIS), thereby contributing to economic growth in the EU's internal market.

ENISA's strategic objectives are derived from the ENISA regulation, inputs from the Member States and relevant communities, including the private sector:

- Develop and maintain a high level of expertise of EU actors, taking into account evolutions in NIS;
- Assist the Member States and the EU institutions and bodies in enhancing capacity building throughout the EU;
- Assist the Member States and the EU institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirement of NIS;
- Enhance cooperation both between the Member States of the EU and between related NIS communities.

KEY ACHIEVEMENTS. HIGHLIGHTS OF THE YEAR

The European Union Agency for Network and Information Security (ENISA) contributes to the policy goal of a high level of network and information security (NIS) within the European Union. The mission of ENISA is to secure Europe's information society, which translates into providing expertise, supporting policy and creating know-how to secure over 500 million citizens using every day ICT to work, live and communicate.

As a centre of excellence and expertise in the field of NIS, ENISA has used its expertise to:

- advise its stakeholders on trends in the digital world that affect security;
- suggest good practices in various areas in relation to information, services and systems security;
- support the development and implementation of policy requirements in the area of security and data protection;
- collaborate with stakeholders and contribute to the NIS capacity and communities' building.

The Work Programme (WP) of 2016 has resulted in 64 deliverables (which include also workshops and similar activities) that have been produced in full.

The highlights of 2016 include new best practices and recommendations for cybersecurity of smart cars, smart hospitals, smart airports and blockchain. The Agency kicked off the process of supporting the Member States in their task of delivering against the NIS directive, continued ongoing activities such as Article 13a reporting, computer security incidents response teams (CSIRT) training and held the biggest EU cybersecurity exercise ever, Cyber Europe 2016. The Agency supported the EU Cybersecurity Challenge event, which brought together teams of students and school pupils from the different Member States to compete against each other in a series of technical challenges and, as in previous years, we played a significant role in supporting the EU Cyber Security Month (ECSM).

In line with its Work Programme, ENISA released a number of reports on different aspects of NIS. These include an updated 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 as well as the emerging area of certification of products. Finally, ENISA compiled a data breach severity assessment tool in close collaboration with several Member State DPAs. The aim of this tool has been to make available a coherent framework to assess data breach severity across EU MS. Requests under Article 14 of ENISA Regulation (EU) No 526/2013 continued unabated as a method for stakeholders to request assistance, culminating in 15 new requests.

As in previous years, the Agency organised a number of high profile events throughout the year, such as the High Level Event, two editions of the ENISA industry event, the Annual Privacy Forum and the European Cyber Security Challenge. ENISA also hosted 14 important thematic workshops and sessions, gathering experts in the field to discuss cybersecurity topics.

Most relevant key performance indicators

In 2016, the Agency delivered against its annual Work Programme and all deliverables met or exceeded the key performance indicators set (see Section I for more details). Notable achievements are mentioned hereunder along with examples of how the Agency reached its goals. It should be noted that in March 2016 the ENISA WP2016 was amended to address the changes in ENISA activities generated by the adoption of the NIS directive. Key achievements include:

- In 2016, ENISA published groundbreaking reports regarding cybersecurity of smart cars, smart airports and hospitals, helping asset owners and all relevant actors in securing citizens and infrastructures from cyber-attacks and incidents. (Impact indicator in WPK1.1. NIS Threat Analysis.)

- With the adoption of the NIS directive, ENISA has cooperated with all EU Member States and the Commission to define the scope, the actions related to ENISA and the next steps. More specifically ENISA has assisted the Commission and MS in the establishment of the Cooperation Group envisaged in the NIS directive. The Agency, as a member of this group, has provided ideas to the Commission and MS about its governance structure, its objectives and themes to focus on as well as its working relationship with the CSIRT Network. (Impact indicator in WPK3.2.A. Assist EU MS and Commission in the implementation of the NIS directive)

- ENISA has continued to collect and analyse national reports on large-scale telecom security incidents in accordance with Article 13a of the framework directive on electronic communications. The Agency, has analysed the national reports, compared them with previous years, identified new trends and developed good practices and lessons learned. The Annual Incidents Report 2016, including the analysis on the incidents reported, was published around September 2016. ENISA together with the Article 13a WG provided feedback to the EC on security aspects regarding the new telecom code. The feedback was well received, as some of the observations are included in the new regulation proposal. (Impact indicator in WPK3.2.C. Assistance in the implementation of mandatory incident-reporting schemes)

- ENISA organised a workshop on National Cyber Security Strategies together with the Slovakian Presidency of the EC in November, bringing together stakeholders from more than 15 Member States. Moreover, the updated good practice guide was published in November 2016 following validation phase with all relevant stakeholders and the ENISA NCSS experts group. (Impact indicator in WPK2.1.B. Assistance in the area of cybersecurity strategies)

- More than 60 participants in the second Trust Services Forum, including stakeholders from Supervisory Bodies, Conformity Assessment Bodies and Trust Service providers.

- ENISA organised the fourth pan-European cyber exercise, Cyber Europe 2016 (CE2016). CE2016 was a large-scale distributed technical and operational exercise started in April 2016, offering the opportunity to cybersecurity professionals across Europe to analyse complex, innovative and realistic cybersecurity incidents. CE2016 overall in the 6-month period engaged over 1 000 participants.

- The 2016 edition of the European Cyber Security Month (ECSM) resulted in a successful advocacy campaign with 32 countries taking part, some 455 activities from public and private stakeholders and an outreach in social media topping the previous year's statistics including 429 articles published in October referring to ECSM. Included within these results are the 465 courses now registered in 28 countries for the NIS Education map.

- ENISA organised the first European Cyber Security Challenge where 100 of the best young security talents from 10 different nations fought for the title in the final of the European Cyber Security Challenge in Düsseldorf, Germany.

- More than 80 participants in the Annual Privacy Forum (APF) 16: (researchers, policymakers and industry participants) (Impact indicator in WPK3.2.B. Assistance in the implementation of NIS measures of EU data protection regulation.)

- ENISA produced a set of deliverables supporting the implementation of the eIDAS regulation seeking to shed more light in the service delivery of trust services.

- ENISA compiled a data breach severity assessment tool in close collaboration with several Member State DPAs. The aim of this tool has been to make available a coherent framework to assess data breach severity across EU MS.

- The Agency analysed important aspects of use privacy protection in a mobile environment.

- The emerging area of product certification received particular attention throughout 2016, as ENISA supported Commission initiatives and it coordinated private and public stakeholders in an effort to shape the field with a view to supporting future policy.

- Finally, reports on incident reporting in the energy sector and on cyber-hygiene guidance have been produced, reviewing the prevailing situation across the EU.

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

ENISA has consolidated internal control standards, 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, in accordance with the standards and suitable to mitigate risks associated with the environment in which it operates.

In 2010, the Management Board of the Agency adopted a set of 16 internal control standards 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 2016, the Agency focused on compliance with the standards that were identified as areas of concern during the risk assessment exercise, as well as on the recommendations raised by the auditing bodies (European Court of Auditors and the Internal Audit Service of the European Commission). It has been reported that with reference to 2014, the Agency achieved compliance with the internal control standards; for more details, please refer to Sections 3 to 6 and to the annexes of this report.

Information for the stakeholders

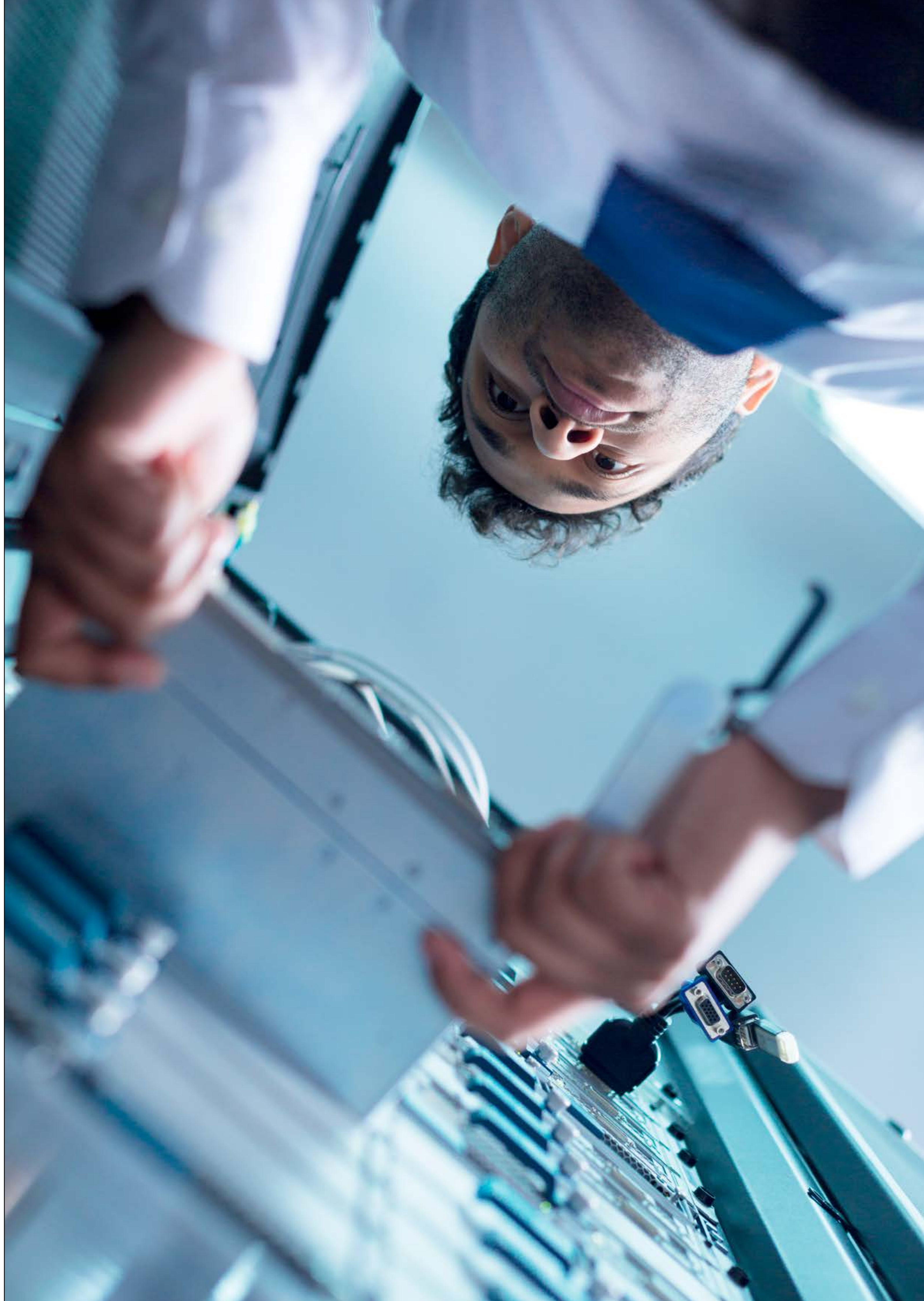
2016 will be remembered as the year of the biggest DDoS attack, the biggest data breach but also as the year of the NIS directive:

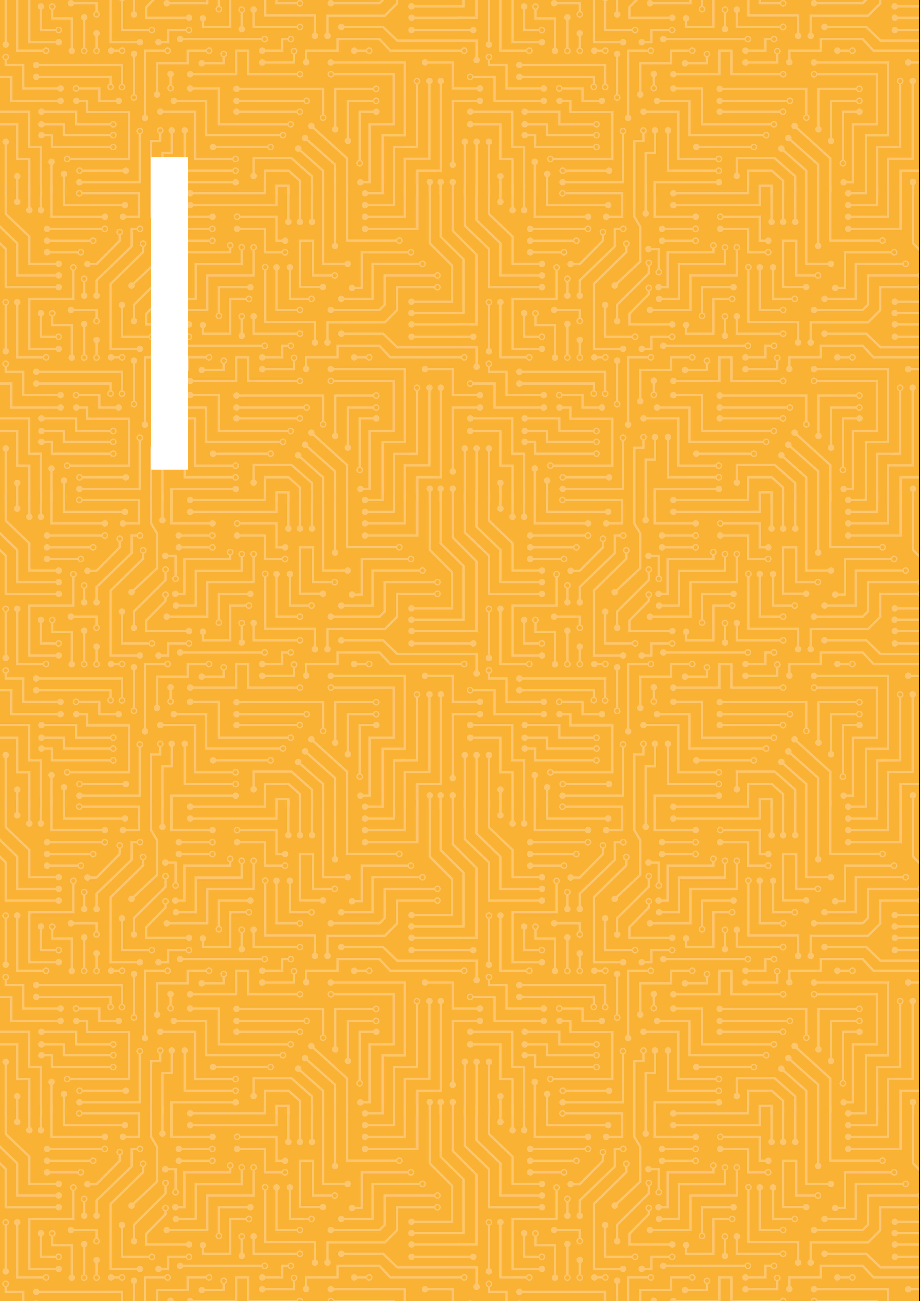
- In autumn 2016 a series of massive (distributed denial-of-service) DDoS attacks occurred. They were mainly propagated through compromised internet of things (IoT) devices. 'Mirai', a type of malware that originally targets IoT devices, was used to orchestrate massive DDoS. In November 2016, another incident related to a variant of the Mirai malware took place. An upgraded variant of the malware targeted customers' home routers of Germany's telecommunication company Deutsche Telekom. A large number of home routers were hit by the outage.

- During 2016 a series of major and massive data breaches emerged exposing hundreds of millions of user emails and passwords (in hashed or plaintext form). It is understood that the data were originally sold on the black market, but soon a lot of them became public. Interestingly, all these data breaches are dated a few years back, but they were only disclosed recently, remaining within private circles for years. Following these data breaches a wide range of attacks on well-known websites occurred because of users reusing their passwords.

- The directive on security of network and information systems (the NIS directive) was adopted by the European Parliament on 6 July 2016. The directive entered into force in August 2016. ENISA's Executive Director Prof. Dr Udo Helmbrecht said: 'The NIS directive is one of the components for the delivery of digital single market. Its success lies with the full engagement of all the stakeholders identified in the directive, including digital service providers. Cybersecurity challenges can be only addressed by working together.'

As underlined by the latest ENISA Threat Landscape, 2016 was characterised by 'the efficiency of cyber-crime monetisation'. Undoubtedly, optimisation of cybercrime turnover was the trend observed in 2016. And, as with many of the negative aspects in cyberspace, this trend is here to stay. On the other side, this is another confirmation of the necessity of an agency like ENISA. Positive developments can be reached only by strengthening the Agency and putting more resources on the fight against cyber-attacks. Only an agency with a clear and comprehensive mandate and adequate resources can contribute to better face all the cybersecurity challenges that are arising and augment its outreach to the benefit of different stakeholders and asset owners across Europe.





PART I

ACHIEVEMENTS IN THE IMPLEMENTATION OF WORK PROGRAMME 2016

This Annual Activity Report (AAR) for 2016 follows the structure of the ENISA Work Programme (WP) 2016 to assist reader understanding of what was achieved. The WP 2016 was aligned with the strategic objectives featured in the strategy and the multiannual planning of the Agency. The strategic objectives (SO) of the WP 2016 were as follows:

SO1: To develop and maintain a high level of expertise of EU actors taking into account evolutions in network and information security (NIS).

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

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.

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

In the following sections, the results of WP 2016 implementation are presented for each of the abovementioned objectives. After the description of the concrete results for each strategic objective, the achievements against indicators and the detailed results for each deliverable are presented in tables.

It should be noted that the ENISA WP2016 was amended in March 2016 to address the changes in ENISA activities generated by the adoption of the NIS directive. This activity report follows the structure of the amended WP2016.

1.1 KEY RESULTS IN THE IMPLEMENTATION OF SO1 — DEVELOP AND MAINTAIN A HIGH LEVEL OF NIS EXPERTISE OF EU ACTORS

SO1 aims to develop and maintain a high level of expertise of EU actors, taking into account evolutions in network and information security (NIS). In 2016, this SO covered the Threat Landscape and risk assessment, including new technologies and specific areas such as smart cars, smart airports and smart hospitals as well as information sharing and good practices and recommendations for critical information infrastructure protection (CIIP).

List of work packages and short description

WPK 1.1 — Improving the expertise related to critical information infrastructures
In this work package (WPK) ENISA developed good practices on emerging smart critical infrastructures and services. This work provided smart critical information infrastructure and service providers and developers with good security and resilience practices to be used when designing, developing and deploying such services in order to minimise the exposure of such networks and services to all relevant cyber threat categories.

WPK 1.2 — NIS Threats Landscape analysis
Ensuring adequate levels of protection for modern IT systems in any context requires recognising and adapting to changes in the evolving threat environment. Whilst it is clearly not possible to predict all future threats (security practices have often been dramatically changed as a result of so called 'black swan' events, which are notoriously difficult to predict), it is possible to predict the evolution of certain threats with a reasonable degree of accuracy based on past data.

ENISA supported its stakeholders by compiling existing data on threat evolution and tailoring this data to the needs of specific stakeholder communities. The approach covered threats across all sectors, whilst identifying specificities particular to particular communities in line with the goals of the WP. This is a more scalable approach than carrying out threat analysis directly.

WPK 1.3 — Research and development, innovation
Although there is state-of-the-art research in Europe in the field of NIS, and this area is extensively supported by European-funded programmes, research is usually not focused on the aspects where NIS policies need available technologies to move forward on their implementation. ENISA aims in this WPK to contribute to the various consultations launched by the Commission in the area of NIS. Such consultations may be conducted in the context of setting the research priorities for future calls for proposals or in the context policy initiatives launched or about to be launched by the Commission. Furthermore, during 2016 ENISA prepared a set of recommendations on aligning research programmes with policy in the area of NIS.

1.1.1 WPK 1.1: Improving the expertise related to critical information infrastructures

In this WPK ENISA developed good practices on emerging smart critical infrastructures and services using the concept of the internet of things (IoT) to deliver new, innovative business models and services.

The reports provide smart critical information infrastructure and service providers and developers with good security and resilience practices when designing, developing and deploying such services in order to minimise the exposure of such network and services to all relevant cyber threat categories. This builds on previous work of ENISA in the area of smart cities (WP 2015), smart grids (WP 2012-2015) and intelligent transportation systems (WP 2015).

The main areas of work of this WPK are as follows.

- ENISA defines smart cars as systems providing connected, added-value features in order to enhance car users experience or improve car safety. It encompasses use cases such as telematics, connected infotainment or intra-vehicular communication. The 2016 report on cybersecurity of smart cars listed the sensitive assets present in smart cars, as well as the corresponding threats, risks, attack scenarios, mitigation factors and possible security measures to implement. Smart cars subject matter experts were contacted to reflect the needs of Europe's automotive cybersecurity stakeholders. The results are further aligned with the C-ITS Platform run by DG Mobility and Transport, to synergise efforts and the input from the ENISA Cars and Roads SECurity (CaRSEC) Expert Group to finalise the results. The goal is to secure smart cars today for safer autonomous cars tomorrow.

> **In this WPK ENISA developed good practices on emerging smart critical infrastructures and services using the concept of the internet of things (IoT) to deliver new, innovative business models and services.**

- The notion of smart hospitals is introduced when internet of things (IoT) components are supporting core functions of a hospital. Due to the great number of significant assets at stake (patient life, sensitive personal information and financial resources) information security is a key issue for smart hospitals. ENISA identified the assets comprising the smart infrastructure inside the hospital walls, threats faced by smart hospitals as well as security measures set to address them. Based on attack scenarios, the Agency identified good practices and finally recommendations for both healthcare operators as well as IoT devices manufacturers and vendors.
- Smart airports are those airports making use of integrated internet of things (IoT) components to bring added-value services. By integrating smart components, airports are exposed to a larger attack surface and new attack vectors. In response to the new emerging threats faced by smart airports, this 2016 'Securing Smart Airports' report provides a guide for airport decision-makers (CISOs, CIOs, IT Directors and Head of Operations) and airport information security professionals, but also relevant national authorities and agencies that are in charge of cybersecurity for airports. Based on an in-depth examination of existing knowledge as well as validation interviews with subject matter experts, this report highlights the key assets of smart airports. Built on this, a detailed analysis and threats mapping was conducted with a particular focus on the vulnerabilities of smart components.

For each area, ENISA identified all relevant public and private stakeholders, engaged them in working groups and jointly took stock of and analysed the current situation in terms of cybersecurity and resilience, placing emphasis on communication security. The Agency also identified EU and national-funded projects in the area of IoT and M2M communication, liaised with them, analysed their findings and deliverables, and further engaged them in corresponding expert groups. Special emphasis was given to the resilience and robustness of such smart critical information infrastructure and services.

Based on the consultation with stakeholders and desktop analysis and research, ENISA developed good practices and propose baseline security requirements targeted at EU and national policymakers, operators and manufacturers.

1.1.2 WPK 1.2: Network and information security threats landscape analysis

The main goal of this work package was to develop the current cyber threat landscape by the collection and collation of publicity available information. The resulting report includes current threats, as well as threat trends in NIS, information about different attack vectors, classification schemes for cyber threats (i.e. taxonomies) and emerging technologies. This information will allow the interested readers to achieve a more complete coverage of the threat analysis life cycle.

In addition, as in previous years, in-depth studies on two emerging technologies for risk assessment and threat analysis were performed: 'Hardware Threat Landscape and Good Practice Guide' and 'Ad hoc and sensor networking for M2M Communications Threat Landscape and Good Practice Guide'. These reports identified related network assets and the security threats, challenges and risks arising from these assets for each technology and identified security mechanisms and good practices for each applicable environment. Finally, based in the collated information, technical, policy and organisational recommendations for proactively enhancing the security for each emerging technology were provided.

1.1.3 WPK 1.3: Research and development, innovation

In 2016, ENISA's Crypto Challenge (which we named Crypt a Bite) was launched. The pilot study aimed to capture the interest of young students for information security and cryptography. We especially aimed at students with an interest in maths and logic. In order to catch the attention of the 'non-geek', we decided on a gamification of the contest. The pilot was successful in the sense that a large fraction of registered users did participate in the actual competition. Further, it is possible to attract students with a viral campaign; however, we also learned that a longer, more coordinated advertisement phase is needed to reach more students. For the pilot more than 700 users registered and performed the training challenges of phase I of which 94 participated at the final round. The full report is published under the name Crypt a Bite — ENISA's Crypto Challenge.

Another aspect of this WPK for 2016 was the preparation of a set of recommendations on aligning research programmes with policy in the specialised area of NIS. The specialised field of Network and Information Security (NIS) is supported extensively by EU-funded research programmes, but is not always focused on the aspects where emerging policy and legislative initiatives need available technologies to move forward on their implementation. The scope of this report was to summarise achievements that have significantly promoted specific pillars of NIS, identify specific outcomes that promoted and support emerging policy and legislative initiatives, namely eIDAS, GDPR, and provide recommendations on the cPPP and the formulation of forthcoming work programmes. During the preparation of this report, selected stakeholders from academia, research, public authorities and research and technology organisations were contacted to provide their subject matter experience and expertise.

Finally, in order to support the R & D in this area, ENISA prepared a study on the security aspects of virtualisation. The recent and widespread adoption of virtualisation technologies has changed the traditional view of ICT, as virtualisation can provide a dramatic increase in the efficiency and effectiveness of complex organisations and communities. However, virtualised environments are increasingly becoming targets of cyber-attacks: More and more elaborate and specialised attacks are currently devised to exploit vulnerabilities and weaknesses at the virtualisation layer. The report prepared by ENISA provides an analysis of the current status of security of virtualisation, by presenting current technologies affected, risks, efforts, gaps, and the impact the latter have on environments based on virtualisation technologies. The final objective of the 'Study on security aspects of virtualisation' report is to provide the basis to understand the main issues and challenges related to the security in virtualisation, and provide a look at common best practices to implement a secure virtualised environment.

1.1.4 General results. Achievement of impact indicators for Objective 1

SO1 — To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security	
WPKs, impact indicators	**Achieved results**
WPK 1.1.: Improving the expertise related to critical information infrastructures	
By 2017, national authorities in at least five MS 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 (CaRSEC) Expert Group. We have received valuable input and feedback from French Ministry of Interior — Gendarmerie Nationale, German Federal Office for Information Security, Joint Research Center, ANSSI — French Network and Information Security Agency and Kuratorium Sicheres Österreich.
By 2017, national authorities in at least five MS use ENISA's recommendations on smart health devices, services and infrastructures.	ENISA has 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; Association of Hospitals in Vienna, Austria; NHS Digital UK; National Oncology Hospital of Sofia, Bulgaria; Jena University Hospital, Sweden; Munich Municipal Hospital, Germany.
By 2017, national authorities in at least five MS use ENISA's recommendations on smart airports.	The study involved several major airports across Europe and related entities such as European Commission, European Aviation Safety Agency, Eurocontrol, SESAR Joint Undertaking and ACI Europe.
WPK 1.2: Network and information security Threats Landscape analysis	
In 2016 at least 15 companies and five Member States participate in the ENISA stakeholder groups established to perform the work.	More than 15 companies and more than 5 Member States contributed in the threat analysis/landscape process as well as the validation of the work.
By 2017 produced results are referenced by at least 500 stakeholders in the area of threat/risk assessment.	ENISA Threat Landscape results have been reused within multiple stakeholders, both within and outside EU. In various discussions, blogs and presentations, references to ENISA Threat Landscape 2016 have also been found widely referenced in different social networks. During the first week of dissemination, the ENISA Threat Landscape 2016 was disseminated via social media with the following rates: ca. 200 views and 70 likes in LinkedIn, ca. 2 000 impressions in Twitter ca. 15 re-tweets and ca. 50 engagements. This response from the community is considered successful. Additional analytics will be obtained after a sufficient time window.
By 2017 produced results are downloaded by at least 10 000 individuals.	Various ENISA Threat Landscape reports (ENISA Threat Landscape and Thematic Landscapes) were downloaded for more than 20 000 individuals in 2016. These numbers are referring to 2015 deliverables disseminated in 2016. For the time being and after ca. one week of dissemination, the uptake of ENISA 2017 deliverables counts ca. 2 500 downloads.
WPK 1.3: NIS Threats Analysis	
At least 10 experts from the community to participate in the validation of the results of the studies.	More than 10 experts from academia, universities and research and technology organisations participated in the validation and review of the results of the studies.
At least five independent high-level experts from the cryptography field to participate in the quality review and the panel for the cryptographic challenges.	Our contractor created a panel with experts knowledgeable in cryptography and experienced in the creation of similar challenges.
At least 50 individuals/teams participate in the cryptographic challenges.	About 700 in round I and 94 in round II participated in the cryptographic challenge
At least six research experts and networking experts from industry to contribute to the study on security aspects of virtualisation.	More than six research and networking experts contributed and reviewed to the study.

1.1.5 Specific results. Mapping of deliverables into papers/publications/activities

SO1 — To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security	
WPKs, deliverables	**Specific achievements: papers/publications/activities**
WPK 1.1: Improving the expertise related to critical information infrastructures	
D1: Good practices on the security and resilience of smart cars and intelligent road systems (report and a workshop, Q4, 2016).	The study was published in January 2017 and included contributions from the several experts across MS, members of the ENISA Cars SECurity (CaRSEC) Expert Group and all participants of the ENISA validation workshop in Munich in October 2016. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars
D2: Good practices on the security and resilience of smart health services and infrastructures (report and a workshop, Q4, 2016).	The study was published in November 2016 following the validation workshop which took place in Vienna (in collaboration with the Vienna Hospitals Association) in which experts from healthcare organisations participated. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals
D3: Good practices on the security and resilience of smart airports (report and a workshop, Q4, 2016).	The study was published in December 2017 and included contributions from several experts across MS. The workshop is to be scheduled according to the requests of the constituency. https://www.enisa.europa.eu/publications/securing-smart-airports
WPK 1.2: Network and information security threats landscape analysis	
D1: Annual threat analysis/landscape report (Q4, 2016).	ENISA Threat Landscape 2016: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016
D2: Assessments on two key technology/application areas (governments, small to medium-sized enterprises (SMEs), etc.) (Q4, 2016).	Ad hoc and sensor networking for M2M Communications Threat Landscape and Good Practice Guide: https://www.enisa.europa.eu/publications/m2m-communications-threat-landscape Hardware Threat Landscape and Good Practice Guide: https://www.enisa.europa.eu/publications/hardware-threat-landscape
By 2017 produced results are downloaded by at least 10 000 individuals.	The study was published in December 2017 and included contributions from several experts across MS. The workshop is to be scheduled according to the requests of the constituency. https://www.enisa.europa.eu/publications/securing-smart-airports
WPK 1.3: Research and development, innovation	
D1: ENISA cryptographic challenges (Q3, 2016).	https://www.enisa.europa.eu/publications/enisa-cryptographic-challenges
D2: Recommendations on aligning research programme with policy in the specialised area of NIS (Q4, 2016).	Recommendations on aligning research programme with policy: https://www.enisa.europa.eu/publications/recommendations-on-aligning-research-programme-with-policy
D3: Study on security aspects of virtualisation (Q4, 2016).	Study on Security aspects of virtualisation. https://www.enisa.europa.eu/publications/security-aspects-of-virtualization

1.2 KEY RESULTS IN THE IMPLEMENTATION OF SO2 — ASSISTANCE IN ENHANCING CAPACITY BUILDING THROUGHOUT THE EU

SO2 aims at providing assistance to MS and EU institutions and bodies, as well as the private sector by supporting NIS enhancement of capacity building through the EU. ENISA worked together with Member States and EU institutions to assist them in capacity building across the EU. In particular, the Agency worked together with all relevant stakeholders to ensure that the approach adopted has been coherent across all EU stakeholders involved.

List of work packages and short description

WPK 2.1 — Assist Member States' capacity building
One of the main goals of this work package (WPK) has been to develop and improve activities related to the operational security support programme. In 2016, ENISA built upon its work in the operational security area, and updated the impact assessment related to this area to concisely draw 'lessons learned' via a dialogue with relevant stakeholders.

Another main goal of this WPK has been to support 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 to secure their networks and data.

WPK 2.2 — Support EU institutions' capacity building
In this WPK ENISA aims at stepping up in its dialogue with EU institutions and support them in reinforcing their NIS capacity building. The Agency provided its key stakeholders with timely and high-quality responses to NIS developments.

WPK 2.3 — Assist private sector capacity building
One of the main obstacles for the implementation of wide and effective cybersecurity programmes in organisations has been the lack of a common language among managers and technical staff, which makes it difficult for the latter to transmit the current security scenario to the former. ENISA reviewed cyber hygiene practices across the Member States for the purpose of helping increase cybersecurity awareness and promote a culture of cybersecurity within organisations and Member States.

The agency collected information on prominent experiences across various MS by focusing on the theme of cyber-hygiene and associated guides that are currently in use in various MS.

WPK 2.3 — Assist in improving the general awareness
ENISA delivered against its long-standing goal of the European Cyber Security Month (ECSM) campaign that dates back to 2010 and it expanded its outreach with numerous activities in the Member States, reaching directly or indirectly a large number of European citizens. By coordinating the ECSM, ENISA seeks to contribute to the efficient management of MS capability in awareness raising on network and information security and on the exchange of good practices among its key stakeholders as it has consistently done over time.

> **ENISA worked together with Member States and EU institutions to assist them in capacity building across the EU.**

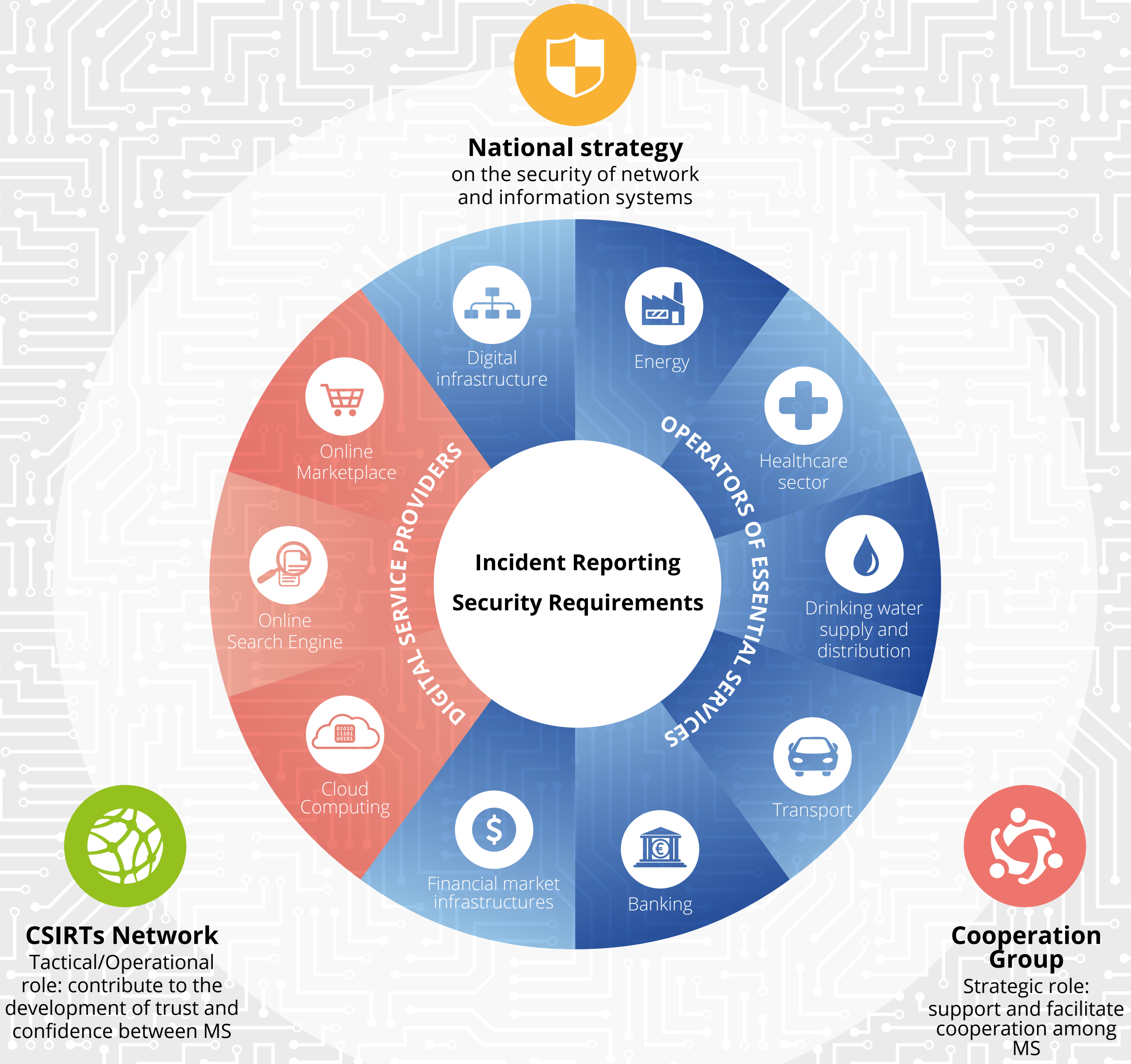
Additionally, ENISA promoted capacity building in the security community by launching a competition named the 'ENISA cyber challenge'. Its goal was to increase the interest in NIS by promoting excellence in the form of competitions, as well as to gather feedback on the areas of interest for the communities.

1.2.1 WPK 2.1: Assist Member States' capacity building

1.2.1.1 WPK 2.1.A: Assistance in the area of operational security and NIS operational training

Objectives:

- Facilitate voluntary information sharing techniques to enhance quality of collection;
- Extend mutual interactions with stakeholders in MS-wide area for incident response collaboration;
- Build upon successful work in the area of 'training methodologies and impact assessment';
- Update training material for operational communities (e.g. CSIRTs);
- Develop new sets of training for NIS;
- Further develop and apply ENISA recommendations for baseline capabilities;
- Provide technical training for MS and EU bodies.



One of the main goals of this WPK was to perform sustainable research, development and improvement of activities related to the multiannual development for the operational security support programme.

In 2016, ENISA updated the training methodologies and 'baseline capabilities' report. The goal was to concisely identify 'lessons learned' via a dialogue with relevant stakeholders, and to reflect constantly on developing CSIRT activities for the coming years.

Another main goal of this WPK is 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 to secure their networks.

Most of the activities in this WPK target maintaining and extending the collection of good practice guidelines in various areas of operational-capability building. In addition, ENISA continues to offer support to the Member States by providing them with means to enhance their national and governmental CSIRT capabilities.

Emphasis in this WPK was put on supporting operational bodies and communities (namely CSIRTs, but other communities where appropriate) via concrete advice (such as good practice material) and concrete actions (such as CSIRT training).

In 2016, ENISA updated and expanded its comprehensive set of training and exercises, consisting of material that can be used by both students and trainers.

In 2016, ENISA updated and expanded its comprehensive set of training and exercises, consisting of material that can be used by both students and trainers. The new training material provides a step-by-step guide on how to address/respond to incidents/issues as an incident handler and investigator. The material is technical and aims to provide a guided training both to incident handlers and investigators, while providing lifelike conditions. New topics in the training material cover aspects of forensic analysis and incident response. The updated training material provides new table top exercises in the areas of incident handling management, including the setting up of CSIRTs.

1.2.1.2 WPK 2.1.B: Assistance in the area of cybersecurity strategies

ENISA published its first National Cyber Security Strategy Good Practice Guide in 2012. Since then, EU Member States and EFTA countries have made great progress in developing and implementing their strategies. The new updated guide includes up-to-date information on the different steps, objectives and good practices for the implementation of NCSS and analyses the status of NCSS in the European Union and EFTA area. The aim is to support EU Member States in their efforts to develop and update their NCSS. Therefore, the target audience of this guide are public officials and policymakers. The guide also provides useful insights for the stakeholders involved in the lifecycle of the strategy, such as private, civil and industry stakeholders.

This guide places a special emphasis on the evaluation and maintaining phase. Suggestions for possible and indicative key performance indicators (KPIs) for objectives of the strategy are described. In addition, the guide presents the status of implementation of NCSS among EU Member States and identifies gaps.

ENISA acts as a facilitator in this process by bringing together MS and the private sector with varying degrees of experience to discuss and exchange good practices, share lessons learned and identify challenges and possible solutions.

1.2.1.3 WPK 2.1.C: Assistance in the area of privacy and trust

ENISA supported Member States in their own decision-making process, by providing advice and referencing to the appropriate ENISA studies in the area of privacy and trust. While this was a task-on-demand, the Agency provided appropriate tools that facilitate Member State implementation of the provisions set out in the trust services regulation and in the general data protection regulation. Supervisory bodies of the MS were involved in this line of work.

Specifically, in the area of personal data breaches, ENISA compiled a data breach severity assessment tool in close collaboration with several Member State DPAs. The aim of this tool has been to make available a coherent framework to assess data breach severity across EU MS.

In addition to this work, defined by the ENISA Work Programme, ENISA supported the Commission in the preparation of the draft ePrivacy regulation.

1.2.2 WPK 2.2: Support European Union institutions' capacity building

1.2.2.1 WPK 2.2.A: Information notes on NIS: production and review mechanisms ('info notes')

The main goal of this work package was to provide information on NIS issues and developments that reached a certain level of public attention to ENISA's key stakeholders, in a timely manner. Through info notes, the Agency was able to timely respond to NIS occurrences beyond its annual work packages, closely following the rapid updates and significant developments in the field of cyber security. Each of the different types of notes focused on highlighting facts and shortcomings behind NIS issues, often providing recommendations for addressing those shortcomings in the long term. One of the essential aims of info notes was to provide an independent, unbiased and 'calm' opinion to the Agency's stakeholders. In addition to previous years' dissemination of info notes to ENISA's key stakeholders, info notes were also published online at ENISA's website, rendering them publicly available to any interested party.

2.2.2.2 WPK 2.2.B: Reinforcement of the NIS of Union institutions, bodies and agencies

In this WPK ENISA aimed to enhance the dialogue among European institutions and support them in reinforcing their NIS. In 2016, concrete actions occurred.

ENISA has identified and liaised with all relevant stakeholders within European institutions and bodies. In cooperation with all relevant European institutions and bodies, the Agency took stock of and initiated an analysis of existing regulations, policies, procedures and practices of many EU institutions related to their NIS.

Through stocktaking and analysis, ENISA identified overlaps and gaps between all these regulations and policies. These findings were discussed with all relevant stakeholders from EU MS in the context of the NIS Directive Cooperation Group. This might pave the way for a permanent strategic dialogue among all European institutions and bodies on the future of NIS policy in the EU.

This dialogue resulted in important recommendations that will allow the simplification of policies, reduction of overlaps, identification of synergies, creation of awareness about NIS challenges and even proposals for new actions to address identified gaps. This will help European institutions and bodies to better focus their efforts and properly use their resources to meet the needs of EU MS and the private sector.

Considering the sensitiveness of the information that ENISA might be provided with by European institutions, deliverables were restricted in distribution.

Building on this work, ENISA will address, in future work programmes, the setting up of a European institution NIS contingency plan, the organisation of dedicated EU institution cyber incidents exercises, and the launch of awareness-raising initiatives.

1.2.3 WPK 2.3: Assist private sector capacity building

ENISA has reviewed best practices in Member States on how to reach out to the private sector to create increased cybersecurity awareness and skills. Additional ways to promote a culture of cybersecurity have been analysed. In 2016, the agency focused on studying and analysing cyber hygiene guides across selected Member States that have such instruments and policies in place and it came up with a set of recommendations for issuers of such guides and their users.

1.2.4 WPK 2.4: Assist in improving general awareness

The growing need for IT security professionals is widely acknowledged worldwide. To help solve this shortage of skill, many countries launched national cyber security competitions addressed towards students, university graduates or even non-ICT professionals with a clear aim: find new and young cyber talent and encourage young people to pursue a career in cyber security.

The European Cyber Security Challenge (ECSC) leverages these competitions by adding a pan-European layer. Top cyber talents from each participating country meet to network and collaborate and finally compete against each. Contestants are challenged in solving security-related tasks from domains such as web security, mobile security, crypto puzzles, reverse engineering and forensics and in the process collect points for solving them.

In a nutshell, ECSC is the annual European event that brings together young talent from across Europe to have fun and compete in cyber security.

The final stage of ECSC was held in Düsseldorf, Germany between 7 and 9 November 2016. Ten countries attended the event: Austria, Estonia, Germany, Greece, Ireland, Liechtenstein, Romania, Spain, Switzerland and the United Kingdom. The participants were expected to discover vulnerabilities in web applications, binaries and document files, solve crypto puzzles and hack hardware systems. However, technical skills were just one part of the challenge. As time and resources were limited, teamwork skills were also extremely important. The competition ended with a presentation by each team.

Between the contestants, coaches and judges, more than 130 people actively took part in the event. The competition was also accompanied by a conference with industry representatives and a job fair.

From its side, the 2016 edition of the European Cyber Security Month (ECSM) resulted in a successful advocacy campaign with 32 countries taking part, some 455 activities from public and private stakeholders and an outreach in social media topping the previous year's statistics including 429 articles published in October referring to ECSM. Included within these results are the 465 courses now registered in 28 countries for the NIS Education map.

European Cyber Security Challenge 2016

1.2.5 General results. Achievement of impact indicators for Objective 2

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

WPKs, impact indicators	Achieved results
WPK 2.1: Assist Member States' capacity building	
WPK 2.1.A: Assistance in the area of operational security and NIS operational training	
Support Member States in enhancing their national and governmental CSIRT baseline capabilities.	Over the year, ENISA supported the update of the CSIRT baseline capabilities covering Challenges for National CSIRTs in Europe in 2016.
Continued CSIRT services training will be provided to a minimum of 20 participants of different organisations in five Member States.	Services and training were provided to 11 Member States for around 150 participants from: Hellenic National Cert training, Hellenic Ministry of Interior, CERT.BE, Czech national CSIRT team, Estonia, Lithuania, Hungary – GovCERT, CSIRT Malta, CSIRT Slovakia, Germany, EC IAS staff
Improved operational practices of CSIRTs in at least 15 Member States (ongoing support with best practices development).	A workshop was organised in The Hague 11 on May 2016 that gathered 50 participants from over 30 teams coming from all EU and EFTA countries. Additionally, over the year, ENISA participated and organised two informal workshops for the EU NIS directive's CSIRTs Network.
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 in their national strategies the recommendations by ENISA:
By 2017, 15 private organisations use ENISA's good practices on NCSS.	Experts from 15 private organisations have provided information and are including in their national strategies the recommendations by ENISA.
By 2017, 10 Member States use ENISA's good practices on national public–private partnerships (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 in their national strategies the recommendations by ENISA.
By 2017, 15 private organisations use ENISA's good practices on national PPPs.	Experts from 15 private organisations have provided information and are including in their national strategies the recommendations by ENISA.
WPK 2.1.C: Assistance in the area of privacy and trust	
At least five data protection authorities (DPA) and 10 large EU data controllers to use the personal data breaches severity assessment tool.	The Agency has received more than 50 requests to access the personal data breaches severity assessment tool.
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 2017, information and feedback from different EU institutions were used for the creation, and as reference, on different info notes. In the same way on-demand topics info notes were created.
In 2017 improved mechanism for producing and distributing of 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 amongst the two work packages.
At least two EU bodies and five public stakeholders will receive the timely information on NIS incidents and significant developments in the field.	In 2016, info notes are published on the ENISA website and are publicly available for all interested stakeholders and announced on relevant channels.
WPK 2.2.A: Information notes on NIS: production and review mechanisms ('info notes')	
ENISA's expertise regarding the MS NIS capacity development is also to be offered to EU institutions, agencies and bodies (hereinafter: 'EU institutions'), in cooperation with CERT-EU.	ENISA, drawing from its expertise in the area of National Cyber Security Strategies (NCSS), NISD, and CIIP, took stock of sectorial initiatives developed by EU institutions, mostly the Commission. The Commission (DG CNECT) actively participated in the study and provided additional comments and suggestions, and as a result helped in validating the content of it. The end result is also presented in the first official meeting of the NISD Cooperation group.
Enhanced knowledge of EU institutions regulations, policies, procedures related to their NIS.	The stocktaking also allowed EU institutions to better understand the complex ecosystem, identify possible overlaps and gaps. Through this, they developed better knowledge and expertise on EU institutions regulations, policies and procedures.
Identification of well-functioning practices that could be disseminated to all or relevant EU institutions, as well as information concerning critical weaknesses that should be addressed.	The report identified several good practices widely used in several sectorial EU initiatives. Examples include PPPs, regulatory provisions (e.g. baseline requirements, incident reporting), information sharing, national NCSS. Such examples also provided better insights and knowledge benefiting EU institutions but also ENISA.
Identification of future actions that ENISA could initiate in order to further reinforce the NIS of EU institutions.	The key conclusion was the necessity to analyse all these initiatives and identify possible synergies and gaps. In addition, it is important to agree how the EU institutions develop their NIS policies in terms of sectors. Such discussion has started within the Cooperation Group of the NISD.
WPK 2.3: Assist private sector capacity building	
At least five MS and five private sector stakeholders contribute to the production of the guidelines for MS to reach the private sector through cybersecurity awareness dissemination activities.	The stock taking activity of cyber hygiene practices across the EU resulted in identifying three MS who actively reach the private sector via guidelines that they produce.
At least 15 private sector stakeholders coming from different MS, sectors of activity and size participate in the elaboration of the recommendations for ICT security staff on improving management level cybersecurity awareness.	A review of cyber hygiene practices was carried out across the EU and specifically to establish the understanding of the private sector's engagement with national cyber hygiene programmes. 15 private sector stakeholders were interviewed for the purpose of the review.
WPK 2.4: Assist in improving general awareness	
At least 50 individuals from MS participate in the ENISA cyber challenge.	More than 130 people, from 10 EU MS, actively took part in ECSC2016
Representatives from the EU-28 MS and five partner countries participate in ECSM and the release of general NIS messages for citizens.	Over 100 participants from EU representatives and partner countries participated in the ECSM kick-off event in Brussels and general NIS messages for citizens were released in a coordinated press release. Activities from all 28 MS were registered on the ECSM portal including 5 partner countries, releasing general NIS messages for citizens.
At least five international stakeholders collaborate, for better coordination, in the ECSM.	Stakeholders from across Europe participated in the ECSM coordinators conference calls and the meeting in Brussels for better coordination of the campaign. International stakeholders included European Banking Federation, Europol EC3, Confederation of European Computer User Associations, ECDL Foundation and ITU Council.
At least 10 experts from the community participate in reviewing the contents of the citizens' portal.	The content of the ECSM portal was reviewed by ENISA experts and external experts for its NIS messages and usability. Content from the citizens' portal was reviewed by over 15 experts from 15 different MS.

1.2.6 Specific results. Mapping of deliverables into papers/publications/activities

SO2 — To assist the Member States and the Commission in enhancing capacity building throughout the EU	
WPKs, impact indicators	**Achieved results**
WPK 2.1: Assist Member States' capacity building	
WPK 2.1.A: Assistance in the area of operational security and NIS operational training	
D2[1]: Follow-up/extension of the training methodologies work from 2014/15 (Q4, 2016).	The provisions of trainings to Member States (e.g. CSIRTs) via Article 14 proved to be very successful. We received, in 2016, 10 requests. The methodology we followed proved to be quite appropriate and stable.
D3: Update of existing training material (Q4, 2016).	The updated training material was published in January 2017. The material covers the area of 'Setting up a CSIRT', and the intended target audience is primarily the national/governmental and other CSIRTs that want to carry out one or more of the training sessions to maintain and/or enhance their effectiveness.
D4: Development of a set of new training material (Q4, 2016).	The new training material was published in January 2017. The material covers the several topics in the area of 'Forensic analysis', and the intended target audience is primarily the national/governmental and other CSIRTs that want to carry out one or more of the training sessions to maintain and/or enhance their effectiveness.
D5: On-request training for MS and EU bodies (Q4, 2016).	During 2016 the following 11 training sessions were provided by ENISA to: Hellenic National Cert training, Hellenic Ministry of Interior, CERT.BE, Czech national CSIRT team, Estonia, Lithuania, Hungary – GovCERT, CSIRT Malta, CSIRT Slovakia, Germany, EC IAS staff.
D6: Good practice in incident tracking and taxonomy (Q4, 2016).	The study was published in February 2017. The content of the study is a collective effort of the project team along with the CSIRT community. It provides a good basis for discussions regarding the topic of information sharing using different taxonomies, in the context of the upcoming CSP platform.
D7: Annual update of baseline capabilities (report) (Q4, 2016).	ENISA updated its baseline capabilities for CSIRTs on the topic 'Challenges for National CSIRTs in Europe in 2016'. The report targets national and governmental CSIRTs concerned by the NIS directive, and proposes a definition of three levels of maturity for these CSIRTs, along with a validation process.
WPK 2.1.B: Assistance in the area of cybersecurity strategies	
D8: Assist and advise Member States on the establishing and evaluation of NCSS (workshops Q1-Q4, 2016).	Workshop organised together with the Slovakian Presidency of the EC in November, bringing together stakeholders from more than 15 Member States.
D9: Update good practice guide on NCSS (report, Q4, 2016).	Updated good practice guide was published in November 2016 following validation phase with all relevant stakeholders and the ENISA NCSS experts group.
WPK 2.1.C: Assistance in the area of privacy and trust	
D11: On-request support for MS decision-making in the areas of privacy and trust (Q4, 2016).	The Agency supported EC DG Connect H1 on the preparation for the proposal for a regulation on privacy and electronic communications and provided working papers on the review of the ePrivacy Directive — Article 4 — Security of processing. In addition, the Agency worked closely with nominated experts from Member States and produced a study on indispensable baseline security requirements for the procurement of secure ICT products and services.

[1] After the amendment of Work Programme, WPK 2.1 starts with D2, due to re-allocation of resources and budget.

SO2 — To assist the Member States and the Commission in enhancing capacity building throughout the EU	
WPKs, impact indicators	**Achieved results**
WPK 2.2: Support European Union institutions' capacity building	
WPK 2.2.A: Information notes on NIS: production and review mechanisms ('info notes')	
D1: Review and adjust mechanism for production of info notes (Q1-4, 2016).	The info notes team set a pre-defined list of public NIS sources to follow and liaise for the topic selection based on the impact, novelty, press misrepresentation and added value of the topic. The notes were peer reviewed before publication and were re-reviewed (when needed) upon receiving external feedback.
D2: Restricted and public info notes on NIS (Q1-Q4, 2016).	In 2016 info notes were published on ENISA's website, becoming available to any interested party. ENISA published 23 info notes covering a wide range of NIS issues, namely: Ransomware, data breaches, cyber-attacks, malware, vulnerabilities, etc. These notes were circulated to ENISA's NLOs and published on the ENISA website. https://www.enisa.europa.eu/publications/info-notes
These notes were circulated to ENISA's NLOs and published on the ENISA website.	In 2016, info notes are published on the ENISA website and are publicly available for all interested stakeholders and announced on relevant channels.
WPK 2.2.B: Reinforcement of the NIS of Union institutions, bodies and agencies	
D3: Restricted. Upon request, support the assessment of existing policies/procedures/practices on NIS within EU institutions (workshop, meetings, Q1-4, 2016).	A report has been produced which served as input to the NIS Directive Cooperation Group meetings.
WPK 2.3. Assist private sector capacity building	
D1: Recommendations for creating a cybersecurity culture and improving management-level cybersecurity awareness (Q4, 2016).	This report has analysed cyber hygiene programmes across Europe https://www.enisa.europa.eu/publications/cyber-hygiene
WPK 2.4: Assist in improving general awareness	
D2: ENISA cyber challenge (Q2, 2016).	ENISA supported the ECSC2016 event by providing project management assistances. The full report of the event is expected to be delivered by the 2016 hosting country, Germany.
D3: Provide guidance and support for ECSM (dissemination material, Q4, 2016).	The 2016 ECSM Deployment Report describes the ECSM campaign and highlights the results and shortfalls for the year. https://www.enisa.europa.eu/publications/ecsm2016-deployment-report
D4: Upgrade the online privacy tools portal and involve privacy experts from different fields (dissemination material, Q4, 2016).	The updated content was promoted through the ECSM portal https://www.enisa.europa.eu/publications/ecsm2016-deployment-report

1.3 KEY RESULTS IN THE IMPLEMENTATION OF SO3 — ASSISTANCE IN DEVELOPING AND IMPLEMENTING THE NIS-RELATED POLICIES

SO3 provides the framework for ENISA to assist the EU MS and the EU institutions in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security (NIS).

List of work packages and short description

WPK 3.1 — Supporting EU policy development
The key objective of this work package (WPK) was for ENISA to proactively contribute to the development of existing or new EU policy initiatives (before they are launched) and assists the Commission, Member States and the private sector in the implementation of existing policies in this area.

ENISA achieved this objective by engaging with public and private stakeholders and leveraging its existing knowledge and expertise in the area of secure infrastructure and services.

Another key objective of this WPK was cybersecurity standardisation. From its initial set up, ENISA has tracked the development of standards in the area of NIS, maintaining close contacts and collaboration with international standardisation organisations. This approach enables ENISA to keep its activities up-to-date with the latest developments as well as informing its stakeholders on new NIS standardisation activities and to flag opportunities and/or risks as they develop.

In line with the more proactive role given to the Agency in the latest mandate, ENISA supported this area, in cooperation with relevant stakeholders, by developing recommendations for improving NIS in EU standardisation policy, providing guidelines of the possible frameworks that can be adopted in order to achieve a harmonised scheme across MS, as well as setting recommendations for the stakeholders involved. Importantly ENISA contributes to standardisation by reviewing standardisation gaps and providing due justification for action by SDOs and stakeholders alike. Finally, ENISA contributes to the coordination of standards by joining key coordination groups and meetings for the purpose of providing the regulatory cybersecurity view to this important area of the EU policy framework.

WPK 3.2 — Supporting EU policy implementation
This WPK covered activities linked to the implementation of EU directives and regulations (i.e. activities linked to electronic identification and trust services (eIDAS) regulation, ePrivacy directive, general data protection regulation and the NIS directive) where ENISA has been assigned a role and responsibilities and where NIS is one of the main goals or means to achieve suitable implementation.

ENISA has cooperated with all EU Member States and the Commission to define the scope and the implementation priorities of the NIS directive, the actions related to ENISA and the sectors and/or services affected. As a result of this, the Agency then identified all relevant public and private stakeholders (e.g. competent authorities, manufacturers and operators) and engaged them in a structured dialogue on the key objectives of the NIS directive and how it can be best implemented within each sector and/or service.

> **ENISA achieved this objective by engaging with public and private stakeholders and leveraging its existing knowledge and expertise in the area of secure infrastructure and services.**

ENISA has been a recognised contributor to policy in privacy and trust and the Agency has extensively contributed to support the implementation of the personal data protection regulatory framework in many of its key technological aspects. ENISA continued supporting the implementation of EC Regulation 611/2013 by providing assistance regarding technical protective measures (appropriate cryptographic protective measures) as the abovementioned regulation requests ENISA to do.

ENISA continued collecting and analysing annual national reports of security breaches from national regulatory authorities (NRAs) in accordance with Article 13a of the framework directive on electronic communications. The Agency, in cooperation with experts from NRAs and the private sector (e.g. ENISA's e-communications reference group) analysed the national reports, compared them with previous years, identified new trends and developed good practices and lessons learned.

Another WPK area has been related to aspects of the implementation of the 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. Trust services are a key enabler for increasing citizens' confidence in online services, and given their nature, they require a high level of security to ensure their integrity and reliability. ENISA has contributed extensively to the area of securing trust services in the past by providing best practices for providers, recommendations on audit schemes, standardisation guidance, security-breach reporting and recommendations, etc. Building on the work of 2015, in 2016 ENISA focused on the key areas of interest for stakeholders' including guidelines on initiation and supervision of trust service providers (TSPs), update on relevant technical standards and security recommendations for relying parties of trust services.

1.3.1 WPK 3.1: Supporting European Union policy development

1.2.1.1 WPK 3.1.A: Contribution to EU policy linked to secure infrastructures and services

In this WPK, ENISA engaged with public and private stakeholders and developed state-of-the-art recommendations and good practices in secure infrastructure and services with the objective of proactively contributing to the development of existing or new EU policy initiatives (before they are launched) and assist the Commission, Member States and the private sector in the implementation of existing policies in this area.

ENISA achieved this objective by engaging with public and private stakeholders, by deploying existing expert groups, e.g. the European SCADA and control systems information Exchange (EuroSCSIE) and the EICS — ENISA ICS Security Stakeholder Group and by leveraging its existing knowledge and expertise in the area of secure infrastructure and services. One of the key vehicles to deliver this are the ENISA dedicated, area-specific, expert groups that develop useful insight, validate good practices and issue practical recommendations. Whenever necessary ENISA liaised with standards bodies to provide its technical opinion on future standards in the areas below.

The main areas covered in this WPK are as follows.

EU cloud computing strategy and partnership
ENISA organised the fourth edition of Secure Cloud conference; a series of very successful events that take place in Europe on Cloud Security with stakeholders from all across the Globe. During this conference, the ENISA Cloud Security and Resilience Experts Group met and discussed the provisions of the NIS directive for DSPs. Supporting the requirements of this group, ENISA published a small paper on 'Exploring Cloud incidents'.

EU smart grids and ICS-SCADA strategy
ENISA assisted the Commission, the Member States and the private sector in the implementation of the EU's smart grid strategy and ICS-SCADA actions. The agency, building on this existing knowledge and expertise, provided sound technical advice, recommendations and information on good practices in the area of minimum security measures for smart grids and ICS-SCADA, communication network dependencies, attacks and incident-reporting mechanisms for national critical industries. ENISA engaged with all relevant stakeholders, provided contributions to the Commission on policy initiatives (e.g. EU CSS, DG Energy's expert group 2 (EG2) and Energy expert cybersecurity platform (EECSP), CEN/Cenelec's M490, EuroSCSIE and distributed energy security knowledge (EE-Densek and Energy ISAC), and made sure that these efforts properly aligned with the EU's overall smart grid policy.

Policy discussions on the certification of components and systems
ENISA cooperated with the Commission, Member States and the private sector in order to foster EU policy discussion regarding a European framework for the certification of components and systems. The agency supported the discussion on the evolution of the existing initiatives. Through this, ENISA was able to provide suggestions to key decision-makers on the way MS and the EU should address this issue.

EU policy on NIS matters of the finance sector
ENISA continues its efforts in the area of the finance sector. The Agency assisted the European Banking Authority and the European Central Bank in the definition and implementation of the Payment Services Directive 2. ENISA organised two workshops with its Expert Group on Finance (EGFI) and discussed technical and policy implementation issues.

1.3.1.2 WPK 3.1.B: Policy development and standards

The new ENISA mandate gives the Agency a more proactive role in the area of standardisation. The task assigned to ENISA by the new regulation is to support standardisation by facilitating the establishment and take-up of European and international standards for risk management and for the security of electronic products, networks and services. A key element towards the objective of improved security standardisation is to facilitate close collaboration between policymakers, standardisation organisations and industry. ENISA facilitated the cooperation of stakeholders by engaging policymakers, standardisation organisations and industry, with the aim of putting forward common strategies to enhance NIS in EU standardisation policy.

Since 2012 ENISA has specifically participated in the creation and further work of the ETSI CEN-Cenelec Cyber Security Coordination Group (CSCG). In 2016 ENISA collaborated in the activities of the CSCG and worked on developing synergies between the CSCG and its WP.

In 2016 the Agency provided recommendations for improving NIS in EU standardisation policy and guidelines on the possible frameworks that can be adopted in order to achieve a harmonised scheme across MS.

1.3.1.3 WPK 3.1.C: Towards a digital single market for NIS and related IT products and services

In 2016, ENISA ran a study to assess the current NIS market in the EU from an economic and technical point of view under the light of the DSM Strategy and its future demands for protection. It focused on the European market, even where NIS offerings are from non-EU providers. The report provided an overview of the current characteristics that make EU products and services successful or non-successful in the market.

This report helped ENISA to advise the Commission and Member States to better identify where efforts should be placed in order to further support European NIS and related ICT industries and services in order to achieve and improve the adequate level of diversity and trust in the EU.

The report proposed guidelines (lessons learned and good practices) and recommendations to strengthen the supply of NIS products and services from EU suppliers, in the context of the DSM.

1.3.2 WPK 3.2. Supporting European Union policy implementation

1.3.2.1 WPK 3.2.A: Assist EU MS and Commission in the implementation of the NIS directive

This work package aimed to help EU MS, the private sector and the Commission to implement the NIS directive.

More specifically ENISA has assisted the Commission and MS in the establishment of the Cooperation Group envisaged in the NIS directive. The Agency, as a member of this group, has provided ideas to the Commission and MS about its governance structure, its objectives and themes to focus on as well as its working relationship to the CSIRT Network.

Digital service providers (DSPs)
ENISA has assisted the Commission and MS in the development of the implementing acts envisaged in the NIS directive on incident reporting schemes imposed on digital service providers (DSPs).

More specifically ENISA took stock of similar provisions, processes, laws and regulations (obligatory or voluntary) in MS and analysed them in order to identify commonalities. Also the Agency collected best practices from the private sector as regards incident reporting and security measures. Emphasis has been placed on the identification of the parameters determining the impact of an incident which will trigger the notification. In this respect, a full-fledged technical proposal on how to address the incident reporting requirements was developed by ENISA. The work done in this area represents a preliminary guideline on how incident notification provisions for DSPs could be effectively implemented across the EU. Based on valuable input from Member States and companies directly impacted by the directive, the guideline proposed arises from their good practices in matters such as identifying types of incidents, parameters and thresholds and results in an outline technical proposal that can tentatively be applied across EU.

At the same time, this guideline serves as a technical input to the foregoing process of adopting the implementing act that will further specify details regarding the incident notification provisions of the NISD.

Operators of essential services (OES)
Moreover, the underlying work in the area of operators of essential services (OES) has already started from 2016. In this respect ENISA started collecting well established approaches different MS use to identify their operators of essential services. The Agency analysed the different approaches in use and tried to identify commonalities that could constitute a basis for a harmonised approach. This work was not concluded in 2016 but will continue in 2017 and 2018. During this period ENISA will continue helping MS to develop more knowledge and expertise on this topic and will contribute in the discussions towards an aligned EU approach, if possible. This would allow operators of essential services operating across several MS to be treated in a seamless and consistent way.

In this effort ENISA has leveraged its existing knowledge and expertise in stakeholder engagement with the public and/or the private sector.

1.3.2.2 WPK 3.2.B: Assistance in the implementation of NIS measures of EU data protection regulation

ENISA has been a recognised contributor to policy in privacy and trust and the Agency has contributed extensively to the implementation of the personal data protection regulatory framework in many of its key technological aspects. As a core activity in supporting the protection of personal information, ENISA provided recommendations on technological measures to protect the confidentiality, integrity and authenticity of personal data. In 2016, ENISA shifted the focus on supporting personal data controllers and processors on calculating the risk related to personal data processing and selecting appropriate technological and organisation security measures. In addition, ENISA also conducted a study on personal data clouds ('PDCs'), identified the different architectures and component of PDCs and discussed their privacy and security challenges.

Furthermore, ENISA ensured continuity for the activities where the Agency has achieved high expertise in the area of privacy, as well as introducing some emerging new topics, which have become relevant for the privacy community. The Agency carried on with its work on privacy enhancing technologies (PETs), their evolution, newest ideas and most up-to-date features of PETs, their building blocks and a maturity assessment tool. Following previous work in the field of privacy engineering, in 2016 ENISA defined the 'PETs control matrix', an assessment framework and tool for the systematic presentation and evaluation of online and mobile privacy tools for end users. The defined framework relies on a set of assessment criteria, which can be broken down into specific parameters and assessment points, acting as indicators of certain properties and features of the tools.

In 2016, ENISA hosted the fourth edition of the Annual Privacy Forum (APF). In light of the general data protection regulation and the European digital agenda, DG CNECT, EDPS, ENISA and, Goethe University Frankfurt organised APF 2016 (http://privacyforum.eu). APF 2016 was held on 7 and 8 September at Goethe University, Frankfurt am Main, Germany. The event encouraged dialogue with keynote speakers, panel discussions, and provided room for exchange of ideas in between scientific sessions. The objective of the Agency for 2016, as in previous years, was to address the topics which are of current interest for the privacy community, in order to reach the maximum number of relevant participants, representing different stakeholder communities across Member States.

Regarding new activities, ENISA undertook a study to support SME's on how to adopt security measures for the protection of personal data, following a risk-based approach. In particular, the objectives of the study were to facilitate SMEs in understanding the context of the personal data processing operation and subsequently assess the associated security risks. Based on that the study also proposes possible organisational and technical security measures for the protection of personal data, which are appropriate to the risk presented and in accordance to the provisions of GDPR.

Finally, during 2016 ENISA supported the European Commission (DG CNECT) in the upcoming revision of the Directive 2002/58/EC (ePrivacy directive). ENISA acted as technical advisor of the EC on the topics below by producing respective working papers:

1. Effectiveness and efficiency of security rules in the electronic communications sector; this includes an assessment of relevance and added value of specific security rules in the electronic communications sector; (Article 4), taking into account the revised relevant provisions of GDPR;
2. Assessment of the option to enlarge the scope of security rules to encompass other critical actors in the electronic communications value-chain, such as component manufacturers, software providers, etc.

1.3.2.3 WPK 3.2.C: Assistance in the implementation of mandatory incident-reporting schemes

This work package focused on assisting regulatory authorities in the implementation of EU regulations related to mandatory incident reporting. It is based on the successful work done in this area over the years in the area of Article 13a.

The main tasks of this work package were to support the following:

- NRAs and EU MS on the implementation of Article 13a (security-breach notification).
- NRAs and EU MS on the implementation of Article 19 of the new regulation on eIDAS.
- ENISA has continued to collect and analyse national reports on security incidents in accordance with Article 13a of the framework directive on electronic communications. The Agency has analysed the national reports, compared them with previous years, identified new trends and developed good practices and lessons learned. The Annual Incidents Report 2016, including the analysis on the incidents reported, was published around September 2016.
- The CIRAS incident reporting platform was also improved to fit to the new requirements of the NRAs, in terms of new services and threats being added, together with an overall improvement of the reporting process and the user interface.

ENISA has cooperated with electronic communications providers and MS competent authorities (e.g. NRAs) to address security issues in an integrated and holistic manner. In that respect the Agency, in cooperation with the Commission, have continued their efforts towards achieving an EU level harmonised reporting scheme for the e-communication providers.

ENISA together with the Article 13a WG provided feedback to the EC on security aspects regarding the new telecom code. The feedback was well received as some of the observations are included in the new regulation proposal.

Also, in the area of security measures for e-communication providers, the Agency has developed a line of work with the objective of identifying concrete security measures deployed in the telecom sector, that draws on experience gathered in terms of security measures.

ENISA has continued its efforts to develop common guidelines for a cost-effective mandatory security breach notification scheme implementing Article 19 of the eIDAS regulation. The Agency, building on the Forum of European Supervisory Authorities for Electronic Signatures (FESA) and other related public stakeholder groups, has brought together most of the EU stakeholders to discuss the scope of the scheme, the services affected, the impact of the incidents reported (e.g. parameters and thresholds), the reporting attributes, the reporting modalities, the reporting tools and others.

In this respect, ENISA has developed a security incident reporting framework for TSPs (trusted service providers) covering Article 19 of the European eIDAS regulation, with the objective of supporting efficient and harmonised incident notification schemes across the European Union. The Agency has also developed a tool (CIRAS-T) which enables supervisory bodies to submit their national reports to ENISA and the Commission.

1.3.2.4 WPK 3.2.D: Support for policy implementation in the area of electronic identification and trust services

The main objective of this WPK was to continue to support the large-scale adoption of secure electronic identification means and trust services across Europe. Trust services are a key enabler for increasing citizens' confidence in online services, and given their nature, they require a high level of security to ensure their integrity and reliability. ENISA has contributed extensively to the area of securing trust services in the past by providing best practices for providers, recommendations on audit schemes, standardisation guidance, security-breach reporting recommendations, etc.

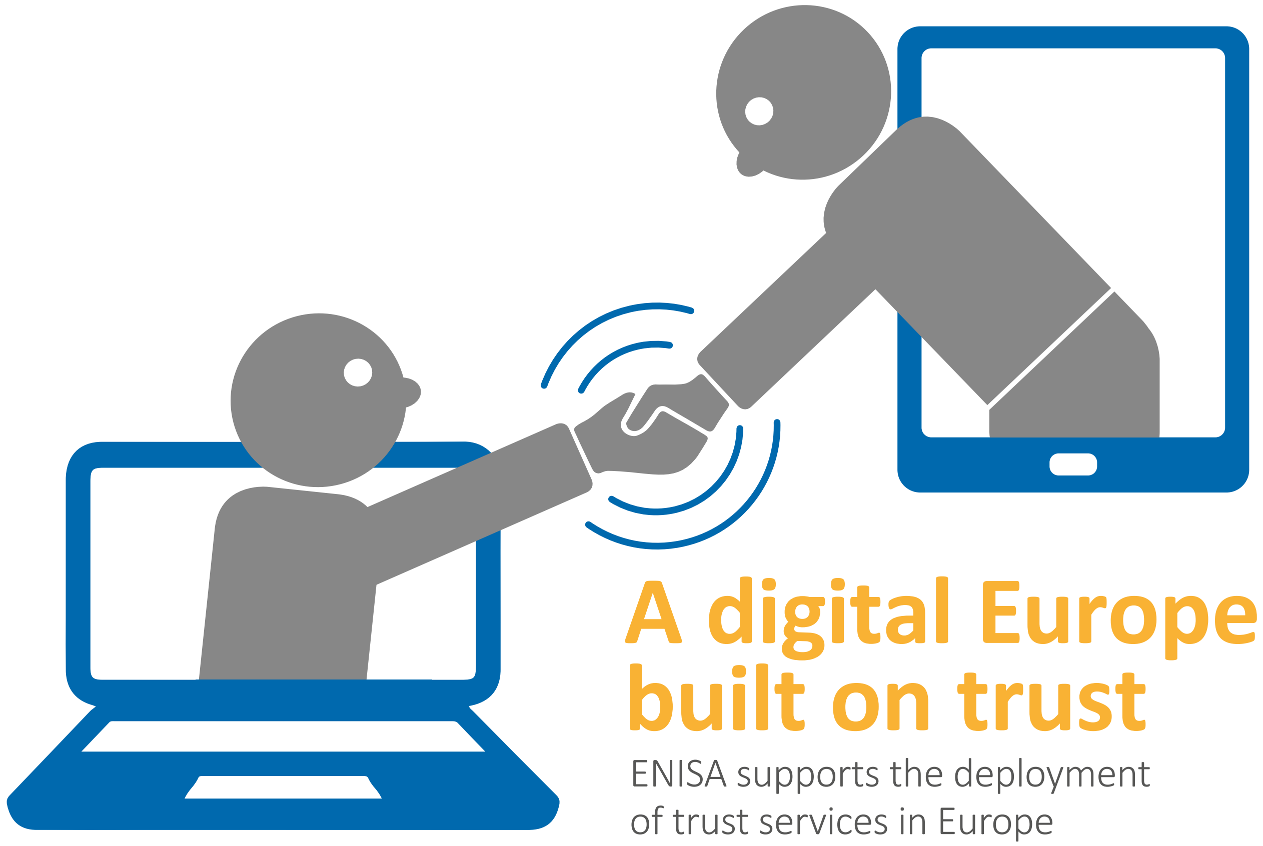
From the policy perspective, a milestone in this area was achieved with the adoption of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market. ENISA aims to support the implementation of the regulation by further focusing on the security aspects related to trust services providers.

In order to identify key aspects and gaps in this area, in 2015 ENISA launched, in collaboration with the EC, a forum that brings together communities, namely: trust service providers from the EU trusted lists, conformity assessment bodies and supervisory authorities. The forum has proven to be a useful tool for identifying gaps and areas where further work is needed, and its activities continued in 2016. The 2016 edition took place on 24 May in Brussels with a broad participation of stakeholders.

ENISA continued working on the implementation and update of the guidelines for security incidents notification to supervisory bodies by trust service providers (facilitating the application of the obligation stemming from Article 19 of the regulation). For this reason, ENISA has launched the Article 19 expert group that brings together the representatives from national competent authorities responsible for the implementation of the eIDAS Article 19 security measures and incident notification requirements.

ENISA continued supporting the EC in the assessment of the candidate standards that might be listed in implementing acts that may be adopted by the EC. This activity aimed to develop a concise set of technical guidelines implementing the eIDAS regulation in the non-mandatory articles, for voluntary use of all stakeholders, including trust service providers, supervisory bodies and conformity assessment bodies. The objective was to provide guidelines to meet requirements originating from specific provisions of the eIDAS regulation.

The study on security recommendations for relying parties of trust services, resulted in a series of five documents which aim to assist parties wishing to use qualified electronic signatures, seals, time stamps, eDelivery or website authentication certificates to understand the subject correctly as well as the potential benefits, amongst others, by giving examples of possible application. This series of documents also targets giving those parties some advice on how to correctly deploy and use the related qualified trust services.



A digital Europe built on trust

ENISA supports the deployment of trust services in Europe

1.3.3 General results. Achievement of impact indicators for Objective 3

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	
WPK 3.1: Supporting European Union policy development	
WPK 3.1.A: Contribution to EU policy linked to secure infrastructures and services	
By 2017, 15 companies and five MS competent authorities contribute to ENISA's efforts in the area of cloud computing.	ENISA involved more than 15 companies and five MS competent authorities in the efforts under Cloud security (Secure Cloud and the paper).
By 2017, 15 companies and five MS competent authorities contribute to ENISA's efforts in the area of smart grids and/or ICS-SCADA.	ENISA involved more than 15 companies and five MS 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 to ICS/SCADA in Frankenthal, Germany in September 2016 and another one during 4SICS in Stockholm in October 2016.
By 2017, 10 companies and five MS competent authorities contribute to ENISA's efforts in the area of certification of components and systems.	Almost 70 participants (six Member States and more than 30 private companies) in the certification workshop organised in March.
By 2017, 10 companies and five MS competent authorities contribute to ENISA's efforts in the area of finance.	ENISA's Expert Group on Finance (EGFI) grew to 35 members all of which 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 implementation of PSD 2.
WPK 3.1.B: Policy development and standards	
At least six stakeholders from policymakers, industry and research experts in NIS standardisation to contribute in ENISA's recommendations for improving NIS in EU standardisation policy.	More than six stakeholders were involved in the preparation of the report, including also experts participated in the review and validation of the findings.
WPK 3.1.C: Towards a digital single market for NIS and related IT products and services	
EU and national policymakers understand how the strengths and weaknesses of the NIS and related IT sector in Europe.	ENISA involved more than 15 companies and associations of organisations in the data collection phase of this report. ENISA organised one work meeting in June and one validation workshop in October to validate the findings.
EU and national policymakers understand how to develop a digital single market (DSM) for NIS and related products and services.	ENISA involved more than 15 companies and association of organisations in the data collection phase of this report. ENISA organised one work meeting in June and one validation workshop in October to validate the findings.
WPK 3.2: Supporting European Union policy implementation	
WPK3.2.A: Assist EU MS and Commission in the implementation of the NIS directive	
By 2017, 10 MS contribute to ENISA's efforts for harmonised implementation of the NIS directive.	ENISA has engaged with almost all MS in our effort of developing guidelines that can contribute to a proper implementation of the NIS directive EU wide. More than 20 MS answered to the surveys launched in the area of NIS directive.
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 has 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, their number was way bigger during workshops and other activities.

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	
By 2018, five MS deploy ENISA's guidelines on NIS directive in three sectors/services.	To be determined in 2018.
By 2018, 10 private organisations deploy ENISA's guidelines on NIS directive in three sectors/services.	To be determined in 2018.
WPK 3.2.B: Assistance in the implementation of NIS measures of EU data protection regulation	
At least five representatives from different MS contributing to ENISA guidelines and best practice recommendations regarding technological measures to protect privacy and trust and privacy-enhancing technologies (PETs), at least 10 actors in the field validating the results of the studies.	ENISA involved more than five representatives from Member States and more than 10 acknowledged researchers in the area of privacy-enhancing technologies during the preparation and validation of the results of the study. Through a specific session that was organised as part of Annual Privacy Forum 2016, valuable insights and feedback was collected and incorporated to the final report.
At least six experts from the health sector and DPA to contribute on the study on online and mobile applications, and six stakeholders to validate the results of the study.	ENISA involved more than six experts from data protection authorities, research and academia while preparing the study. Through a specific session that was organised as part of Annual Privacy Forum 2016, valuable insights and feedback was collected and incorporated to the final report.
More than 80 participants in Annual Privacy Forum (APF) 16: (researchers, policymakers and industry participants).	Annual Privacy Forum 2016 was attended by more than 100 registered participants from research, academia, industry and policymakers.
At least six stakeholders from policymakers, industry security practitioners and data controllers to contribute to the study on guidelines for data controllers on securing the automated processing of personal data, and six stakeholders to validate the results of the study.	ENISA involved more than six representatives from data protection authorities, researchers and policymakers on designing the guidelines. Through a specific session that was organised as part of Annual Privacy Forum 2016, valuable insights and feedback was collected and incorporated to the final report.
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 nationally level.	Almost all MS take part in Article 13a workshops. All MS 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.
By 2017, 15 Member States contribute to ENISA's efforts on harmonised implementation of Article 19 of eIDAS regulation.	Three meetings of eIDAS Article 19 expert group organised in 2016. On average, more than 15 MS participated in each one of them.
WPK 3.2.D: Support for policy implementation in the area of electronic identification and trust services	
At least six stakeholders from trust service providers, online services providers, conformity assessment bodies and supervisory authorities contribute in ENISA guidelines and best practices recommendations regarding electronic identification and trust services.	More than six stakeholders were involved in the preparation and validation of the reports, including Member State representatives participating at eIDAS expert group, members of Forum of European Supervisory Authorities for trust service providers — FESA, CA/Browser Forum, and ETSI. The findings of the reports were also presented in the Trust Services Forum.
At least 10 experts from the community participate in the validation of the results of the studies.	More than 10 experts in the area of trust services stakeholders were involved in the preparation and validation of the reports. The findings of the reports were also presented in the Trust Services Forum.

1.3.4 Specific results. Mapping of deliverables into papers/publications/activities

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, deliverables	**Specific achievements: papers/publications/activities**
WPK 3.1: Supporting European Union policy development	
WPK 3.1.A: Contribution to EU policy linked to secure infrastructures and services	
D1: Contribute to EU policy in the area of cloud computing (workshops, meetings, Q1-Q4, 2016).	ENISA organised the Secure Cloud conference and published a paper on Exploring Cloud incidents (cloud forensics). https://www.enisa.europa.eu/publications/exploring-cloud-incidents
D2: Contribute to EU policy in the area of smart grids and ICS-SCADA (workshops, meetings, Q1-Q4, 2016).	ENISA organised open sessions on network attacks to ICS/SCADA in Frankenthal, Germany in September 2016 and another one during 4SICS in Stockholm in October 2016. Together with MSB it also co-hosted an EUROSCSIE members meeting in Stockholm in October 2016 at MSB premises.
D3: Support the policy discussions in the area of IT security certification (workshops, meetings, Q1-Q4, 2016).	ENISA organised a series of workshops in the area of ICT security certification and supported the EC in the discussions for a roadmap proposal.
D4: Contribute to EU policy in the area of finance (workshops, meetings, Q1-Q4, 2016).	ENISA organised two workshops with the Expert group on Finance. Also organised an industry event for the financial institutions in Brussels.
WPK 3.1.B: Policy development and standards	
D5: Recommendations for improving NIS in EU standardisation policy (Q4, 2016).	ENISA published in 2017 'Challenges of security certification in emerging ICT environments' and 'Recommendations for improving NIS in EU standardisation policy'; https://www.enisa.europa.eu/publications/challenges-of-security-certification-in-emerging-ict-environments; https://www.enisa.europa.eu/publications/gaps-eu-standardisation
WPK 3.1.C: Towards a digital single market for NIS and related IT products and services	
D6: Restricted. Towards a DSM for NIS products and services (workshop, report, Q4, 2016).	Work meeting and validation workshop took place in 2016. The preliminary findings were disseminated with the targeted stakeholders and ENISA MB.
WPK 3.2: Supporting European Union policy implementation	
WPK 3.2.A: Assist EU MS and Commission in the implementation of the NIS directive	
D1: Contribute to the establishment of the cooperation group (meetings, workshops, Q2-Q4, 2016)	ENISA has participated in one meeting of the cooperation group and two meetings of the informal NIS group. More specifically ENISA has assisted the Commission and MS in the establishment of the Cooperation Group envisaged in the NIS directive. The Agency, as a member of this group, has provided ideas to the Commission and MS about its governance structure, its objectives and themes to focus on as well as its working relationship to the CSIRT network.
D2: Advice on the implementation of mandatory incident reporting for DSPs — input to the Implementation Acts (report, workshop, Q4, 2016).	Paper published in 2017. The workshop was held in Bratislava in October 2016 together with the Slovakian Presidency gathering representatives from all MS and EFTA countries. https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive
D3: Advice on the implementation of security requirements for DSPs — input to the Implementation Acts (report, workshop, Q4, 2016)	Paper published. ENISA has also provided input in order for COM to draft the implementing act on security measures for DSPs. The workshop was held in Bratislava in October 2016 together with the Slovakian Presidency gathering representatives from all MS and EFTA countries. https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers
D4: Assist MS in the identification of operators of essential services (workshop, Q2-Q4, 2016)	The workshop was held in Bratislava in October 2016 together with the Slovakian Presidency gathering representatives from all MS and EFTA countries.
WPK 3.2.B: Assistance in the implementation of NIS measures of EU data protection regulation	
D5: Evolution and state of the art of privacy enhancing technologies and their building blocks (Q4, 2016)	Paper published in 2017. A specific session that was organised as part of Annual Privacy Forum 2016. https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art
D6: 2016 edition of the report on appropriate technological protection measures to preserve privacy and trust (Q4, 2016).	Paper published in 2017. A specific session that was organised as part of Annual Privacy Forum 2016. https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing
D7: Data protection and security in online and mobile applications (i.e. healthcare) (Q4, 2016).	Paper published in 2017. https://www.enisa.europa.eu/publications/privacy-and-security-in-personal-data-clouds
D8: Annual Privacy Forum (Q2, 2016)	The event was organised in 7-8 September 2016 in Frankfurt, Germany. http://2016.privacyforum.eu http://link.springer.com/book/10.1007%2F978-3-319-44760-5; https://www.enisa.europa.eu/publications/annual-privacy-forum-2016
D9: Guidelines for data controllers on securing the automated processing of personal data (Q4, 2016)	Paper published in 2017. A specific session that was organised as part of Annual Privacy Forum 2016. https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing
WPK 3.2.C: Assistance in the implementation of mandatory incident-reporting schemes	
D10: Annual incident analysis report (Article 13a) (workshop and report, Q3, 2016).	In the context of Art. 13a, ENISA organised three workshops: in Budapest in March, in Lillesand in June and in Prague in November. All the MS and EFTA countries participated. The Annual Report was published in September 2016. https://www.enisa.europa.eu/publications/annual-incident-reports-2015
D11: Analysis of security measures deployed by e-communication providers (workshop and report, Q4, 2016).	The report was published and a validation session was held during Art. 13a workshop in November in Prague. https://www.enisa.europa.eu/publications/security-measures
D12: Contribute to EU policy in the area of electronic communications sector (workshops, meetings, Q1–Q4, 2016).	ENISA organised a workshop on mobile network attacks in Berlin in October 2016 and involved relevant stakeholders in the activities of the INFRASEC group.
D13: Engaging eIDAS competent authorities in the implementation of Article 19 (workshops, Q1–Q4, 2016).	ENISA organised three (3) meetings for the Article 19 expert group, the representatives from the eIDAS Article 19 national competent authorities, in 2016.
D14: Guidelines for mandatory incident reporting in the context of eIDAS (report, Q4, 2016).	Published in 2017. https://www.enisa.europa.eu/publications/article19-incident-reporting-framework

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, deliverables	**Specific achievements: papers/publications/activities**
WPK 3.2.D: Support for policy implementation in the area of electronic identification and trust services	

D15: Update on standards for trust services and electronic identification (Q4, 2016).	A series of focused reports were published in 2017
	https://www.enisa.europa.eu/publications/tsp-supervision;
	https://www.enisa.europa.eu/publications/tsp-initiation;
	https://www.enisa.europa.eu/publications/tsp-security;
	https://www.enisa.europa.eu/publications/tsp-audit

D16: Report on security recommendations for relying parties of trust services (Q4, 2016).	A series of reports, one for each Trust Service, was published in 2017 https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-signatures https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-seals https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-time-stamps https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-registered-delivery-services https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-website-authentication-certificates

1.4 KEY RESULTS IN THE IMPLEMENTATION OF SO4 — COOPERATION ENHANCEMENT BETWEEN NIS-RELATED COMMUNITIES AND STAKEHOLDERS

SO4 covers aspects of cooperation between the EU MS and the EU and between related NIS communities where ENISA could play a role in enhancing NIS cooperation.

List of work packages and short description

WPK 4.1 — Cyber crisis cooperation and exercises
In the context of this work package (WKP), ENISA further enhanced its methodology, seminars, training and technical capabilities on the organisation and management of large-scale cyber crisis exercises. The Agency continued enhancing its internal capabilities for managing complex, distributed exercises, by building on its previous efforts. ENISA explored new opportunities that will enhance the overall realism of cyber exercises.

In 2016, ENISA organised the fourth pan-European cyber exercise, Cyber Europe 2016 (CE2016). This exercise builds on the experience gained in previous exercise and takes into account previously identified recommendations and findings.

Furthermore, ENISA continued supporting Member States towards the development of a sound and implementable European cyber crisis cooperation framework and procedures.

WPK 4.2 — NIS community building
The key goal of this WPK is to build upon the good experience ENISA has in supporting different operational communities (CSIRT network, law enforcement communities, European financial institutes — information sharing and analysis centre (FI-ISAC), A-ISAC, etc.) to enhance mutually satisfactory ways to collaborate.

ENISA developed and provided guidance based on good practice in the area of operational community efforts (operational cooperation, information exchange, etc.). Where possible, synergies with other ENISA collaboration- and community-supporting efforts were extended and, where needed, developed.

The Agency continued its work and support of the Transits training in the area of CSIRTs in order to build communities through a 'learning by doing' approach.

ENISA continued to support the collaboration between CSIRT and law enforcement communities, based on the recent policy and technical developments in this area in Member States.

1.4.1 WPK 4.1 Support for EU cooperation initiatives through initiatives amongst NIS-related communities in the context of the EU CSS

In 2016 ENISA further enhanced capacity on the organisation and management of large-scale cyber crisis exercises, while also organised a number complex, distributed exercises with enhanced realism.

Exercise Organisation
In 2016, the Agency organised together with the MS the fourth pan-European cyber exercise, Cyber Europe 2016 (CE2016). CE2016 was a large-scale distributed technical and operational exercise started in April 2016, offering the opportunity to cybersecurity professionals across Europe to analyse complex, innovative and realistic cybersecurity incidents.

On 13 and 14 October, ICT and IT security industry experts together with cybersecurity authorities, were called upon to mitigate the apex of this 6-month long cyber crisis, to ensure business continuity and, ultimately, to safeguard the European ICT market. The Cyber Europe motto is 'stronger together': Indeed cooperation at all levels is key to the successful mitigation of major, borderless cyber incidents. CE2016 overall in the 6-month period engaged over 1 000 participants.

EuroSOPEx 2016 was another exercise organised by the Agency during this year. EuroSOPEx is a distributed table-top exercise for the national and governmental CSIRTs that trains on multinational cooperation procedures. The exercise was organised in four sessions in June and engaged over 50 participants.

Finally, ENISA supported the exercise Multilayer 2016 (ML16) organised the European External Action Service (EEAS). In particular, after a formal request (c.f. Article 14 of the Agency's regulation) from EEAS developed the cybersecurity sub-scenarios of this joint civil–military exercise and provided support during the execution of the exercise, in relation with the cybersecurity scenarios.

Enhanced capacity to support and organise cyber exercises
In 2016 ENISA further enhanced its methodology, seminars, training and technical capabilities on the organisation and management of cyber crisis exercises. The Agency developed capabilities for managing complex, distributed exercises with enhanced realism.

In the context of this effort ENISA expanded and improved its cyber exercise platform (CEP). CEP is a set of interconnected infrastructures supporting exercise management as well as the exercise play/reality through a virtual universe. The former includes capabilities such as exercise planning, scenario management, injection, visualisation, control, monitoring and evaluation. The latter includes virtual universe of several simulated online web services, such as social media, websites, video streaming services and network infrastructures.

As a result of an agreement reached in 2016, ENISA is also assisting the European Defence Agency (EDA) in the organisation of cyber exercises for their community.

Cyber crisis cooperation and exercises activities overview
In 2016 ENISA, in close cooperation with the EU Member States and institutions, drafted a proposal for a pan-European roadmap for cyber exercises. This roadmap will guide the exercise developments in the coming years.

ENISA continued supporting the EU Member States towards the development of sound and implementable European cyber crisis cooperation framework and procedures. The Agency will continue exploring requirements for developing infrastructures for cooperation, e.g. secure communications channels or directories. In this context, ENISA supported the effort to review and revise the EU Cyber Standard Operational Procedures (EU-CSOPs). These EU-CSOPs were put under test both in EuroSOPEx and Cyber Europe 2016. Related to this set of activities, in 2016 the European Commission announced in the Communication COM(2016)/410 — 'Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry' the development in 2017 of a 'blueprint' that will ensure the synergies and coherence for the crisis cooperation during significant cyber incidents.

1.4.2 WPK 4.2. Support for EU cooperation initiatives amongst NIS-related communities in the context of the EU CSS

Objectives:

- Support incident-response community building and information exchange.
- Contributing to the existing communities' efforts in the incident response field.
- Enable continuous trust and collaboration building for communities through regular events.
- Information provided to key stakeholders on NIS policy developments.

The key goal of this WPK was to build upon the good experience ENISA has acquired in supporting different operational communities (CSIRT, law enforcement communities, European FI-ISAC, A-ISAC, CSIRT network provided for by the NIS directive, etc.) to enhance mutually satisfactory ways to collaborate.

ENISA developed and provided guidance based on good practice in the area of operational community efforts (operational cooperation, information exchange, etc.). Where possible, synergies with other ENISA collaboration- and community-supporting efforts will be extended and, where needed, developed.

The Agency continued its work and support of the TRANSITS training in the area of CSIRTs in order to build communities through a 'learning-by-doing' approach.

ENISA also continued to support the collaboration between CSIRT and law enforcement communities, based on the recent policy and technical developments in this area in Member States.
This work included close collaboration with other institutions, which are active in this field, namely the EC3. Activities agreed upon in the collaboration agreement between ENISA and EC3 were further developed. For example, in the area of encouraging a more practical and regular flow of information between CSIRTs and law enforcement communities, the exchange of specific knowledge and expertise, elaboration of general situational reports, reports resulting from strategic analyses and best practice and strengthening capacity building through training and awareness raising in order to safeguard NIS at EU level. To support better coordination and in order to avoid overlaps with ENISA activities, the agency will stay engaged in the EC3 programme board. The very well established, commonly organised ENISA-EC3 workshop was held in October that gathered 33 teams from 30 countries from the EU and EFTA countries.

Following its successful mechanism for building the European national and governmental CSIRT community trust and collaboration, ENISA organised its traditional workshop to support the national and governmental CSIRT community grow. (11th CSIRTs in Europe workshop).

In its Article 8b, the NIS directive established the CSIRTs network 'in order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation'. It is 'composed of representatives of the Member States' CSIRTs and CERT-EU'.

The CSIRTs Network provides a forum where Member States' National CSIRTs can cooperate, exchange information and also build trust. Member States CSIRTs are able to improve the handling of cross-border incidents, and even discuss how to respond in a coordinated manner to specific incidents.

ENISA provides the secretariat of the CSIRTs Network and actively support the cooperation among the CSIRTs. In 2016 the Agency organised the informal meeting of the CSIRTs Network adjacent to its 11th CSIRTs in Europe workshop. ENISA also provided its expertise and advice both to the Commission and Member States, either in the form of guidance or in answer to specific requests.

1.4.3 General results. Achievement of impact indicators for Objective 4

SO4 — To enhance cooperation both between the Member States of the EU and between related NIS communities	
WPKs, impact indicators	**Achieved results**
WPK 4.1: Cyber crisis cooperation and exercises	
At least 10 Member States and EU institutions take part in the study on cyber crisis cooperation and exercise activities and findings.	Fulfilled — over 20 experts from EU Member States, EFTA countries and EU institutions took part in the study on cyber crisis cooperation, while more than 1 000 participated in the exercises
At least 24 EU Member States and European Free Trade Association (Stockholm Convention) (EFTA) countries confirm their support for Cyber Europe 2016 (CE2016).	Fulfilled — all 28 EU Member States, two EFTA and several EU institutions participated in CE2016
At least 20 EU Member States will attend the ENISA event which aims to promote cyber crisis cooperation activities within the context of the existing NIS policy framework.	Fulfilled — over 50 experts from EU Member States, EFTA and several EU institutions participated in ENISA's 2016 events and conferences that promoted cyber crisis cooperation activities
WPK 4.2: Network and information security community building	
WPK 3.2.A: Assist EU MS and Commission in the implementation of the NIS directive	
At least 15 Member States participating at ENISA annual national and governmental CSIRT workshop and also in the joint ENISA-EC3 workshop on CSIRT-law-enforcement agency (LEA) collaboration.	The national and governmental CSIRT gathered 33 teams from 30 countries from the EU and EFTA countries.
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 Program Committee.

1.4.4 Specific results. Mapping of deliverables into papers/publications/activities

SO4 — To enhance cooperation both between the Member States of the EU and between related NIS communities	
WPKs, deliverables	**Specific achievements: papers/publications/activities**
WPK 4.1: Cyber crisis cooperation and exercises	
D1: Cyber Europe 2016: exercise plan and exercises (exercise Q4, 2016).	https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/ce-2016
D2: EuroSOPEx 2016: exercise plan and exercises (exercises Q4, 2016).	https://www.enisa.europa.eu/topics/cyber-exercises/other-cyber-exercises
D3: Pan-European cyber exercises roadmap (report Q4, 2016).	Restricted report
D4: Cyber crisis cooperation procedures: follow up the NIS policy framework (report Q4, 2016).	https://www.enisa.europa.eu/news/enisa-news/standard-operational-procedures-to-manage-multinational-cyber-crises-finalised-by-eu-efta-member-states-and-enisa
WPK 4.2: Network and information security community building	
D1: Continuation of existing community efforts (European FI-ISAC, FIRST, TF-CSIRT-TI, etc.).	In 2016, ENISA supported existing communities like FIRST, TF-CSIRT and the FI-ISAC, by promoting their activities, being present in their meetings, and taking part in their governance structure (TF-CSIRT Steering Committee, FIRST Conference Program Committee).
D2: Annual ENISA national and governmental CSIRT workshop (Q4, 2016).	The annual technical workshop for national and governmental CSIRTs was held in Riga on 11/05/2016. The event gathered representatives from more than 30 CSIRTs from the EU and EFTA countries (https://www.enisa.europa.eu/events/11th-csirt-enisa-workshop/11th-csirt-workshop).
D3: Annual ENISA/EC3 cybercrime workshop (Q4, 2016).	The annual ENISA/EC3 cybercrime workshop for CSIRTs and LEAs was held in The Hague on 08/11/2016. The event gathered over 80 CSIRT and LEA representatives from the EU and EFTA countries (https://www.enisa.europa.eu/events/5th-enisa-ec3-workshop)
D4: Supporting European network of MS CSIRTs.	ENISA participated in the inaugural informal meeting of the CSIRTs Network held in The Hague, and organised two further informal meetings on 10/05/2016 (Riga, Latvia) and 09/11/2016 (The Hague, The Netherlands). The Agency worked with the different Presidency teams to elaborate the Terms of Reference and the Work Plan for the CSIRTs Network.
D5: Review on new operational communities' development (A-ISAC, etc.) (Q4, 2016).	ENISA published a new report 'Cyber Security Information Sharing in the Energy Sector' that addresses the development of CSIRTs, ISACs, as well as relevant initiatives on information sharing on cyber security incidents in the energy sector by focusing on the subsectors identified in the NIS directive (European Parliament and Council, 2016) — namely electricity, oil and gas — complemented by the nuclear and alternative fuels subsectors. The report is available at https://www.enisa.europa.eu/publications/information-sharing-in-the-energy-sector

1.5 HORIZONTAL ACTIVITIES AND KEY RESULTS

1.5.1 Management Board, Executive Board and Permanent Stakeholders Group secretariat

During 2016, ENISA continued to support its formal bodies, the Management Board (MB) and the Permanent Stakeholder Group (PSG) as well as the Executive Board (EB) in their functions by providing secretariat functions.

For the MB, one ordinary meeting was organised during October 2016, to adopt decisions on budgetary and administrative matters as well as to discuss the approach and timeline of the preparation of Draft Programming Document 2018-2020. In June 2016 the MB held its extraordinary meeting to elect the Chairperson and the Deputy Chairperson. Mr Jean-Baptiste Demaison (France) has been appointed as Chairperson of ENISA's MB. Jean-Baptiste Demaison's mandate became effective starting of 18 October 2016. Mr Krzysztof Silicki (Poland) has been also appointed as the Deputy Chairperson of ENISA's MB with immediate effect.

In March 2016, the MB adopted the amended Work Programme 2016, which reflects the tasks addressed to ENISA in the NIS directive; the amended WP includes more activities addressed to the implementation of adopted NIS directive. In 2016, the MB decided to discontinue the MB Ad Hoc Group and instead held three MB informal meetings.

In 2016 the existing electronic newsletter was converted into a broader publication to reach other stakeholders, however the MB Portal is maintained for the exclusive benefit of the MB.

For the PSG, one formal meeting was organised in the course of the year to keep ENISA close to the industry, academia and all other society sectors that are represented in the Group and gather advice to the ENISA Executive Director on drawing up a proposal for the Agency's Work Programme.

Four of the EB formal meetings were organised during 2016; once per quarter (Q).

1.5.2 National Liaison Officer Network

Since 2014, ENISA has initiated a number of activities with the aim of strengthening cooperation within the national liaison officers' (NLO) network. In 2016, ENISA built upon these efforts and improved its cooperation with the NLO network, the first point of contact for ENISA in the MS. The agency maintained and shared with the NLO network information on all relevant ENISA project activities. Information was sent to the members of the NLO network at regular intervals on ENISA project-related tenders, vacancy notices, and events organised by ENISA or which the Agency contributed to (for example co-organiser, etc.) and a NLO meeting was organised to discuss improvements of the collaboration.

1.5.3 European Union relations

As in previous years, the Agency carried out the EU relations work with the statutory stakeholders: the Commission, the EU Parliament, the Council (working groups) and MS. Several meeting took place, at the highest level these were managed by the ED so that the level of participation is appropriate. A similar approach was taken for speaking engagements.

1.5.4 Stakeholders communication and dissemination activities

In 2016, ENISA continued to improve its focus on its key activities and to provide regular information to the press and media regarding these activities. In order to achieve this, constant contact with the media was maintained and trust relations established to assure adequate information of the EU citizens about ENISA's work and activities.

The Agency continued to develop various tools and channels such as info graphics, the ENISA website, social media, social networking and videos with continuous improvement of outreach. This resulted in an increase in numbers of press releases, website news item, wider media coverage, social media followers and interactions and overall communication with different stakeholders.

1.5.5 Quality management system

During 2016, the Agency started to put in place a quality management system. A quality management manual as well as standard operation procedures (SOPs) and work instructions (WINs) were drafted bases on ISO 9001 standards (the Agency does not have as objective to be certified). All these documents are in the phase of revision by the management and will be implemented in 2017.

Article 14 requests

Country	Effort person/ days	Effort in euros	Budget in euros	Status
Austria	9.0	4 608.00	6 787.00	In progress
Belgium	16.7	8 551.48	1 500.00	Complete
Cyprus	1.0	512.00	0.00	Complete
Czech Republic	28.0	14 337.82	1 700.00	Complete
Estonia	24.7	12 648.01	4 000.00	Complete
EP	40.0	20 482.60	4 500.00	Complete
EU	15.0	7 680.95	2 500.00	Complete
EU	10.0	5 120.00	1 000.00	Complete
EU	1.5	768.09	0.00	Complete
EU	0.5	256.03	0.00	Complete
EU	10.0	5 120.00	0.00	Complete
EU	13.0	6 656.84	7 000.00	Complete
EU	0.0	0.00	0.00	Starts in 2017
Germany	5.0	2 560.32	923.00	Complete
Germany	10.0	5 120.00	3 000.00	Complete
Germany	22.0	11 265.43	17 000.00	Complete
Greece	16.0	8 193.04	0.00	Complete
Greece	16.0	8 193.04	0.00	Complete
Hungary	14.0	7 168.91	2 200.00	Complete
Lithuania	28.0	14 337.82	5 500.00	Complete
Luxembourg	5.0	2 560.32	0.00	Complete
Macedonia	0.0	0.00	0.00	Declined
Malta	23.5	12 033.53	2 800.00	Complete
Poland	0.0	0.00	0.00	Starts in 2017
Romania	2.0	1 024.13	0.00	In Progress
Slovakia	36.0	18 434.34	3 300.00	Complete
Sweden	0.0	0.00	0.00	Starts in 2017

The quality control of the Agency aims to respond to a mix of regulatory and stakeholder requirements, to improve organisational performance and compliance. The primary goal of the QC is to improve performance across the agency while reducing operational costs and enhancing stakeholders satisfaction. The methodology is based on the plan-do-check-act (PDCA) cycle.

1.5.6 Article 14 requests

Article 14 of ENISA regulation provides a mechanism that allows the MS or EU institutions to make direct requests to ENISA for carrying out particular activities. This mechanism has become increasingly accepted in the last few years and it has grown in significance. In Work Programme 2016, under SO2, both WPKs WPK2.1 Assist MS capacity building and WPK2.2 Support EU institutions include deliverables dedicated to assistance/on-request support for EU MS and institutions. The table on the left provides a summary of Article 14 requests and their status at the end of 2016. It should be noted that some of these requests foresee activities during 2017.

1.5.7 Data Protection Officer

The main tasks of the Data Protection Officer (DPO) during 2016 included information and advice for the Agency on its obligations pursuant to Regulation 45/2001/EC. Activities included the requirements for data security, information of data subjects and their requests in exercising their rights under Regulation 45/2001/EC, as well as the requirements for prior check or prior consultation with EDPS.

1.6 KEY RESULTS FOR MANAGEMENT AND ADMINISTRATION ACTIVITIES

The ED is responsible for the overall management of the Agency. During 2016, the ED decided to set up an Executive Director's Office (EDO) to support his activities. The tasks covered by EDO include policy advice, legal advice, Management Board Secretariat and coordination of the Work Programme. In 2016, EDO continued to support the Management Board (MB) and the Executive Board in their functions by providing secretariat assistance.

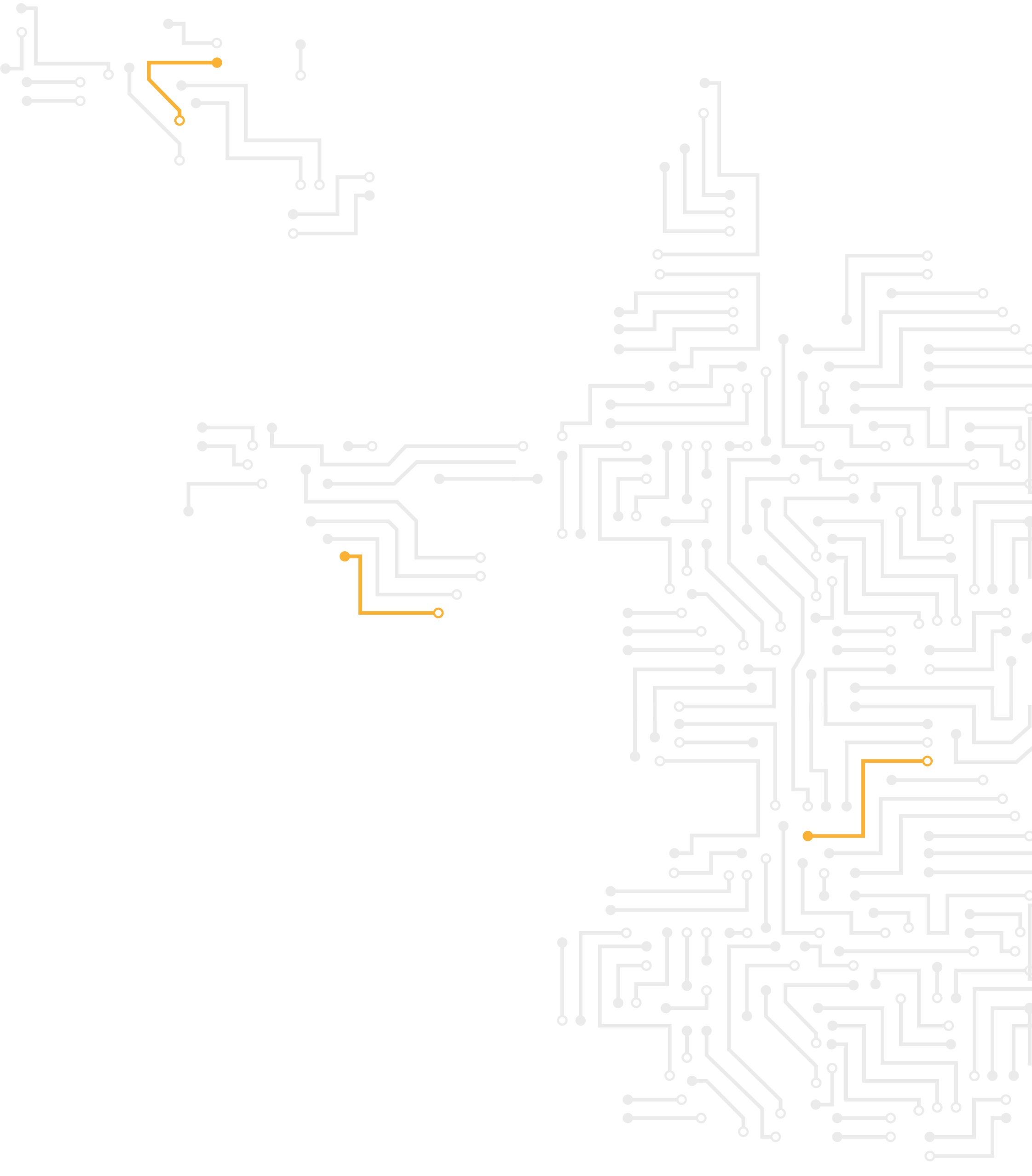
In order to gain in efficiency and effectiveness, the Administration and support department (ASD) became the Stakeholder Relations and Administrative Support Department (SRAD) during 2016.

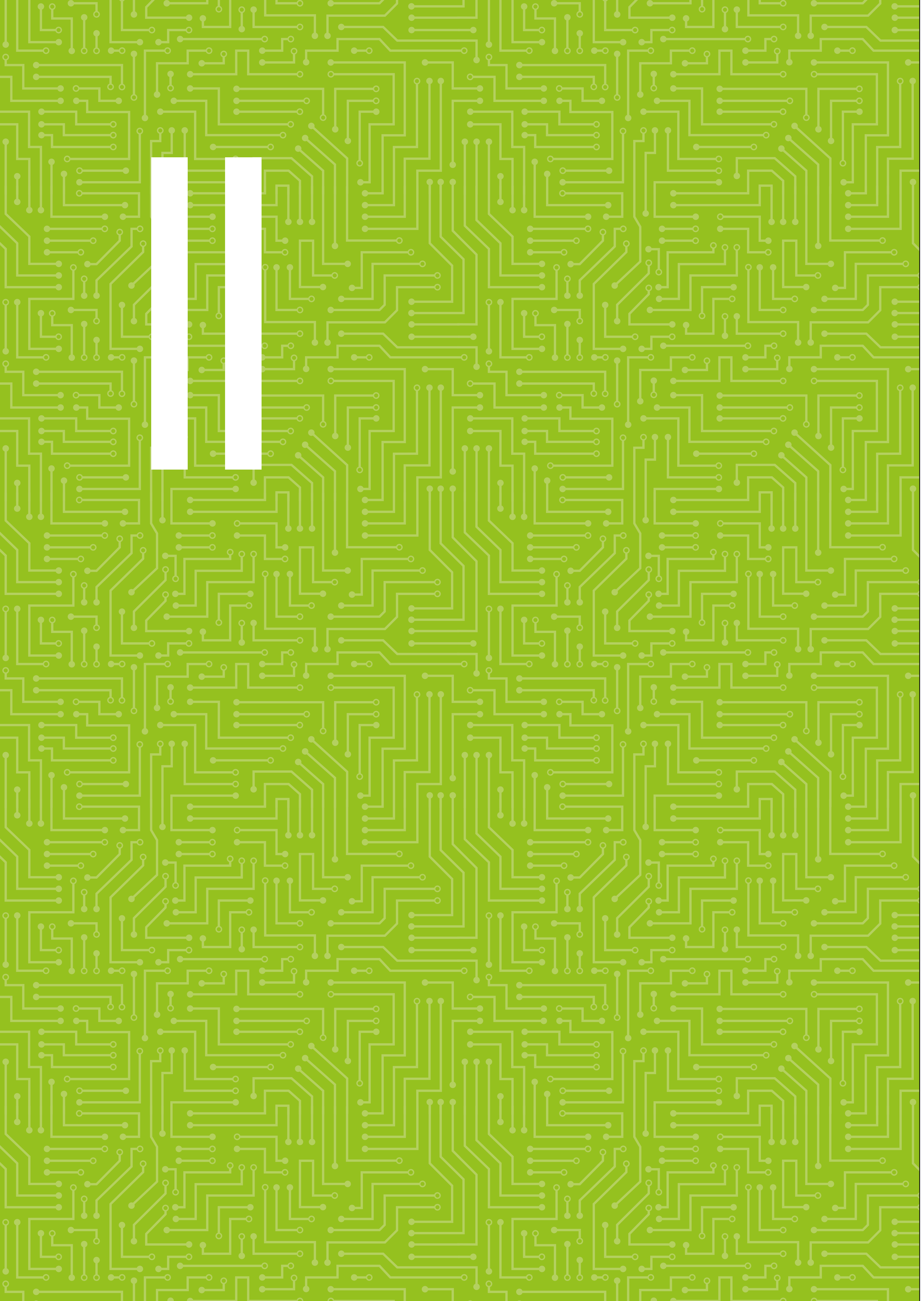
The SRAD is responsible for ensuring that the management of the Agency is in line with the regulatory framework established by the competent EU institutions, the MB and the ED. The regulatory framework is composed of the financial regulation and the staff regulations and their respective implementing rules, as well as administrative procedures, the internal control framework and other control mechanisms put in place to ensure compliance with the rules.

The SRAD monitors the Agency control and risk framework. Constant upgrading of the internal systems and revision of the operating standards set the ground for continuous optimisation of the internal processes and procedures. Benchmarking with other organisations, as well as the recommendations of the European Court of Auditors (CoA) and the Internal Audit Service (IAS) are used as internal performance indicators and relevant possibilities of improvement are considered. Furthermore, the SRAD department is the main contact point as regards administrative matters, with external stakeholders, including Hellenic authorities, etc.

The activities carried out in SRAD are reflected in the following table:

ASA 0: Executive director's office and general management	ASA1: QMS, ICC, security, fm and internal communications	ASA2: Finance and procurement	ASA3: Human resources	ASA4: Information and communications technology
Planning development	Organisational structure	Budget preparation and management	Multiannual Staff policy Plan	Service strategy
Implementation of Agency's strategy and Work Programme	Management reporting	Financial transactions' initiation	Management of individual staff rights and obligations, according to the stipulations of the Staff Regulations (SR)	Service transition
Overall management activities coordination	Meeting internal and external stakeholder's expectations	Central financial verification of all financial transactions	Recruitment procedures	Service security
Policy advice	Hellenic authorities and protocol	Financial helpdesk and reporting	Entitlements and leave management	Service operations
Legal advice	Development of quality management system	Mission management and helpdesk	Drafting internal HR policies and implementing rules of the SR	External services service support
MB Secretariat	Implementation of internal control standards	Statutory reporting activities, including discharge procedure	Medical services and health in work environment	
Work Programme coordination	Coordination and support to Internal Audit Service and European Court of Auditors	Accounting activities	Training plan and career development	
	Ex post controls	Procurement procedures, overall management, including procurement planning	Work environment and well-being	
	Physical security and safety	Internal training-related to FAP activities		
	Facilities management	Optimisation of internal financial workflows		
	Internal communication and staff welfare			





PART II
MANAGEMENT

The Annual Activity Report follows the guidelines published in Annex 2 'Template for Consolidated Annual Activity Report' part of Ares(2014)4305716-19/12/2014. However, to avoid duplication, information regarding Management Board is already located in section **2.5.1 Management Board, Executive Board and Permanent Stakeholders Group secretariat**. Furthermore, details regarding major developments are described in section **1.2 Highlights of the year** and in particular, in section **1.2.3 Information for the stakeholders**, as well as in section **2.6 Key results for management and administration activities**.

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 of ENISA Budget 2016 of EUR 10 984 847, were committed at a rate of 98.55 % on 31 December 2016. The remaining amount is a not automatic carry over committed in 2017 for refurbishment project.

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

The overall performance demonstrates the already proven capacity of the Agency to efficiently use the entrusted funds, in order to implement its annual Work Programme as well as manage its administrative expenditure and investments.

The respective payment rate on expenditure appropriations was 90.00 % in 2016. This payment rate is high and demonstrates that the capacity of the Agency to finalise its annual activities as well as 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 (2015) and enabled the launch of projects related to the Work Programme in early 2016, 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 effect of the Budget transfers No 1 to 8, approved by the Executive Director (ED) of ENISA, and the Amending Budget (AB) 1/2016, approved by the Management Board, on the initial Budget 2016:

Table — Summary of transfers and AB 1/2016 effect

Title	Initial budget	Transfers 1–8 B2016 approved by the ED	Amending Budget 1/2016	New Appropriations 2016 (AB 1/2016)
Title 1 — Staff	6 334 000.00	– 200 763.03	– 117 222.22	6 016 014.75
Title 2 — Administration	1 600 000.00	129 591.46	227 857.54	1 957 449.00
Title 3 — Operations	3 126 564.00	71 171.57	– 137 225.16	3 060 510.41
Total	**11 060 564.00**	**0.00**	**– 26 589.84**	**11 033 974.16**

The table below summarises the effect of Budget transfer No 9, approved by the ED after the adoption of the AB 1/2016 to the final budget execution:

Table — Summary of transfers' effect on final budget execution

Title	New Appropriations 2016 (AB 1/2016)	Transfers 9 B2016 approved by ED	Final Budget Execution 2016
Title 1 — Staff	6 016 014.75	– 4 012.18	6 012 002.57
Title 2 — Administration	1 957 449.00	7 965.01	1 965 414.01
Title 3 — Operations	3 060 510.41	– 3 952.83	3 056 557.58
Total	**11 033 974.16**	**0.00**	**11 033 974.16**

2.1.3 Carry forward of commitment appropriations

The commitment appropriations corresponding to the EU subsidy (C1 appropriations), which were not consumed by payments at the end of 2016, were carried forward (automatic carry forward) to 2017 (C8 appropriations).

The appropriations corresponding to the EU subsidy (C1 appropriations), which were not committed by the end of 2016, were carried over (non-automatic carry over to C3 appropriations in 2017).

The commitment appropriations corresponding to the subsidy from the Hellenic Authorities for the lease of ENISA premises in Greece (external assigned revenue — R0 appropriations) which were not paid by 31 December 2016, were carried forward (automatic carry forward to R0 appropriations 2017).

The funds carried forward to 2017 (C8 appropriations) are detailed below:

Title	Total C1 appropriations carried forward to 2017	Carried Over (C1 2016 to C3 2017) EU subsidy	Carried Forward (R0 2016 to R0 2017) Subsidy from Hellenic Authorities	
Title 1 — Staff	380 610.17	0.00	0.00	380 610.17
Title 2 — Administration	300 018.38	159 000.00	51 364.89	510 383.27
Title 3 — Operations	287 569.77	0.00	0.00	287 569.77
Total	**968 198.32**	**159 000.00**	**51 364.89**	**1 178 563.21**

The total cancelled appropriations carried forward from 2015 to 2016 (C8 appropriations of 2016) but finally not paid in 2016, was EUR 38 615.93.

2.1.4 Types of procurement procedures

In 2016, a total of 39 procurement procedures were launched, resulting in 52 contracts (20 framework contracts, 9 service contracts and 21 specific contracts awarded under Re-Opening of Competition) and 320 purchase orders (127 of which were issued under pre-existing framework contracts) were signed.

2.1.5 Interest charged by suppliers

During 2016, the Agency had to pay no interest to its suppliers as result of keeping the payment terms agreed with the suppliers.

2.2 MANAGEMENT OF HUMAN RESOURCES

2.2.1 Human resources

At the end of 2016, 69 statutory staff were employed in the Agency.

During 2016, 11 staff left the Agency, nine vacancy notices were published and 11 staff were recruited/took up new duties within the Agency. ENISA still experiences significant challenges in attracting and retaining suitably qualified staff to support the activities of the Agency. This is a challenge due to several factors, mainly the types of post that are being offered (CA posts) that are not financially competitive for the IT NIS job market, and moreover the low salary coefficient which contributes even more to a non-competitive package offer, especially for CA positions.

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 the staff. Several children of staff members in ENISA Heraklion attended the European School in Heraklion in 2016, which offers education at the following levels: nursery, primary and secondary education. ENISA has a service level agreement with DG Human Resources and Security for the provision of these services.

In 2016, ENISA adopted by analogy four implementing rules, namely: C (2015) 5320 on Unpaid Leave and Leave on personal ground, C (2015) 1509 on the Use and Employment of TA's 2(f), C (2015) 9650 on Reclassification of Temporary Agents and C (2015) 9561 on Reclassification of Contract Agents.

Additionally, in accordance with Article 110 of the SR, the Agency received the agreement of its Management Board to derogate from four implementing rules as sent by the European Commission: C (2016) 3828 on the implementation of the Learning and Development Strategy, C (2016) 3288 on Middle Management, C (2016) 3214 on the function of Advisor and C (2015) 9151 on the implementation of telework. The Agency is waiting for the Agencies' Models to be adopted in order to adopt them or to decide to draft its own rules (ex novo decision).

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

2.2.2 Results of screening

Following European Commission methodology, the Agency performed the 'job screening' benchmarking exercise for 2016. The result of the exercise, which is a snapshot of the staffing situation at end December 2016, appears in Annex A.4. It is relevant to mention that the 'Overhead', support functions, is only 20.24 % of the total statutory staff count, which is below the maximum value accepted for the Agencies that is estimated at 25 %. This is only possible due to very efficient resources 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 Internal Control Standard 8 (ICS 8 Processes and Procedures), the Agency has done the ex post control report for the financial year 2015. The recommendations issued on the report were addressed during the year.

The ex post controls of the financial year 2015 were quite extensive. A total of 267 financial transactions were sampled and controlled, representing 13.17 % of all financial transactions of the Agency and representing 76.43 % of the 2015 Agency's budget. As a result, one recommendation was issued which regards a delay of payments which did not generate any interest to be paid.

Moreover, the European Court of Auditors (ECA) is in charge of the annual audit of the Agency, which is concluded by the publication of an annual report according to the provisions of Article 287(1) of TFEU. For several consecutive years, the ECA reports have confirmed the improvement in the Agency's overall internal controls 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 Services (IAS)

The Agency has no open recommendations with the Internal Audit Service in 2016. In September, the IAS performed the Agency Risk assessment. The report shows the next three topics for auditing: Stakeholders involvement in the deliverables, Human Resources and IT. The Agency shall take immediate actions regarding the construction of a quality management system as well as in implementation of its risk management policy.

2.5.2 European Court of Auditors (ECA)

The annual report of ECA on the accounts of ENISA for 2015 does not contain recommendations.

2.5.3 Follow up of audits plans, audits and recommendations

The Agency will focus on the quality management system as well as on the implementation of the risk management policy.

2.6 FOLLOW UP OF OBSERVATIONS FROM THE DISCHARGE AUTHORITY

Regarding the European Parliament decision of 28 April 2016, the Executive Director of the Agency was granted a discharge in respect of the implementation of the Agency's budget for the financial year 2014.

Regarding the European Parliament decision of 28 April 2016, the closure of the accounts of the Agency for the financial year 2014 was approved.

2.6.1 Follow up of the 2013 discharge

The Agency did not have any comment made by the Court.

2.6.2 2014 discharge

2.6.2.1 Budget and financial management

The Discharge authority noted that budget monitoring efforts during the financial year 2014 resulted in a high budget implementation rate of 100 % and that the payment appropriations execution rate was 85.61 %.

2.6.2.2 Commitments and carryovers

The Discharge authority noted that, according to the Court's report, the total amount of committed appropriations carried over to 2015 amounted to EUR 1 332 421 (15 % of total appropriations). It took note of the fact that the carry-overs were EUR 612 981 (49 %) for Title II (administrative expenditure), representing a decrease of 10 % compared to 2013 and acknowledged the fact that those carry-overs related to investments in IT infrastructure ordered as planned near the year-end for the Agency's two offices.

The Discharge authority observed that an amount of EUR 717 927 was carried forward from the financial year 2013; notes that EUR 49 460 (6.89 %) of the 2013 carry-forwards were cancelled.

2.6.2.3 Transfers

The Discharge authority noted with satisfaction that, according to the Agency's Annual Report, as well as the Court's audit findings, the level and nature of transfers in 2014 remained within the limits of the financial rules.

2.6.2.4 Recruitment procedures

The Discharge authority noted that from the Agency's Annual Activity Report that, at the end of 2014, 62 statutory staff were employed; notes, furthermore, that during 2014, three staff left the Agency, 10 vacancy notices were published and seven staff were recruited.

The Discharge authority observed that the Agency experiences challenges in attracting and holding suitably qualified staff to support its activities, mainly due to the location of its office in Crete, where international education is a challenging factor. It acknowledged the fact that the Agency concluded a service level agreement with each of the private schools being used by the children of the staff in the Athens office, as no European schools are based there. The Discharge authority furthermore noted that a new mandate and service agreement was concluded between the Commission and the Agency which provides the detail of the funding for European schools used by the children of Agency staff.

The Discharge authority noted according to the Agency's Annual Activity Report, the Agency conducted a job-screening exercise using the common methodology adopted for the Agencies for the first time in 2014. The Discharge authority furthermore noted that, according to that exercise, 68 % of the Agency's staff were in the operational functions category, 22 % were in the administrative support and coordination category and 10 % were employed in relation to neutral functions.

2.6.2.5 Internal Audit

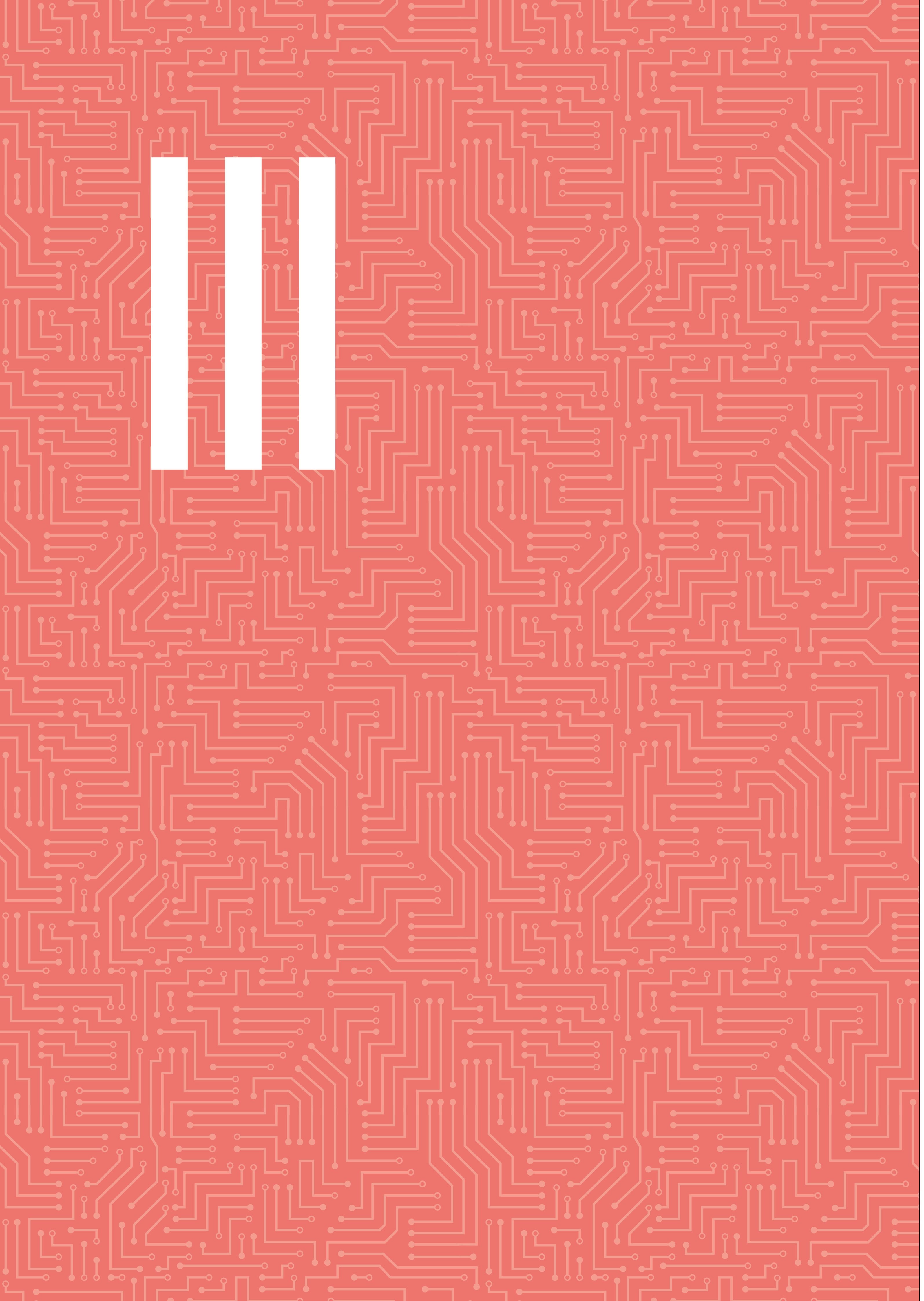
The Discharge authority took note of the fact that at the beginning of 2014, the Agency had 25 open recommendations from previous reports of the Commission's Internal Audit Service ('IAS'). It acknowledged the fact that 24 recommendations were closed during 2014 as confirmed by the IAS in its 'on-the-spot' visit to the Agency in November 2014. The Discharge authority noted that one remaining open recommendation was closed in 2015, after the tool for e-workflows had been implemented.

2.6.2.6 Other comments

The Discharge authority acknowledged the fact that the Agency adopted internal policies in order to improve cost-effectiveness and the environmental friendliness of its facilities. It noted that an important step towards satisfying both requirements was the adoption of a ‘paperless’ platform serving as workflow and storage of internal documents. It also noted with satisfaction that the Agency has practically eliminated all paper-based workflows, including financial transactions and human resources files and documents, and has replaced them with electronic documents and workflows in an effort to achieve a paperless office environment. The Discharge authority acknowledged the fact that this tool was successfully introduced in January 2015.

The Discharge authority stated that the annual reports of the Agency could play an important role in compliance regarding transparency, accountability and integrity and called on the Agency to include a standard chapter on those components in its annual report.

The Discharge authority acknowledged the fact that, as a follow up from the 2013 discharge of the Agency, according to the lease agreement between the Greek authorities, the Agency and the landlord, rent for the offices in Athens is paid by the Greek authorities. The authority is concerned about the constant late payment of rent, which continued in 2014 and 2015 and which presents significant reputational, financial and business-continuity risks for the Agency. Furthermore, it noted with concern that in 2015, the payment of the instalment for the first 6 months of the year was made on 27 August 2015 and only after the Agency received a warning that litigation would be launched by the landlord of the Athens office. The Discharge authority urges the Commission, the Agency and the Greek authorities to find a solution for this issue in order to reduce significantly the risks to which the Agency is exposed.



PART III

ASSESSMENT OF THE EFFECTIVENESS OF THE INTERNAL CONTROL SYSTEMS

3.1 RISK MANAGEMENT

The Agency was using the risk assessment done by the Internal Audit Service in 2012. In September 2016, the Internal Audit Service produced the new risk assessment of the Agency.

Regarding the specific whistleblowing policy, the latter was submitted to the European Data Protection Supervisor for comments.

3.2 COMPLIANCE AND EFFECTIVENESS OF INTERNAL CONTROL STANDARDS

ENISA has adopted a set of internal control standards, 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 the organisational structure and the 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 internal control standards 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, as well as on the recommendations raised by the auditing bodies (ECA and IAS). During 2015, the Agency achieved compliance with the internal control standards listed below.

3.2.1 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 2016. The roles and tasks of each department and unit are clearly defined.

3.2.2 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.

3.2.3 Staff allocation and mobility (ICS 3)

Whenever necessary, management aligns organisational structures and staff allocations with priorities and workload.

3.2.4 Staff evaluation and development (ICS 4)

In the context of the Career Development Report (CDR) process, discussions are held individually with all staff to establish their annual objectives. Staff performance is evaluated according to standards set by the Agency. An annual training plan is developed at Agency level based on needs deriving from the policy of the Agency. As part of the CDR process, every year each staff member completes an individual training plan. Management ensures that at a minimum every staff member attends the compulsory training courses defined in the annual training plan.

3.2.5 Objectives and performance indicators (ICS 5)

The Work Programme (WP) for 2017, part of the Programming document (PD) 2017-2019, of the Agency was developed by the Agency services, with continuous input and guidance from its two governing bodies, the Management Board and the Permanent Stakeholders Group. The PD 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 PD objectives are established on SMART (Specific, Measureable, Achievable, Relevant, Time-bound) criteria and 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 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 (KPIs) that are applied to all areas of activity. KPIs 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 KPIs, including self-assessments that have been carried out in the form of progress reports and follow-up actions that seek to re-align 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 managed again to optimise the budget execution for five consecutive years. The commitment rate of budget appropriations available for the year 2016 (C1) reached 99 %.

3.2.6 Risk management process (ICS 6)

The Agency did not have any open recommendation for 2016. The IAS performed a risk assessment of the Agency in September 2016. The report shows the three next topics for auditing: Stakeholders involvement in the deliverables, Human Resources and IT. The Agency shall take immediate actions regarding the construction of a Quality Management System as well as in implementation of its Risk Management policy.

3.2.7 Operational structure (ICS 7)

Delegation of authority is clearly defined, assigned and communicated by means of the Executive Director's Decisions (EDD). 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) as well as the individual delegation EDD.

The Agency's sensitive functions are clearly defined, recorded and kept up to date. The Agency records derogations granted to allow staff to remain in sensitive functions beyond 5 years along with documentation of the risk analysis and the controls for mitigation.

As regards sensitive functions, due care has been taken in order 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.

3.2.8 Processes and procedures (ICS 8)

Several policies were developed to strengthen the processes and procedures internal control standard. The Agency created a policy on financial circuits. The roles and responsibilities of financial actors are described in this policy as well as existing workflows (see comment on '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 2016 with the full 2015 ex post control exercise, and, it will deliver the 2016 ex post control report in the first semester of 2017.

Importantly in 2016, a quality management system was introduced, strengthening the performance management of the Agency.

3.2.9 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 monthly 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 units 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 PD 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.

3.2.10 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 BCP's Agency identified the functions, services and infrastructure that need to be restored within certain time limits and the resources necessary for this purpose. Electronic and hardcopy versions of both BCPs are stored in secure and easily accessible locations, which are known to relevant staff.

3.2.11 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 level RESTREINT UE/EU RESTRICTED, an administrative arrangement between the Security Directorate of the European Commission and the Agency was signed on 27 May 2011.

Management at all levels supervises the activities for which they are responsible and tracks the main issues identified.

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, ENISA adopted in January 2015 a SharePoint-based application, 'Paperless', which routes documents to staff involved in 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 of workflow actors. Approved workflows are permanently stored and an appropriate audit trail is produced.

3.2.12 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 sub-systems, and 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 platform of communication between all departments. Every week, staff members can share their work with the rest of the Agency.

3.2.13 Accounting and financial reporting (ICS 13)

All finance and accounting procedures are documented in the Internal Control Manual of the Agency. 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.

3.2.14 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.

3.2.15 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.

> **All finance and accounting procedures are documented in the Internal Control Manual of the Agency.**

3.2.16 Internal audit capability (ICS 16)

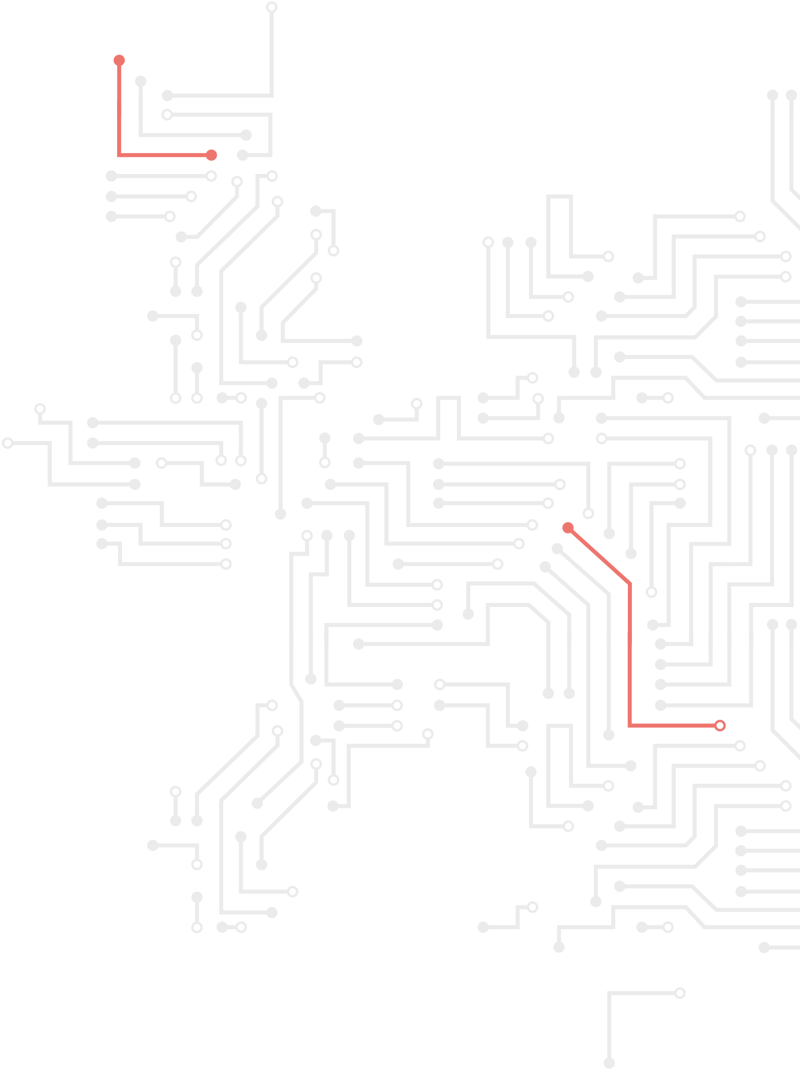
The Head of the Stakeholders Relations and Administration Department assumes the Internal Control Coordination (ICC) function. He is responsible for implementing internal control systems in the Agency and liaising with the IAS of the European Commission. As the Agency lacks human resources, the role of Internal Audit Capability (IAC) 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.

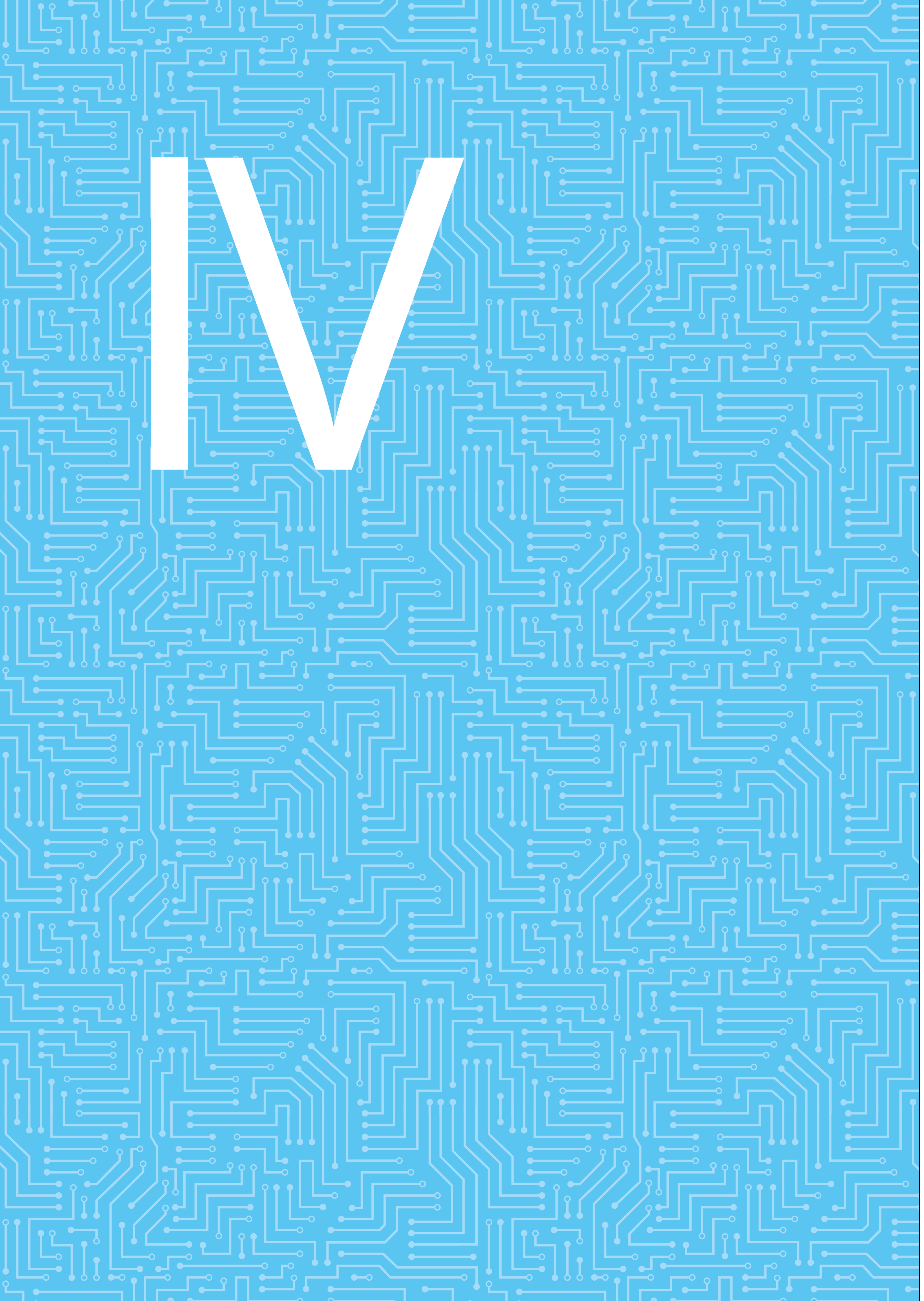
Internal Control tasks performed in ENISA include 100 % of ex ante verifications, annual ex post controls, hierarchical controls and outsourced engagements, coordinated by the ICC. The role of ICC was reinforced in order to comply with all the recommendations issued by the IAS and ECA.

Concerning the overall state of the internal control system, generally the Agency complies with the three assessment criteria for effectiveness:

- staff that have the required knowledge and skills;
- systems and procedures designed and implemented to manage the key risks effectively; and
- 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.





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', as well as a structure for the assessment, reporting and monitoring of risk. The risk framework defines the categories, sub-categories and business risks applicable at the organisational level, for ENISA as a whole. It includes:

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

Assessment by management:
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 the SPD in terms of operational and administrative activities;
- Contractors that support operational activities and other support activities that cannot be in-sourced 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 co-organisation of events. Alternatively, in the case of working group members, they may be chosen by means of a selection procedure.

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

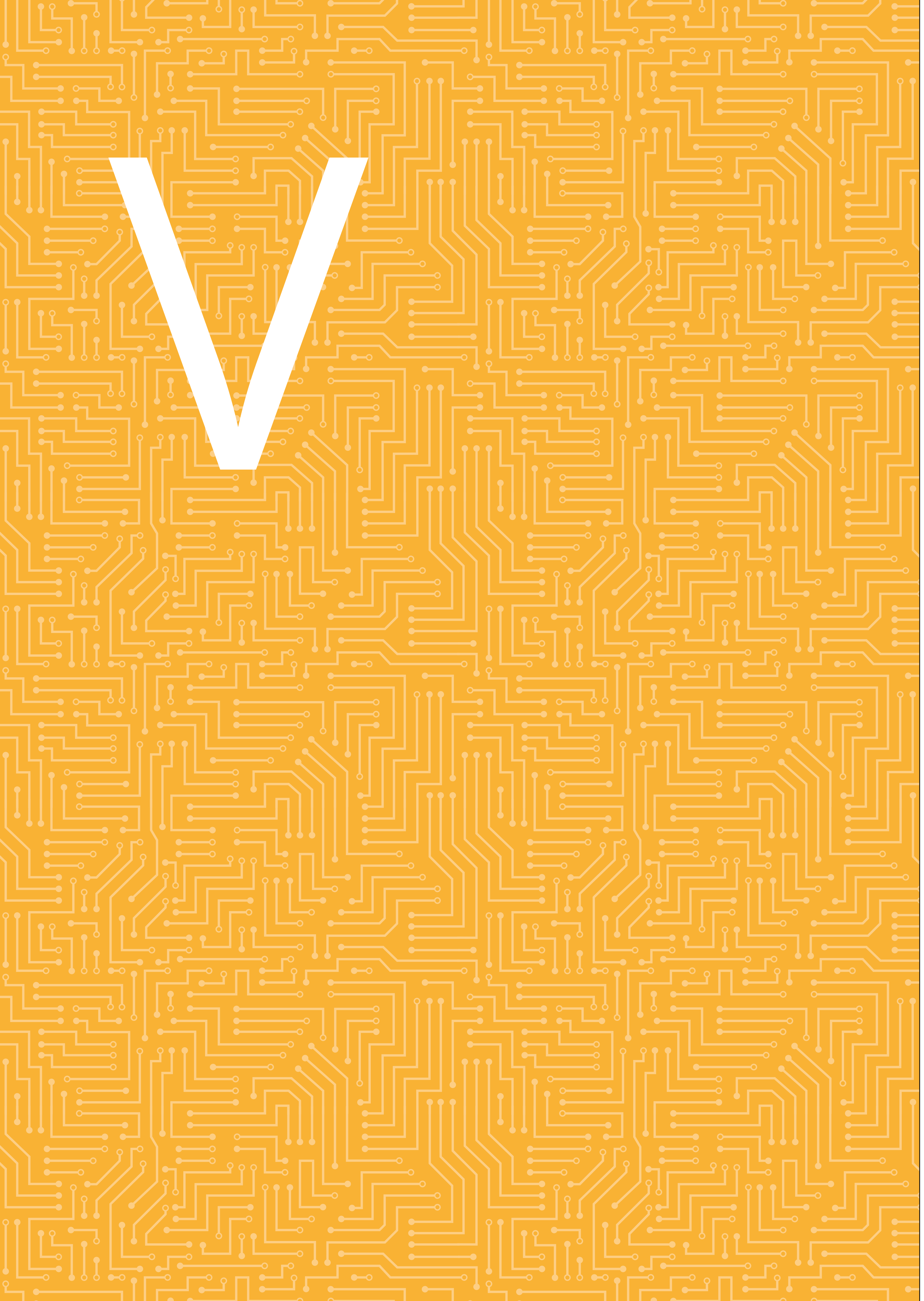
4.2 EXCEPTIONS

In 2016, the Agency recorded 18 exceptions. Only one is with high materiality (> 60 000). This case is related to an a posteriori commitment. A human error on a handover provided by a previous staff member created a delay in concluding the budgetary commitment.

The information reported in Parts 2 and 3 stems from the results of auditing by management and auditors. The results are contained in the reports listed. 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.

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

	Systemic process	Activity	Performance indicator
1	Follow up on auditor's comments and recommendations regarding ADM practices and procedures as they are implemented in line with financial regulation (FR), implementing rules (IR) and the Staff Regulations (SR).	Update of documents and activities 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 tree opened, appropriations posted properly.	Annual budget lines open and running by the end of the year with the anticipated budget, economic outturn 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 procedural, operational and financial level.	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.



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 which could harm the interests of the Agency.

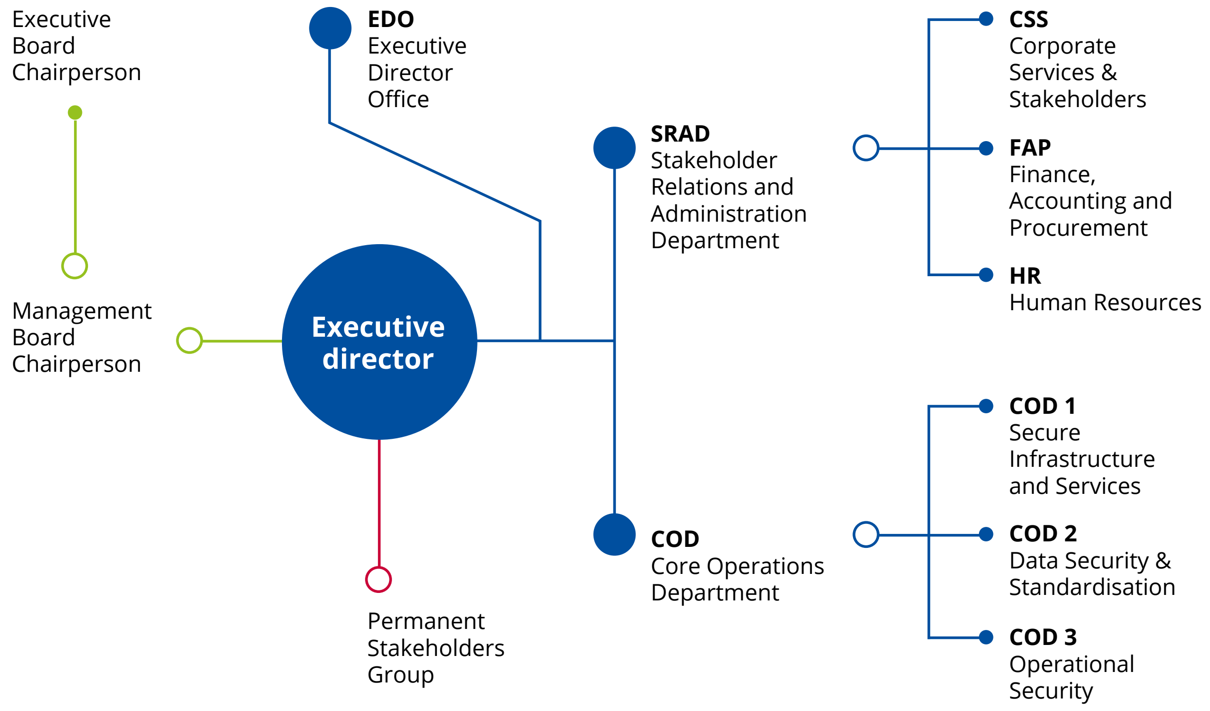
Heraklion, June 2017.

Udo Helmbrecht
Executive Director

A

ANNEX 1
HUMAN RESOURCES

A 1.1 ORGANISATIONAL CHART


Executive Board Chairperson
Management Board Chairperson
EDO
Executive Director Office
Executive director
Permanent Stakeholders Group
SRAD
Stakeholder Relations and Administration Department
COD
Core Operations Department
CSS
Corporate Services & Stakeholders
FAP
Finance, Accounting and Procurement
HR
Human Resources
COD 1
Secure Infrastructure and Services
COD 2
Data Security & Standardisation
COD 3
Operational Security

A 1.2 ESTABLISHMENT PLAN 2016

FUNCTION GROUP AND GRADE (TA/AST)	POSTS 2016: 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		9
AD 8		9
AD 7		7
AD 6		
AD 5		
AD Total:		**34**
AST 11		
AST 10		
AST 9		
AST 8		
AST 7		
AST 6		3
AST 5		5
AST 4		1
AST 3		3
AST 2		2
AST 1		
AST Total:		**14**
Grand Total:		**48**
Total Staff:		**48**

A 1.3 INFORMATION ON ENTRY LEVEL FOR EACH TYPE OF POST

NR	JOB TITLE	TYPE OF CONTRACT (OFFICIAL, TA OR CA)	ENTRY LEVEL	INDICATION OF FUNCTION DEDICATED TO ADMINISTRATIVE, SUPPORT OR OPERATIONS
1	Executive Director	TA	AD 14	TOP OPERATIONS
2	Head of Stakeholders Relations and Administration Department	TA	AD 11	ADMINISTRATIVE
3	Head of Core Operations Department	TA	AD 11	TOP OPERATIONS
4	Head of Data Security and Standardisation	TA	AD 11	TOP OPERATIONS
5	NIS Adviser	TA	AD 10	OPERATIONS
6	Head of Operational Security	TA	AD 9	TOP OPERATIONS
7	Head of Finance and Procurement (FAP) —	TA	AD 9	NEUTRAL
8	Head of Secure Infrastructure and Services	TA	AD 8	TOP OPERATIONS
9	Head of Human Resources	TA	AD 8	ADMINISTRATIVE
10	Head of Corporate Services and Stakeholders Relations	TA	AD 8	ADMINISTRATIVE
11	Head of EDO/Policy Adviser and 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 Security Tools and Architecture	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

NR	JOB TITLE	TYPE OF CONTRACT (OFFICIAL, TA OR CA)	ENTRY LEVEL	INDICATION OF FUNCTION DEDICATED TO ADMINISTRATIVE, SUPPORT OR OPERATIONS
33	Administrative Officer to the Management Board	TA	AD 5	OPERATIONS
34	IT Team Leader	TA	AST 5	ADMINISTRATIVE
35	Verification, Payments and Missions Team Leader	TA	AST 4	NEUTRAL
36	Safety, Security and Facilities Management Team Leader	TA	AST 4	ADMINISTRATIVE
37	Procurement Officer and Team Leader	TA	AST 4	NEUTRAL
38	Administrative Assistant	TA	AST 3	OPERATIONS
39	HR Assistant	TA	AST 3	ADMINISTRATIVE
40	IT and Facilities Support Assistant	TA	AST 3	ADMINISTRATIVE
41	Stakeholders Communication 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 Core Operations Department	TA	AST 1	OPERATIONS
48	Budget Team Leader	TA	AST 1	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	Communications 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 (Quality and Control)	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
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	SNE	SNE	OPERATIONS
78	Expert in Network and Information Security	SNE	SNE	OPERATIONS
79	Officer in Network and Information Security	SNE	SNE	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 1.4 INFORMATION ON BENCHMARKING EXERCISE

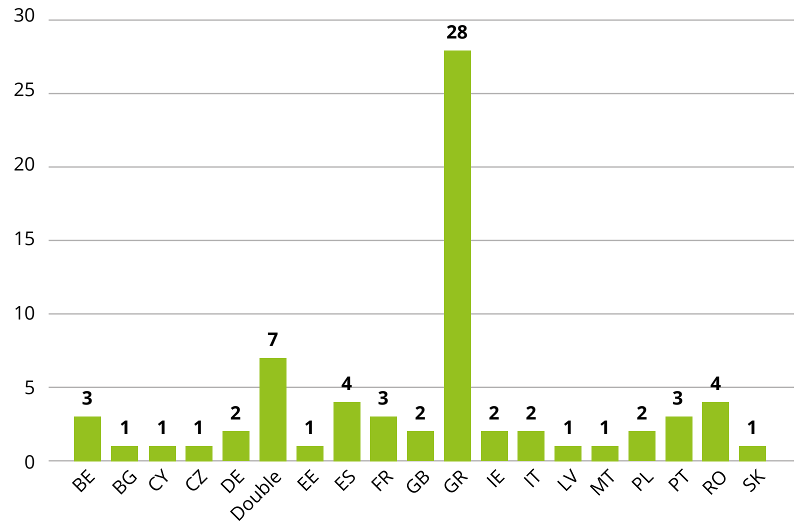
Job Type	2016	2015
Total Administrative support and Coordination	19.04 %	20.22 %
Administrative support	15.47 %	16.85 %
Coordination	3.57 %	3.37 %
Total Operational	66.66 %	66.29 %
Top operational coordination	7.14 %	8.99 %
General Operational	59.52 %	57.30 %
Total Neutral	14.29 %	13.48 %
Finance and Control	14.29 %	13.48 %

The benchmarking exercise followed the EU Commission methodology. All the values are within the acceptable values for an Agency of ENISA size (i.e. Overhead (Administrative support and Coordination) is below 25 %).

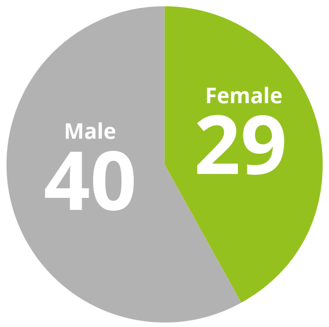
A 1.5 HUMAN RESOURCES STATISTICS

As of 31.12.2016, ENISA counts 69 staff members: 43 TAs (28 ADs and 15 ASTs), 25 CAs and 1 SNE.

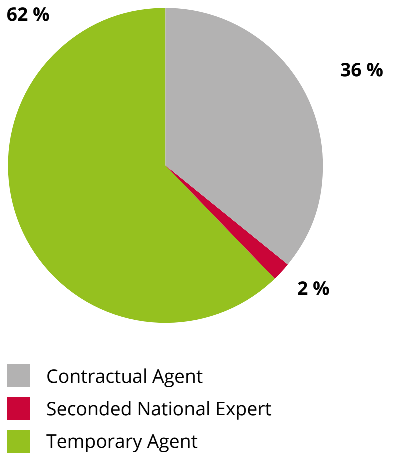
Staff members by Nationality



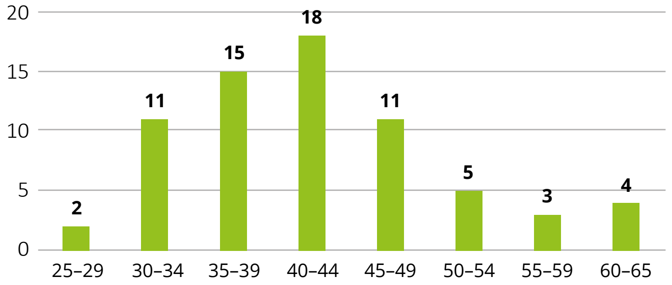
Gender Balance



Staff members by Category



Age Analysis



A 1.6 HUMAN RESOURCES BY ACTIVITY

Core operational activities (Strategic objectives 1 to 4)	Operational activities — FTEs
SO1. To develop and maintain a high level of expertise of EU actors, taking into account evolutions in network and information security	**9.5**
WPK1.1. Improving the expertise related to critical information infrastructures	4.1
WPK1.2. Network and information security threats landscape analysis	2.6
WPK1.3. Research and development, innovation	2.8
SO2. To assist the Member States and the European Union institutions and bodies in enhancing capacity building throughout the European Union	**14.4**
WPK2.1. Assist Member States' capacity building	8.0
WPK2.2. Support European Union institutions' capacity building	2.6
WPK2.3. Assist private sector capacity building	1.1
WPK2.4. Assist in improving the general awareness	2.7
SO3. To assist the Member States and the European Union institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security	**25.7**
WPK3.1. Supporting European Union policy development	8.1
WPK3.2. Supporting European Union policy implementation	17.6
SO4. To enhance cooperation both between the Member States of the European Union and between related network and information security communities	**11.6**
WPK4.1. Cyber crisis cooperation and exercises	6.6
WPK4.2. Network and information security community building	5.0

Horizontal activities supporting core operations stakeholders relations, corporate communication, project support activities	Operational Activities — FTEs
HA. Horizontal activities supporting core operations	**14.5**
HA1. Management board, executive board and permanent stakeholders group secretariat	1.3
HA2. National liaison officer network	0.7
HA3. European Union relations	1.3
HA4. Spokesperson, stakeholders communication and dissemination activities	2.6
HA5. Quality control and project office	7.2
HA6. Article 14 requests	0.7
HA7. Data protection officer	0.7

Operational activities	Operational Activities — FTEs
Total operational activities	75.6

Administration and support activities	Operational activities — FTEs
ASA. Administration and support activities	8.4
ASA0. Executive director's office and general management	1.1
ASA1. Quality management systems, ICC, security, facilities management, internal communications	1.6
ASA2. Finance, accounting and procurement	2.5
ASA3. Human resources	1.3
ASA4. Information and communications technology	1.9

HUMAN RESOURCES TOTAL	84.0

Remark: The figures in the table above provide an estimation of the human resources attributed in each of the operational activities of the Agency, according to the Work Programme 2016.

ANNEX 2
FINANCIAL RESOURCES

A 2.1 PROVISIONAL ANNUAL ACCOUNTS 2016

Balance Sheet 2016 (in EUR)	2016	2015
NON-CURRENT ASSETS	**891 267**	**878 678**
Intangible Assets	864	1 409
Property, plant and equipment	890 403	877 269
CURRENT ASSETS	**1 470 630**	**1 065 148**
Short-term Receivables	245 857	280 069
Cash and Cash Equivalents	1 224 773	785 079
ASSETS	2 361 897	1 943 826
NON-CURRENT LIABILITIES	**-**	**-**
Provisions (long term)	-	-
CURRENT LIABILITIES	**670 842**	**686 251**
EC Pre-financing received	38 436	80 397
EC Interest payable	-	-
Accounts Payable	232 730	289 761
Accrued Liabilities	399 676	316 093
Short-term provisions	-	-
LIABILITIES	670 842	686 251
NET ASSETS (ASSETS less LIABILITIES)	1 691 055	1 257 575

Statement of Financial Performance 2016 (in EUR)	2016	2015
OPERATING REVENUES	**10 995 538**	**10 062 303**
Revenue from the European Union Subsidy	10 359 496	9 345 552
Other revenue	913	83 089
Revenue from Administrative operations	635 129	633 662
OPERATING EXPENSES	**– 10 560 858**	**– 10 243 489**
Administrative Expenses	– 8 260 628	– 8 062 292
Operational Expenses	– 2 300 230	– 2 181 197
Adjustments to provisions	-	-
OTHER EXPENSES	**– 1 200**	**– 1 487**
Financial Expenses	– 1 020	– 1 118
Exchange rate loss	– 180	– 369
ECONOMIC RESULT FOR THE YEAR	433 480	– 182 673

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 European Court of Auditors. It is thus possible that amounts included in these tables may have to be adjusted before the final accounts are adopted (deadline 1 July 2017).

A 2.2 FINANCIAL REPORTS 2016

OUTTURN ON COMMITMENT APPROPRIATIONS IN 2016

Chapter		Commitment appropriations authorised *	Commitments made	%
		1	2	3=2/1
Title A-1 STAFF				
A-11	Staff in Active Employment	4 587 793.92	4 587 793.92	100.00 %
A-12	Recruitment Expenditure	167 568.39	167 568.39	100.00 %
A-13	Socio-medical Services and Training	118 052.08	118 052.08	100.00 %
A-14	Temporary Assistance	1 138 588.18	1 138 588.18	100.00 %
Total Title A-1		**6 012 002.57**	**6 012 002.57**	**100.00 %**
Title A-2 FUNCTIONING OF THE AGENCY				
A-20	Buildings and Associated Costs	1 100 888.59	941 888.59	85.56 %
A-21	Movable Property and Associated Costs	81 448.62	81 448.62	100.00 %
A-22	Current Administrative Expenditure	63 426.29	63 426.29	100.00 %
A-23	Information and Communication Technologies	670 523,61	670 523.61	100.00 %
Total Title A-2		**1 916 287.11**	**1 757 287.11**	**91.70 %**
Title B-3 OPERATING EXPENDITURE				
B-30	Group Activities	776 561.59	776 561.59	100.00 %
B-32	Horizontal Operational Activities	438 459.11	438 459,11	100.00 %
B-36	Core Operational Activities	1 841 536.68	1 841 536.68	100.00 %
Total Title B-3		**3 056 557.58**	**3 056 557.58**	**100.00 %**
TOTAL ENISA		**10 984 847.26**	**10 825 847.26**	**98.55 %**

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

OUTTURN ON PAYMENT APPROPRIATIONS IN 2016

Chapter		Payment appropriations authorised *	Payments made	%
		1	2	3=2/1
Title A-1 STAFF				
A-11	Staff in Active Employment	4 587 793.92	4 587 793.92	100.00 %
A-12	Recruitment Expenditure	179 947.04	175 040.37	97.27 %
A-13	Socio-medical Services and Training	200 505.27	162 034.26	80.81 %
A-14	Temporary Assistance	1 379 744.49	1 018 436,22	73.81 %
Total Title A-1		**6 347 990.72**	**5 943 304.77**	**93.62 %**
Title A-2 FUNCTIONING OF THE AGENCY				
A-20	Buildings and Associated Costs	1 183 851.91	986 753.26	83.35 %
A-21	Movable Property and Associated Costs	82 369.54	37 269.72	45.25 %
A-22	Current Administrative Expenditure	67 489.66	64 421.79	95.45 %
A-23	Information and Communication Technologies	763 613.92	547 433.58	71.69 %
Total Title A-2		**2 097 325.03**	**1 635 878.35**	**78.00 %**
Title B-3 OPERATING EXPENDITURE				
B-30	Group Activities	828 452.75	734 087.29	88.61%
B-32	Horizontal Operational Activities	500 836.64	383 167.42	76.51 %
B-36	Core Operational Activities	1 884 762.66	1 797 115.72	95.35 %
Total Title B-3		**3 214 052.05**	**2 914 370.43**	**90.68 %**
TOTAL ENISA		**11 659 367.80**	**10 493 553.55**	**90.00 %**

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

BREAKDOWN OF COMMITMENTS TO BE SETTLED ON 31.12.2016

Chapter		2016 Commitments to be settled			
		Commitments 2016	Payments 2016	RAL 2016	% to be settled
		1	2	3=1-2	4=1-2/1
Title A-1 STAFF					
A-11	Staff in Active Employment	4 587 793.92	– 4 587 793.92	0.00	0.00 %
A-12	Recruitment Expenditure	167 568.39	– 162 883.05	4 685.34	2.80 %
A-13	Socio-medical Services and Training	118 052.08	– 83 931.89	34 120.19	28.90 %
A-14	Temporary Assistance	1 138 588.18	– 796 783.54	341 804.64	30.02 %
Total Title A-1		**6 012 002.57**	**– 5 631 392.40**	**380 610.17**	**6.33 %**
Title A-2 FUNCTIONING OF THE AGENCY					
A-20	Buildings and Associated Costs	941 888.59	– 904 038.99	37 849.60	4.02 %
A-21	Movable Property and Associated Costs	81 448.62	– 36 496.73	44 951.89	55.19 %
A-22	Current Administrative Expenditure	63 426.29	– 61 112.85	2 313.44	3.65 %
A-23	Information and Communication Technologies	670 523.61	– 455 620.16	214 903.45	32.05 %
Total Title A-2		**1 757 287.11**	**– 1 457 268.73**	**300 018.38**	**17.07 %**
Title B-3 OPERATING EXPENDITURE					
B-30	Group Activities	776 561.59	– 689 580.69	86 980.90	11.20 %
B-32	Horizontal Operational Activities	438 459.11	– 320 939.36	117 519.75	26.80 %
B-36	Core Operational Activities	1 841 536.88	– 1 758 467.76	83 069.12	4.51 %
Total Title B-3		**3 056 557.58**	**– 2 768 987.81**	**287 569.77**	**9.41 %**
TOTAL ENISA		**10 825 847.26**	**– 9 857 648.94**	**968 198.32**	**8.94 %**

* 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 as well as miscellaneous payment appropriations for the period (e.g. internal and external assigned revenue).

SITUATION ON REVENUE AND INCOME IN 2016

Title	Description	Year of Origin	Revenue and Income recognised	Revenue and Income cashed in 2016	Outstanding Balance
9000	SUBSIDY FROM THE EU GENERAL BUDGET	2016	10 397 932.00	10 397 932.00	0.00
9200	Subsidy from the Ministry of Transports of Greece	2016	616 378.68	565 013.79	51 364.89
9300	REVENUE FROM ADMINISTRATIVE OPERATIONS	2016	19 663.48	19 663.48	0.00
TOTAL ENISA			**11 033 974.16**	**10 982 609.27**	**51 364.89**

AVERAGE PAYMENT TIME FOR 2016

Average Payment Time for 2016	Total number of payments	Within Time Limit	Percentage	Average Payment Time	Late Payment	Percentage	Average Payment Time
18.39	2 021	1 719	85.06 %	12.96	302	14.94 %	49.32

ANNEX 3
OTHER ANNEXES

A 3.1 LIST OF ACRONYMS

APF: Annual Privacy Forum

cPPP: Cyber Security Public–Private Partnership

CE2016: Cyber Europe 2016

CERT-EU: Computer Emergency Response Team for the EU Institutions, Bodies and Agencies

CEN: European Committee for Standardisation

Cenelec: European Committee for Electrotechnical Standardisation

CIIP: critical information infrastructure protection

CSCG: ETSI CEN-Cenelec Cyber Security Coordination Group

CSIRT: computer security incidents response teams

COD: core operational department

COM: European Commission

CSS: cyber security strategy

DG: EU directorate-general

DG CNECT: EC Directorate-General CNECT

DPA: data protection authorities

DPO: Data Protection Officer

DSM: Digital Single Market

EB: ENISA Executive Board

EC3: European Cybercrime Centre, Europol

ECA: European Court of Auditors

ECSC: European Cyber Security Challenge

ECSM: European Cyber Security Month

ED: Executive Director

EDO: Executive Directors Office

EDPS: European Data Protection Supervisor

eID: electronic Identity

eIDAS: Regulation on electronic identification and trusted services for electronic transactions in the internal market

ENISA: European Union Agency for Network and Information Security

ETSI: European Telecommunications Standards Institute

EU: European Union

FAP: finance, accounting and procurement

FIRST: Forum of Incident Response and Security Teams

FM: facilities management

FTE: full-time equivalents

HoD: Head of Department

HR: human resources

IAS: Internal Audit Service

ICC and IAC: Internal Control Coordination and Internal Audit Capability

ICS: internal control standards

ICT: information and communication technologies

IS: information systems

ISP: internet service providers

IXP: internet exchange point

KPI: key performance indicator

LEA: law enforcement agency

M2M: machine to machine

MB: Management Board

MS: Member State

NCSS: National Cyber Security Strategies

NIS: network and information security

NISD: NIS directive

NLO: national liaison officer

NRA: national regulatory authority

O: output

OES: operators of essential services

P: publication, type of output covering papers, reports, studies

PDCA: plan-do- check-act

PETs: privacy enhancing technologies

PPP: public–private partnership

PSG: permanent stakeholders group

Q: quarter

QMS: quality management system

SB: supervisory body

SCADA: supervisory control and data acquisition

SDO: standard developing organisation

SME: small and medium-sized enterprise

SO: strategic objectives

SOP: standard operating procedure

SRAD: Stakeholder Relations and Administration Department

TF-CSIRT: Task Force of Computer Security Incidents Response Teams

TRANSITS: Computer Security and Incident Response Team (CSIRT) personnel trainings

TSP: trust service provider

WP: Work Programme

A 3.2 LIST OF POLICY REFERENCES

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

Reference	Policy/legislation reference. Complete title and link
2016	
Work Programme 2016	Work Programme 2016 with amendments, Consolidated version. Version adopted by the MB on 15.03.2016, available at: https://www.enisa.europa.eu/publications/corporate/amending-work-programme-2016
The 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: ELI: http://data.europa.eu/eli/dir/2016/1148/oj
COM communication 0410/2016 on 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/2016/0410 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0410
COM decision C(2016)4400 on cPPP	COMMISSION DECISION of 5.7.2016 on the signing of a contractual arrangement on a public–private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation, Brussels, 5.7.2016, 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/2016/018 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) (Text with EEA relevance), 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: ELI: http://data.europa.eu/eli/dir/2016/681/oj
2015	
Digital Single Market Strategy for Europe (DSM)	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/2015/0192 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 (Text with EEA relevance), OJ L 337, 23.12.2015, pp. 35-127, available at: http://data.europa.eu/eli/dir/2015/2366/oj
The 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/2015/0185 final, available at:http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2015:0185:FIN

Reference	Policy/legislation reference. Complete title and link
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	Towards a thriving data-driven economy, COM(2014) 442 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the regions, July, 2014, 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
COM Regulation 611/2013 on the measures applicable to the notification of personal data breaches	Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, OJ L 173, 26.6.2013, pp. 2-8, available at: http://data.europa.eu/eli/reg/2013/611/oj
2012	
Action Plan for an innovative and competitive Security Industry	Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee regarding an Action Plan for an innovative and competitive Security Industry, COM(2012) 417 final
European cloud computing strategy	The Communication COM(2012)529 'Unleashing the potential of cloud computing in Europe', adopted on 27 September 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF
EP 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:
COM Communication on CIIP	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', Brussels, 31.3.2011, 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, Version consolidated, after amendments, available here: http://data.europa.eu/eli/reg/2011/1077/2015-07-20
Single Market Act	Single Market Act — Twelve levers to boost growth and strengthen confidence 'Working Together To Create New Growth', COM(2011)206 Final
Telecom Ministerial Conference on CIIP	Telecom Ministerial Conference on CIIP organised by the Presidency in Balatonfüred, Hungary, 14 15 April 2011
2010	
Internal Security Strategy for the European Union	An internal security strategy for the European Union (6870/10), http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/113055.pdf
Digital Agenda	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe, COM/2010/0245 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010DC0245&from=EN
2009	
COM 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/2009/0278 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
ePrivacy 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), Official Journal L 201 , 31/07/2002 P. 0037-0047, Consolidated version, after amendments, available at: http://data.europa.eu/eli/dir/2002/58/2009-12-19

NOTES

TP-AB-17-001-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 EU, its Member States, the private sector and Europe's citizens. 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 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

ISBN: 978-92-9204-220-2
ISSN: 2314-9434
DOI: 10.2824/558297

enisa.europa.eu