ANNUAL ACTIVITY REPORT

The EU Cyber Security Agency

ENISA.EUROPA.EU

2015

CONTACT

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

Catalogue number: TP-AB-16-001-EN-N
ISBN: 978-92-9204-167-0
ISSN: 2314-9434
DOI: 10.2824/698162

ANNUAL ACTIVITY REPORT

2015

European Union Agency for Network and Information Security

Decision No MB/2016/7 of the Management Board of the European Union Agency for Network and Information Security (ENISA)

THE ASSESSMENT OF THE CONSOLIDATED ANNUAL ACTIVITY REPORT FOR THE YEAR 2015 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 2015 Annual Activity Report produced by the Executive Director of ENISA in his quality of Authorising Officer for the implementation of the annual budget on 13 June 2016.

After the Executive Board scrutinized the draft assessment of the Management Board, here follows the assessment by the Management Board of the consolidated annual activity report (hereafter AAR):

- Section 1 of the report presents key results in the implementation of the ENISA Work programme 2015 and leads to conclusion that The Agency completed all deliverables agreed with the Management Board both within time and within budget. 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 2015. Overall, the report is in line with the ENISA Work Programme 2015 in this regard.

- Section 2 describes ENISA's management of resources. This section reports on 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 23,35% of the total statuary staff count, which is below the maximum value (25%) accepted for the Agencies.

- This sections also provides a follow up of the 2012 Discharge, and control results. The Agency has set up internal control processes to ensure the management of risks. The Agency has followed up on recommendations of Internal Audit Service as well as of the Court of Auditors. In 2015 no new recommendations were issued. This section also notes the main categories of deviation that led to exceptions reported in the Register of Exceptions.

- The annexes complete the report 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, performance information included in evaluations, a list of ENISA Management Board Representatives and Alternates, the Permanent Stakeholders' Group 2015-2017, as well as the annual accounts.

- The Management Board takes note of the achievements of ENISA in 2015. It notes the fact that the Work Programme tasks were completed on time and within budget and that the Agency continued to follow the recommendations emanating from audits carried out by the Court of Auditors and the Internal Audit Services.

- A coherent link is provided between activities planned in the Work Programme 2015 and the actual achievements reached in the reporting period.

Done by written procedure on 27 June 2016.

Mr Jörgen Samuelsson
The Chair of the Management Board of ENISA

TABLE OF CONTENTS

A MESSAGE FROM THE EXECUTIVE DIRECTOR

OVERVIEW

I would like to hereby let the readers of this report know that 2015 was yet another successful year for the Agency, with ENISA maintaining its track record of delivering according to plan and within its allocated budget. At the same time, we improved the positioning of services towards our major stakeholders while ensuring compliance with the regulatory framework.

EXTERNAL IMPACT

Broadly speaking, ENISA's activities can be divided across three main areas:

- recommendations to its stakeholders;
- support for policy development and implementation;
- 'hands on' work with operational communities.

Throughout 2015, ENISA strengthened its contribution in each of these areas, supporting Member States and private sector actors in responding to a rapidly developing threat environment and helping to lay solid foundations for the information systems of the future. ENISA activities are carried on in close collaboration with its stakeholders and during 2015 a number of high profile events have been organised or co-organised by ENISA such as: EU Cyber Security Month (ECSM) campaign, Annual Privacy Forum (APF), High Level Event (HLE), Industry Event, etc. At the same time the pan-European exercises scheduled for 2016 have been prepared in 2015.

As far as the 2015 annual Work Programme is concerned, the Agency successfully produced a total of 53 deliverables on a wide variety of subjects ranging from national issues such as the protection of critical infrastructure to issues affecting individual citizens such as privacy and Data Protection.

This year's highlights include best practices and recommendations in sectors such as eHealth, Finance and Smart Infrastructure and Services.

The work carried out in the area of Article 13a of the Telecommunications Framework Directive of 2009 continues to be the best known example of where ENISA is working to support policy initiatives, but it is important to mention that during 2015 the Agency has continued a number of other well known activities such as CSIRT Training and preparations for Cyber Exercises.

Article 14 requests, which are essentially a mechanism that allow Member States and EU institutions to request specific items of work from the Agency outside the work programme execution process, continue to be popular. ENISA received 23 new requests in 2015, which represents an increase of 92 % over the previous year, and continued to work on 19 ongoing requests.

All the activities carried out in 2015 resulted in various best practices and recommendations, available on the ENISA website for the benefit of stakeholders and citizens.

INTERNAL IMPROVEMENTS

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.

During 2015 the Agency has introduced a new system that supports a fully electronic workflow. This new 'Paperless' system responds to the compliance requirements of our regulations and has satisfied our internal and external stakeholders. 'Paperless' was a great opportunity to start a full revision of work methods and risk assessment in our business. This improvement also contributed to the objective of being a green organisation, where paper use has been significantly reduced.

A formalisation of a Quality Management system is foreseen for 2016 with the objective to consolidate the excellent compliance and good performance of the Agency. Our people are considered to be the best asset of ENISA, and having this in mind the Agency will continue to promote the value of the people that contribute to the success of our work.

CONCLUSIONS

The year 2015 has been another very successful year for the Agency. It has been a year in which we have strengthened our relations with our stakeholders and assisted them in making significant improvements to the state of cybersecurity throughout the EU. In parallel, we continue to make internal improvements that keep staff morale high and make the Agency a challenging and pleasant place to work.

I would like to end by thanking both our stakeholders and staff for their contributions to this success.

Udo Helmbrecht
Executive Director, ENISA

LIST OF ABBREVIATIONS

AAR: Annual Activity Report
APF: Annual Privacy Forum
CDR: Career Development Report
CEP: Cyber Exercises Platform
CERT: Computer Emergency Response Team
CEN: European Committee for Standardization
CENELEC: European Committee for Electrotechnical Standardization
CII: Critical Information Infrastructures
CIIP: Critical Information Infrastructure Protection
CISO: Chief Information Security Officer
CSCG: ETSI CEN-CENELEC Cyber Security Coordination Group
CSIRT: Computer Security Incidents Response Teams
COD: Core Operational Department
CSS: Cyber Security Strategy
D: Deliverable
DG: EC Directorate-General
DG CONNECT: EC Directorate-General CONNECT
DPA: Data Protection Authorities
DPO: Data Protection Officer
DSM: Digital Single Market
EC: European Commission
ECA: European Court of Auditors
EC3: Europol's European Cybercrime Centre
ECSM: European Cyber Security Month
ED: Executive Director
eID: electronic Identity
ENISA: European Union Agency for Network and Information Security
ETSI: European Telecommunications Standards Institute
EU: European Union
EURO SCSIE: European SCADA Security Information Exchange
FAP: Finance, Accounting & Procurement Unit
FIRST: Forum of Incident Response and Security Teams
FM: Facilities Management
FTE: Full Time Equivalents
GAGR: Compound Annual Growth Rate
GDPR: General Data Protection Regulation
H2020: Horizon 2020
HCCI: Heraklion Chamber of Commerce and Industry
HLE: High Level Event
HR: Human Resources Section
IAS: Internal Audit Service
ICC & **IAC**: Internal Control Coordination and Internal Audit Capability
ICS: Industrial Control Systems
ICT: Information and Communication Technologies
IoT: Internet of Things
IS: Information Systems
ISO: International Organization for Standardization
ISO: Information Security Officer
ISP: Internet Service Provider
ITU: Information Technology Unit
IXP: Internet exchange point
KII: Key Impact Indicator
KPI: Key Performance Indicator
LEA: Law Enforcement Agency
LIBE: Civil Liberties Committee
MB: Management Board
MS: Member State
n/g CERT: National/Governmental CERT
NCO: National Contact Officer
NCSS: National Cyber Security Strategies
NIS: Network and Information Security
NLO: National Liaison Officer
NRA: National Regulatory Authority
PET: Privacy Enhancing Technology
PPP: Public Private Partnership
PSG: Permanent Stakeholders Group
Q: Quarter
QMS: Quality Management System
QWACs: Qualified Website Authentication Certificates
R & D: Research and Development
SCADA: Supervisory Control And Data Acquisition
SEE: School of European Education
SME: Small and Medium Enterprise
SOGIS: Senior Officials Group Information Systems Security
SOP: Standard Operating Procedures
TF-CSIRT: Task Force of Computer Security Incidents Response Teams
TSP: Trust Service Provider
US: United States of America
WP: Work programme
WPK: Work Package
WS: Work Stream

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 [1] 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 solutions that are based on solid operational experience. ENISA also supports the development of the European Union (EU) policy and law on matters relating to network and information security (NIS), thereby contributing to economic growth in Europe'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.

In cooperation with and in support of Member States and EU institutions, ENISA prioritises contributions in terms of:

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

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

Capacity: Support Europe in maintaining state-of-the-art network and information security capacities by assisting the Member States and European Union bodies in reinforcing their NIS capacities.

Community: Foster the emerging European network and information security community, by reinforcing cooperation at the EU level among Member States, European Union bodies and relevant NIS stakeholders, including the private sector.

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

According to Article 4 of Regulation (EU) No 526/2013, the Agency comprises of the Management Board (MB); the Executive Director and staff; and the Permanent Stakeholders Group (PSG). In order to contribute to enhancing the effectiveness and efficiency of the operation of the Agency, the MB has established an Executive Board.

The MB held its ordinary meeting to adopt decisions on budgetary and administrative matters as well as rules implementing provisions of ENISA Regulation (EU) No 526/2013 and Staff Regulations. The Board also adopted planning documents such as an annual Work programme, a multi-annual staff policy plan, a Statement of Estimates and others.

The PSG is a body that advises the Executive Director on drawing up a proposal for the Agency's work programme. In 2015, 2 formal PSG meetings were held.

1 For the links and names of all relevant policy documents please see Annex G.

SUMMARY

IMPLEMENTATION OF ENISA ANNUAL WORK PROGRAMME

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. Ensuring adequate levels of protection for contemporary IT systems in any context requires recognising and adapting to changes in the evolving threat environment by making appropriate policy adjustments. 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 2015 contained a total of 53 deliverables (which includes also workshops and similar activities) that have been produced in full.

The highlights of 2015 include new best practices and recommendations in sectors such as eHealth, finance, and smart infrastructure and services. The Agency's continued brand activities such as Article 13a reporting, Computer Security Incidents Response Teams (CSIRT) training and preparations for Cyber Europe 2016. ENISA updated the Threat Landscape and published guidelines and best practice recommendations regarding Privacy Enhancing Technologies. Requests under Article 14 of the ENISA Regulation (EU) No 526/2013 continued unabated as a method for stakeholders to request assistance, culminating in 23 new requests, almost double compared to 2014.

The Agency also organised a number of high profile events throughout the year, such as the High Level Event, the first ENISA Industry event, the Annual Privacy Forum and the EU Cyber Security Month campaign. ENISA also hosted a number of important workshops, gathering experts in the field to discuss cybersecurity topics.

MOST RELEVANT KEY PERFORMANCE INDICATORS

In 2015, 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 on how the Agency reached its goals.

- By 2016 10 private stakeholders use ENISA's Threat Analysis/Landscape process in their corporate risk management processes. (Impact indicator in WPK1.1. NIS Threat Analysis.)
  - Major organisations from Member states in both governmental and sectoral areas have quoted ENISA Threat Information. In performed impact assessments, ENISA Threat Landscape has achieved top results. And individual external stakeholders continuously contact ENISA to obtain additional information/details on threat information. Finally, the

achieved level of cooperation with competent EU and Member State organisations is indicative of the impact level achieved through this stream of work.

- By 2017, 8 MS use ENISA's recommendations and good practices on National Cyber Security Strategies. (Impact indicator in WPK 2.1: Assist in public sector capacity building.)
  - 2015: 2 workshops in 2015 together with the EU Presidency (Riga: 30 participants, 15 from MSs; Luxembourg: 28 participants, 18 from MSs), 4 MSs created their national cybersecurity strategy based on ENISA recommendations (until November 2015), ENISA NCSS map was the most popular webpage (features update).
- By 2017, continued CSIRT training will be provided to a minimum of 20 participants of different organisations in 5 MS. (Impact indicator in WPK 2.1: Assist in public sector capacity building.)
  - 2015: 11 CSIRT trainings were delivered across 7 MSs reaching over 200 participants representing various private and public organisations. ENISA CSIRT training is the most popular Article 14 request in many EU MSs.
- Engage at least 5 key sector actors in launching and establishing a forum that brings together 3 communities, namely: trust service providers from the EU Trusted List, conformity assessment bodies and supervisory authorities. The degree of activity of the relevant key sector actors in this forum is of importance to its success. (Impact indicator in WPK 3.1: Provide information and advice to support policy development.)
  - The 1st TSP Forum was organised in late 2015 and it was attended by more than 100 participants, including representatives of all key sectors, many EU MS National Authorities, etc. A follow up with the organisation's 2nd TSP Forum is currently underway for 2016.
- By 2017, 12 MSs will make direct use of the outcomes of Article 13(a) work by explicitly referencing it or by adopting it at the national level. (Impact indicator in WPK 3.2: Assist EU MSs and Commission in the implementation of EU NIS regulations.)
  - In 2015, a study on the impact assessment of Article 13a in the EU was published. In total 23 countries responded that they have implemented the Article 13 requirements (although the actual figure is greater), and on average 15 out of them (more than 60 %) declared that they have used different work items produced by the group in their national implementation and work. More than this, 19 (82 %) National Regulatory Authorities (NRAs) are currently satisfied with the current work model of the Article 13a expert group, drafting and agreeing on common technical guidelines and on sharing experiences. (82 %) NRAs are currently satisfied with the current work model of the Article 13a expert group.
- More than 80 participants in APF'15 (researchers, policy-makers and industry participants) (Impact indicator in WPK 3.3: Assist EU MSs and Commission in the implementation of NIS measures of EU data protection regulation.)
  - The Annual Privacy Forum (APF) 2015 was attended by more than 100 participants and the next editions of this conference have been planned.

KEY CONCLUSIONS ON THE EFFECTIVENESS OF THE INTERNAL CONTROL SYSTEMS AND FINANCIAL MANAGEMENT

ENISA has adopted a set of internal control standards, based on international good practice, that aim to ensure that policy and operational objectives are achieved. As regards financial management, compliance with these standards is compulsory and the Agency 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 2015, 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

While during 2015 the Agency continued to deliver against its annual work programme, it is worth stating that the need for activities aimed at securing Europe's information security has been increasing.

It should be noted that the objectives of the Agency address NIS, a fast-changing area. The use of IT, the development of new technologies but also new challenges and new security risks are emerging at a relentless pace. For instance, according to Eurostat, 'ICT have become widely available to the general public, both in terms of accessibility as well as cost. A boundary was crossed in 2007, when a majority (55 %) of households in the EU-28 had internet access. This proportion continued to increase and in 2014 reached 81 %'[2].

In 2015, the worldwide cybersecurity market was estimated [3]as ranging from USD 75 billion and forecasted to grow to USD 170 billion by 2020. The cybersecurity market size in Europe, according to Gartner [4], was estimated to grow from EUR 20.1 billion (out of Gartner's EUR 71.7 billion worldwide estimation for 2015) with 6 % Compound Annual Growth Rate (CAGR) to EUR 24.4 billion in 2018, maintaining a share above one quarter of the worldwide cybersecurity market.

At the same time, the estimated worldwide economic impact of cyber-attacks has reached half a trillion USD[5]. Global surveys [6] find that 15 % of businesses say they have faced a cyber-attack in the past year. Businesses in the EU (19 %) and North America (18 %) have been most heavily targeted according to the same source.

ENISA carries out the analysis of cyberthreats and publishes a yearly Threat Landscape report [7] that vouches for the smooth advancement of maturity on both cybersecurity defence and protection as well on cybersecurity threats. Cyberspace stakeholders have gone through varying degrees of further maturity. While friendly agents have demonstrated increased cooperation and orchestrated reaction to cyberthreats, hostile agents have advanced their malicious tools with obfuscation, stealth and strike capability.

On the defenders' side, improvements have been achieved in coordinated campaigns to disrupt and dismantle malicious infrastructures, strengthen the legal and governance cyberdefence framework and develop more efficient products.

Adversaries have achieved considerable advances too. Cyberthreats have undergone significant evolution and just as in 2014, significant breaches have covered front pages in the media. It is alarming, however, that seemingly cyberthreat agents had the margin and resources to implement a series of advancements in malicious practices.

In 2015, changes observed referred to two areas mentioned hereinafter. The attention of cybersecurity experts has been drawn to incidents in the area of the Internet of Things (IoT) and attacks against cyber-physical interfaces, both being upcoming areas of concern for the cybersecurity community. For instance, from incident statistics it becomes evident that human error and insider threats, if taken together, are sufficient to top the list of cyberthreats. Taking into account the relatively novel features of IoT and the relatively large number of 'insiders' within a smart environment (i.e. smart home) as well as the interactions with health and safety, it is likely that IoT becomes the next frontier for abuse. Policy work in cybersecurity needs continuity and the ability to adjust to frequent and often disruptive developments.

Positive developments can be reached by strengthening the Agency. While the Agency features mandatory tasks emanating from the regulatory framework (ENISA regulation, eIDAS regulation, ePrivacy directive, etc.), emerging policy and regulatory requirements (Telecom pack review, Data protection regulation, NIS directive) create new impetus. In view of these developments it is expected that if the Agency's resources are reinforced, it can contribute to better policy outcomes and augment its policy outreach to the benefit of many more stakeholders across Europe. Especially in the area of a digital single market, ENISA can further enhance the capacity and preparedness of MSs to prevent, detect and respond to NIS problems and incidents.

2 Eurostat, Information society statistics — households and individuals, June 2015, available at: http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_and_individuals

3 Cybersecurity market report, Cybersecurity Ventures, Q4 2015, available at: http://cybersecurityventures.com/cybersecurity-market-report/

4 Cyber-security market size in Europe, Gartner 2014.

5 McAfee, Net Losses: Estimating the Global Cost of Cybercrime, report summary, 2014, available at: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2-summary.pdf

6 Grant Thornton, Cyber-attacks cost global business $300bn+, available at: http://www.grantthornton.global/en/insights/articles/cyber-attacks-cost-global-business-over-$300bn-a-year/

7 ENISA Threat Landscape 2015 (ETL 2015), January 2016, available at: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015

1.

SECTION I.

KEY RESULTS IN THE IMPLEMENTATION OF ENISA WORK PROGRAMME 2015

This Annual Activity Report (AAR) for 2015 follows the structure of the ENISA Work programme (WP) 2015. The WP 2015 was aligned with the strategic objectives featured on the strategy and the multi annual planning of the Agency. The strategic objectives of the WP 2015 were as follows:

SO1: To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network & 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 2015 implementation are presented for each of the above mentioned objective. 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.

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

Ensuring adequate levels of protection for contemporary IT systems in any context requires recognising and adapting to changes in the evolving threat environment. Whilst it is clearly not possible to foresee 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.

The Agency supported the MSs and the Commission in their efforts to improve Critical information Infrastructure protection (CIIP) by fostering a common approach across the MSs and by ensuring that good practice and lessons learnt are shared and properly deployed in an effective manner. The Agency worked with the MSs, the Commission and the private sector in capacity building across the EU. In particular, the Agency supported the development of voluntary baseline security requirements for CIIP sectors and harmonised efforts in the area of mandatory incident reporting, taking under consideration existing national and international frameworks (e.g. NIST). The approach was not limited to securing Internet related services, but took into consideration other networks and services as appropriate.

Where technology is concerned, information security has traditionally been viewed as an approach to secure

people, processes and technology. Of these three factors, it is mainly technological evolution that impacts the way in which people's behaviour and processes change. A large part of modern information security therefore boils down to adapting current methods to emerging technologies, and business models.

As a centre of excellence and expertise in the field of NIS, ENISA used the expertise of its staff to advise its stakeholders about trends in the digital world that affect security and suggested good practices to be taken in order to successfully mitigate the associated risks at an early stage of end-user adoption. In particular, ENISA sought to identify the consequences of deploying new technologies and approaches in order to enable the opportunities that such developments bring.

ENISA assisted the Commission and MSs in defining and implementing a framework for training professionals in NIS to meet the requirements of industry at all levels. The goal was to align training goals with career paths for security professionals and to provide a more global background in NIS for professionals in other areas.

The following work packages were part of this Strategic Objective:

WPK 1.1 — NIS Threats Analysis
The main goal of this WPK was to develop the current cyberthreat landscape. This information is important in the identification of NIS gaps and security needs for a wide spectrum of stakeholders.

WPK 1.2 — Improving the Protection of Critical Information Infrastructures
In this WPK, ENISA's aim was to provide advice and assistance on request to targeted stakeholders of Critical Information Infrastructures (CIIs).

WPK 1.3 — Securing emerging Technologies and Services
This WPK aimed to develop good practices on emerging smart infrastructures and services and work with relevant stakeholders to deploy them at an early stage of adoption.

WPK 1.4 — Short- and mid-term sharing of information regarding issues in NIS
This WPK aimed to define and implement a framework that allowed the Agency to provide timely and high quality responses to NIS developments.

1.1.1 WPK 1.1: NIS Threats Analysis

The main objective of this work package was to collect and collate current data in order to develop the ENISA threat landscape. It includes current threats, as well as threat trends in NIS and emerging technologies. The threat landscape is based on existing publicly available material on threats, risks and trends.

ENISA assisted the Commission and MS in defining and implementing a framework for training professionals in NIS to meet the requirements of industry at all levels.

The ENISA Threat Landscape 2015 was a continuation of the work started in 2012. Compared to previous years, there is noticeable improvement in the quality of threat information collected within related organisations due a wider spread and depth of information sources.

In addition, in this work package ENISA further identified emerging technologies for risk assessment and threat analysis. A report was published highlighting the threats and potential compromises related to the security of SDN/5G networks. The report identified related network assets and the security threats, challenges and risks arising from these assets. Driven by the identified threats and risks, existing security mechanism and good practices for SDN/5G/NFV were identified. Finally based in the collated information technical, policy and organisational recommendations for proactively enhancing the security of SDN/5G were provided.

1.1.2 WPK 1.2: Improving the protection of Critical Information Infrastructures

The objective of this work package was to provide advice and assistance to targeted stakeholders of Critical Information Infrastructures (CIIs).

More specifically ENISA took stock of MS policies, regulations and strategies including international frameworks (e.g. US NIST) and identified gaps related to CIIs. The Agency cooperated with public and private stakeholders to identify good practices, collected and analysed requirements and issued recommendations for improving the way MSs address the protection of CIIs.

In the area of Internet Interconnections, ENISA continued in its development of methodologies for the identification of critical communication networks, links, and components. ENISA considered existing outputs from projects and initiatives in the security and resilience of Internet interconnections. In cooperation with ISPs and other public stakeholders ENISA validated the methodology and developed a maturity assessment mechanism. This mechanism allows MSs to assess the situation within their borders. The Agency also assessed whether this methodology could be extended to other CIIs and targeted stakeholders so as to customise it to their needs and requirements.

In the area of ICS-SCADA security, ENISA cooperated with SCADA and Control Systems Information Exchange (EuroSCSIE) as well as other related expert groups to take stock and conduct an analysis of cybersecurity maturity levels in critical sectors (e.g. transport, energy, water supply, etc.). ENISA's work will be utilised by policy-makers in MSs and EU Institutions to create a secure framework for the implementation and deployment of more efficient ICS-SCADA systems. The study also made general recommendations to EU Member States and the European Commission on how to improve CIIP across the European Union. The Agency will continue promoting its work on the security of ICS-SCADA devices.

In the area of smart grids, ENISA continued its work on appropriate security measures and national governance security models of smart grids. The Agency promoted its existing appropriate security measures and further cooperated with public and private stakeholders to improve their existing security governance models for smart grids. A study was published on the evaluation of the interdependencies and communications between the assets that make up the new power grids, their architectures and connections in order to determine their importance, threats, risks, mitigation factors and possible security measures to implement. ENISA also conducted a study identifying the maturity level of ICS-SCADA cybersecurity in Europe and identified good practices used by European Member States to improve. It should be noted that smart grid area covers more than ICS; so for this activity more areas were considered: smart cities, smart energy etc. ENISA also continued its contribution to DG ENER's Smart Grid Task Force and all relevant EU initiatives (e.g. CEN/CENELEC/ETSI, ERNCIP, DENSEK, etc.). Finally the Agency contributed to national and EU efforts (e.g. SOGIS) related to better alignment of certification policies and strategies at the EU level.

In the area of cloud computing, ENISA actively contributed to the EU Commission's EU Cloud Computing Strategy by delivering targeted advice on cybersecurity matters (e.g. certification, appropriate security measures, procurements, SLAs and others). The Agency continued its work in the area of governmental clouds, assisted MSs to develop their national governmental strategy's and deploy ENISA's good practice guide. ENISA also worked with the public and private sector to promote its work on the certification of cloud computing components and services. The Agency worked to establish its meta-certification framework as a model to be used by users, SMEs and leading players in the market, so as to allow cloud users to select the most appropriate existing certification scheme for their needs.

In the area of finance, ENISA, through consultation with public and private stakeholders, identified policy, technical and regulatory barriers and challenges for using cloud, either as infrastructure or as a service, in the finance sector. Based on the analysis ENISA provided recommendations to financial institutions, regulators and cloud service providers about what ENISA believes should be done to support the secure adoption of cloud services in the finance sector. The Agency has issued recommendations for policy-makers, EU MSs and industry in mitigating barriers and challenges. By removing known barriers ENISA has helped the EU industry become more competitive and innovative. Also the Agency in consultation with public and private stakeholders has positioned itself to better understand the security and privacy challenges related with third party payments providers.

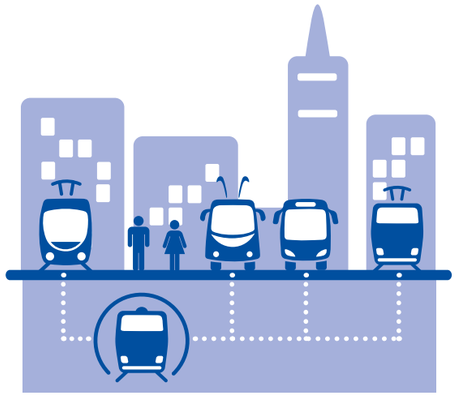
Finally in the area of eHealth, ENISA, with the consultation of public and private stakeholders, published a study that took stock and assessed the security and resilience of major eHealth infrastructures and services. The Agency developed good practices and recommendations for policy-makers, industry and EU MSs on the resilience and security of eHealth infrastructures and services.

1.1.3 WPK 1.3: Securing emerging Technologies and Services

ENISA developed good practices on emerging smart infrastructures and services in such areas as [8]:

- intelligent transportation systems used in the context of smart cities;
- Big Data and corresponding services used for offering critical services;
- Smart Home Environments.

In each of these areas ENISA identified 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. The Agency identified EU and nationally funded projects on these topics, liaised with them, assessed their findings and deliverables, and further engaged them in the corresponding expert groups and with the organisation of workshops.



Based on consultation with stakeholders and desk-top research and analysis, ENISA developed good practices and issued recommendations addressing policy-makers, manufacturers, developers, infrastructure owners, operators and service providers. The following reports were published with the aim to provide smart infrastructure service providers, operators, manufacturers and developers with good security and resilience practices when designing and deploying such services in order to minimise the exposure of such networks and services to all relevant cyberthreat categories.

The *Cyber security and resilience of intelligent public transport* report gives an overview of the existing security measures (good practices) that could be deployed to protect these critical assets and ensure security of the IPT system, based on a survey and interviews of experts from the sector, municipalities, operators, manufacturers and policy-makers.

The *Cyber security for smart cities — an architecture model for public transport* report describes how good practices are put into a relationship with different city maturity levels thus allowing representatives of operators and municipalities to quickly assess whether or not they lag behind other cities with the same maturity level in terms of cybersecurity and, if so, to take appropriate actions.

The *Good practices and recommendations on the security and resilience of Big Data services* study aims at identifying the key security challenges that companies face when implementing Big Data solutions, from infrastructures to analytics applications, and how those are mitigated. The analysis focuses on the use of Big Data by private organisations in given sectors (e.g. Finance, Energy, Telecom).

The *Security and resilience of Smart Home environments* study aims at securing Smart Home environments from cyberthreats by highlighting good practices that apply to every step of a product lifecycle: its development, its integration in Smart Home environments, and its usage and maintenance until end-of-lifecycle.

It is expected that the early adoption of these recommendations and good practices will boost the trust and confidence of potential users of such technologies and pave the way for wider deployment.

1.1.4 WPK 1.4: Short- and mid-term sharing of information regarding issues in NIS

ENISA implemented a framework that allows the Agency to provide timely and high quality responses to NIS developments. ENISA acted on NIS issues and occurrences that reached a certain level of public and media attention by giving information and, where appropriate, guidelines for dealing with the issue on short notice. The guidelines did not address immediate responses, but concentrated on medium- to long-term preparatory measures. The overall goal for each Note was to highlight fundamental facts and shortcomings behind specific NIS issues and occurrences, and to give independent advice to key stakeholders.

8 Infrastructure can be defined as 'smart' when investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure support sustainable economic development and a high quality of life, with wise management of natural resources, through participatory action and engagement.

1.1.5 General results. Achievement of Impact indicators for Objective 1

SO1 — To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network & Information Security (NIS)	
WPKs, Impact Indicators	**Achieved results**
WPK 1.1: NIS Threats Analysis	
Engage 10 public and 10 private stakeholders in the Threat Analysis/Landscape process. These stakeholders should participate in the validation of the work.	More than 10 public and 10 private stakeholders contributed in the Threat Analy sis/Landscape process as well as the validation of the work.
Engage 10 public and 10 private stakeholders in the risk assessment of each emerging technology/sector. These stakeholders should participate in the validation of the work.	More than 10 public and 10 private stakeholders contributed to the risk assessment of each emerging technology/sector as well as the validation of the work
5 MSs use, by 2016, ENISA's Threat Analysis/Landscape process in their national risk management processes.	ENISA Threat Landscape results have been reused within multiple states, both within and outside EU. In various discussions, blogs and presentations initiated by public stakeholders, references to ENISA Threat Landscape 2015 have been found.
10 private stakeholders use, by 2016, ENISA's Threat Analysis/Landscape process in their corporate risk management processes.	ENISA Threat Landscape results have been referenced/used by multiple private stakeholders. One interesting reference that has been made is the inclusion of ENISA Threat Landscape content (threat taxonomy) within the MISP (Malware Information Sharing Platform) document platform as reference document with regard to the classification of cyber threats.
WPK 1.2: Improving the protection of Critical Information Infrastructures	
By 2017, 8 MSs use ENISA's findings and good practices in their national CIIP strategies.	By 2015, 1 workshop in September about CIIP. More than 8 MSs participated in the workshop, more than 16 MSs took part in interviews and surveys providing input for the study.
Engaging 8 public and 8 private stakeholders (ISP, IXPs, Telcos) in the development of the methodology on internet interconnections	By 2015, — 1 workshop in October about communication network dependencies for smart grids study (25 experts from national authorities and critical infrastructure operators in Europe), — 1 meeting in November of the Internet Infrastructure Security and Resilience Reference group of experts (INFRASEC 14 experts: 2 cyber sec agencies, 3 major IXPs in Europe, 2 internet security research organisations), — study completed and dedicated resilience portal area about internet threats created.
By 2016, 5 MSs use ENISA's government cloud good practices in their national strategy.	By 2015, 1 workshop in June on Cloud Security (50 participants, more than 25 from private sector). In this event a session on Governmental Clouds was created with the participation of experts from 3 Member States: Estonia, Netherlands, UK.
5 MSs and 5 private stakeholders use ENISA's recommendations on finance in their corporate/national risk assessment and management approach.	By 2015, — 1 workshop in October in cooperation with the European Banking Authority (EBA). In this event 26 EU national financial regulators, 12 EU private banks and 4 major cloud service providers participated. — the Expert Group in Finance was engaged and on average 15 experts from financial private sector participated.

5 MSs and 5 private stakeholders use ENISA's recommendations on eHealth in their corporate/national risk assessment and management approach.	By 2015, — participation in the workshop of 10 MSs, 10 eHealth providers and the EC, — 12 MSs participated in the study/survey.
WPK 1.3: Securing emerging Technologies and Services	
By 2016, 5 MSs and 8 private stakeholders use ENISA's recommendations on smart cities in their corporate risk assessment and management approach.	By 2015, — 1 workshop in October about Security in Transport and Smart Cities. Co-organisation with DG MOVE. 22 participants attended to the workshop from 12 MSs as well as 1 non-EU country (7 participants from the public sector, 15 participants from the private sector). — 12 MSs participated in the study.
By 2016, 5 MSs and 8 private stakeholders use ENISA's recommendations on big data in their corporate risk assessment and management approach.	21 entities from private sector participated in the survey on Big Data security. The following sectors were represented: Finance, Energy, Telecom, Research and Academia.
By 2016, 8 MSs and 8 private stakeholders use ENISA's recommendations on Smart Home Environments in their corporate risk assessment and management approach.	By 2015, — 1 workshop in October about Security in Transport and Smart Cities. Co-organisation with DG MOVE. 20 participants attended to the workshop from 10 MSs as well as 1 non-EU country (6 participants from the public sector, 14 participants from the private sector). — 12 MSs participated in the study.
WPK 1.4: Short- and mid-term sharing of information regarding issues in NIS	
Improve information flows between the CERT EU, ENISA and the CSIRT community.	Continuous support via different types of engagement (steering board/CERT-EU, steering committee/TI-TF-CSIRT, liaison membership/FIRST and ad hoc mutual support on projects).
Provide timely information to stakeholders, e.g. CISO, CIO level, in a coordinated manner.	Info Notes regularly published (in 2015 only ENISA internal/all management levels).

Copyright ©Shutterstock

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

SO1 — To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network & Information Security (NIS)	
WPKs, Impact Indicators	**Achieved results**
WPK 1.1: NIS Threats Analysis	
D1: Annual Threat Analysis/Landscape Report (Q4, 2015)	ENISA Threat Landscape 2015, https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015
D2: Risk Assessment on 2 emerging technology/application areas (Q4, 2015)	Big Data Threat Landscape, https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/bigdata-threat-landscape Threat Landscape and Good Practice Guide for Software Defined Networks/5G, https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/sdn-threat-landscape
WPK 1.2: Improving the protection of Critical Information Infrastructures	
D1: Stock Taking, Analysis and Recommendations on the protection of CIIs (Q3, 2015)	Stocktaking, Analysis and Recommendations on the protection of CIIs, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis
D2: Methodology for the identification of Critical Communication Networks, Links, and Components (Q4, 2015)	Communication network interdependencies in smart grids, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/communication-network-interdependencies-in-smart-grids/
D3: Analysis of ICS-SCADA Cyber Security of Devices in Critical Sectors (Q4, 2015)	Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/maturity-levels/
D4: Recommendations and Good Practices for the use of Cloud Computing in the Finance Sector (Q4, 2015)	Secure Use of Cloud Computing in the Finance Sector, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/cloud-in-finance/
D5: Good Practices and Recommendations on resilience and security of eHealth Infrastructures and Services (Q4, 2015)	Security and Resilience in eHealth Infrastructures and Services, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/ehealth_sec/security-and-resilience-in-ehealth-infrastructures-and-services
WPK 1.3: Securing emerging Technologies and Services	
D1: Good Practices and Recommendations on the Security and Resilience of Intelligent transportation systems (Q4, 2015)	Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/intelligent-public-transport/good-practices-recommendations Architecture model of the transport sector in Smart Cities, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/intelligent-public-transport/smart-cities-architecture-model
D2: Good Practices and Recommendations on the Security and Resilience of Big Data Services (Q4, 2015)	Big Data Security, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/big-data-security/
D3: Good Practices and Recommendations on the Security and Resilience of Smart Home Environments (Q4, 2015)	Security and Resilience of Smart Home Environments, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/smart-homes/security-resilience-good-practices

WPK 1.4: Short- and mid-term sharing of information regarding issues in NIS	
D1: Establish necessary procedures, workflows, tools, etc. to enable ENISA to carry out the Info Notes service (Q2, 2015)	Info Notes service established, procedures and workflows defined. Until now the service is defined for internal use. Service will be continued in 2016 for restricted public use.
D2: Info Notes on a specific NIS issue (ongoing service with pilot from Q2, 2014; conclusions on first year of activity in Q4, 2015)	InfoNotes in 2015 were published as internal only. The following topics were addressed: Ransomware, The Next Evolution of Ransomware, Access routers leave users vulnerable, Internal Briefing on Gemalto, FREAK Attack — Export Restrictions Gone Wrong, Aircraft Cyber Security, Brute Force, Vulnerability of Life Support and Other Critical Systems, Malware, The Venom Vulnerability, Airplane Hacking — Beyond the Headlines, Phishing / Spear phishing, Authentication Methods, Duqu 2.0 — The Malware that Hit Kaspersky, Cross-site scripting (XSS), The Samsung Keyboard Vulnerability, Social Engineering, The Hacking Team Debacle, Zero-Day, Hacking Team Series — The dangers of Flash, Hacking Team Series — Password Policy, Hacking Team Series — The business of Zero-Days, Hacking Team Series — The Insider Threat, Hacking Team series — The Wassenaar Arrangement, Stagefright, Man-in-the-Middle, Buffer Overflow, Public Key Infrastructure (PKI), TSA Master Keys, or: How security through obscurity will hurt you, Abusing MSISDNs, the WhatsApp case, From carjacking to car hacking, The case of the vigilante virus, The Takedown of the Angler Exploit Kit, Decryption of VPN traffic by state actors, Botnets, DNS Sinkhole, The illusion of security, Baidu's Moplus SDK WormHole, What's behind eDellRoot.

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

ENISA assisted MSs and designated EU institutions on capacity building across the EU in terms of government, private sector and wider public sector. In particular the Agency worked together with national bodies (NRAs, CSIRTs, etc.) that had been mandated to carry out these tasks within the MSs, with private sector representatives and with the European Commission to ensure that the approach was coherent across the EU. The Agency continued to support the Commission and the MSs in the implementation of methods and tools for ensuring adequate privacy protection and adherence to EU Data Protection legislation. By supporting initiatives such as the EU cybersecurity month, the implementation of an NIS driving licence and MSs' efforts to introduce NIS topics into education at all levels, ENISA contributed to increasing the level of participation of the EU citizens in activities aimed at improving the level of NIS throughout the Union.

The following work packages constituted this Strategic Objective:

WPK 2.1 — Assist in public sector capacity building
This Work Package aimed at helping operational bodies and communities (namely CSIRTs, but other communities where appropriate) in developing and extending the necessary capabilities in order to meet the ever growing challenges to secure their networks.

WPK 2.2 — Assist in private sector capacity building
This WPK aimed at helping the private sector develop their capacities in the area of cybersecurity (e.g. in the area of Network and Information Security driving licence).

WPK 2.3 — Assist in improving awareness of the general public
This WPK aimed at further developing ENISA's multi-stakeholder facilitation approach and public-private activities.

1.2.1 WPK 2.1: Assist in public sector capacity building

ENISA made great strides to fulfil its aim in terms of helping the EU MSs and other stakeholders, such as EU Institutions and bodies, to develop and extend the necessary capabilities to meet the ever growing challenges to network security. Emphasis was made on supporting operational bodies and communities (namely CSIRTs) by providing good practice material and advice and concrete actions such as CSIRT trainings.

The Agency provided support and advice to MSs on the development, implementation and evaluation of National Cyber Security Strategies (3 specific requests received). The information was diffused through the NCSS Experts Group who shared lessons learnt and prior experience. Taking utmost account of the knowledge shared, these MSs are currently in the adoption phase of their NCSS. The Agency also maintains an interactive NCSS map, with information on the strategies of the MSs as well as of countries around the globe. This map is one of the most popular ENISA sites and on a regular basis the Agency receives information to keep it up to date.

Another important aspect of this support to MS capability building, was the rolling out of training for IT specialists (CSIRTs, etc.) of which more than 200 trainees were trained in 7 Member States and carrying out national exercises.

A number of handbooks where published in the area of CSIRT good practices to further strength the knowledge base of the trainers and maintain an up to date training library. These included:

- Mobile threat incident handling;
- Introduction to advanced artefact analysis;
- Advanced dynamic analysis;
- Advanced static analysis.

An impact assessment of ENISA's support to CSIRTs in 2014 was conducted so as to serve as a basis for a proposed roadmap to 2020. The impact of the ENISA support to the CSIRT community was assessed from a dual perspective — legislative and regulatory — as well as operational, with the key objectives to: update the policy analysis; gather additional input from practitioners, including specific input on the new duties; and together with ENISA, propose concrete projects or actions towards the roadmap implementation.

Finally, in line with ENISA's responsibility to develop capabilities in the area of national Public Private Partnerships the Agency provided targeted and customised assistance (e.g. in a form of a seminar, training) and continued to support the Commission in the management of the NIS platform by targeted public and private stakeholders (especially experts from small industry players), assisting in the formation of virtual groups of experts, and contributing its expertise to position papers developed within the working groups of the NIS platform.

1.2.2 WPK 2.2: Assist in private sector capacity building

The background to ENISA's work in this field includes the EU's Cyber Security Strategy suggestion to develop a roadmap for a 'Network and Information Security driving licence' as a voluntary certification programme to promote and enhance skills and competences of IT professionals.

User education is key to cybersecurity and as such a study was undertaken with the following objectives: to identify gaps between available training courses, certifications and NIS education needs with particular emphasis on ePrivacy and to suggest further actions based on the analysed needs of NIS communities in Europe. The report concludes with a list of recommendation for both the EU and educational organisations in Member States.

The 2015 network and information security quiz to test users' knowledge of ENISA recommendations built upon the success of the previous year's quiz by using feedback received by the users and making functional enhancements.

1.2.3 WPK 2.3: Assist in improving awareness of the general public

The 2015 edition of the European Cyber Security Month (ECSM) resulted in a successful advocacy campaign with 32 countries taking part, some 242 activities from public and private stakeholders and an outreach in social media topping the previous year's statistics. Included within these results are the 417 courses now registered in the NIS Education map.

ENISA has produced a basic cyberhygiene report to help web users (general public) recognise and use tools for online privacy and security. The objectives of the report were to define the current level of information and guidance that is provided to the general public and to provide a proposal for an assessment model for online privacy tools that could bring more assurance in their use, supporting their wider adoption by internet and mobile users. The Agency has found out that a combined effort of all involved stakeholders is needed in the promotion of online, privacy enhancing technologies.

1.2.4 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 in public sector capacity building	
By 2017, 8 MSs use ENISA's recommendations and good practices on National Cyber Security Strategies.	2 workshops were held in 2015 together with the EU Presidency (Riga: 30 participants, 15 from MSs; Luxembourg: 28 participants, 18 from MSs), 4 MSs created their national cybersecurity strategy based on ENISA recommendations (until November 2015), ENISA NCSS map the most popular webpage (features update). In 2016 ENISA will continue work on this topic through updating the NCSS online map, creating training material in a training platform and updating the good practice guide.
By 2017, continued CSIRT training will be provided to a minimum of 20 participants of different organisations in 5 MSs.	In 2015, 11 CSIRT trainings provided in 7 MSs for more than 200 participants representing various private and public organisations.
By 2017, improved operational practices of CSIRTs in at least 15 MSs (ongoing support with best practices development).	In 2015, a Good practice guide on vulnerability disclosure was added to the ENISA's online library for CSIRT services and operational practice improvement. The annual CSIRT workshop for national and governmental CSIRTs held in May in Latvia to discuss and address 'the CSIRT role and services during the EU Presidency' topic (40 participants from 17 MSs).
More streamlined CSIRT exercise and training material with CSIRT and other operational communities' services and methodologies.	In 2015, ENISA's start-up train the trainer program was launched. First workshop for CSIRT trainers in Europe held in September to streamline CSIRT training material and training methodology development (24 educators from 18 MSs including GEANT/TRANSITS; FIRST).
WPK 2.2: Assist in private sector capacity building	
10 public-private stakeholders from MSs follow up on the recommendations from the Roadmap on the NIS in Education.	A mapping of relevant stakeholders in the NIS Education interactive map gathered more than 400 entries from over 20 countries. ENISA further developed a model to disseminate the existing information to interested parties and a new model of engagement for education providers.
Further develop an effective work process to involve more universities and certifications providers (NIS in Education).	ENISA introduced an interactive map to be used by all education providers in the EU to give visibility to their courses. This established a one-stop-shop for NIS education providers and offers them better interactions at EU level. The NIS Education interactive map is available following this link: https://cybersecuritymonth.eu/references/universities.
WPK 2.3: Assist in improving awareness of the general public	
D1: Provide guidance and support for European Cyber Security Month (dissemination material, Q4 2015)	European Cyber Security Month 2015 — Deployment Report, https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2015/ecsm15-deployment-report
D2: Basic cyberhygiene: guidelines for recognizing and using trustworthy security and privacy products for the general public (Q4, 2015)	Online privacy tools for the general public, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/basic-cyber-hygiene

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

In 2015, ENISA continued to provide the Commission and MSs with high quality information, data and advice to support policy-making having an EU dimension.

The Agency also had taken into consideration policy and legislative requirements that are not directly related to cybersecurity, but which had a bearing on how cybersecurity principles are integrated.

At the same time, the Agency continued to support research and development by acting in an advisory role to the Commission for future Framework Programme initiatives in this area. Additionally, ENISA continued its work on Privacy enhancing technologies.

ENISA worked together with the public sector, standards organisations and industry representatives to identify ways for improving the process for agreeing on suitable NIS standards and for promoting their uptake in a cross-border environment.

The following work packages constitute this Strategic Objective:

WPK 3.1 — Provide information and advice to support policy development
This WPK aimed at supporting work on regulation especially in the area of eID.

WPK 3.2 — Assist EU MSs and Commission in the implementation of EU NIS regulations
This WPK aimed at supporting EU MSs in implementing regulation, especially in the area of reporting according to Article 13a of the Telecoms Directive.

WPK 3.3 — Assist EU MSs and Commission in the implementation of NIS measures of EU data protection regulation
This WPK aimed at supporting developing and implementing regulation in the area of Data Protection and Privacy.

WPK 3.4 — R & D, Innovation & Standardisation
This WPK aimed at supporting work on Standardisation (i.e. collaborating with standardisation bodies) and Research & Development (especially in the area of H2020)

1.3.1 WPK 3.1: Provide information and advice to support policy development

In order to remove existing barriers for cross-border e-ID based services, a new Regulation (914/2014) on electronic identification and trust services for electronic transactions in the internal market was published in 2014.

In 2015 ENISA continued to support activities in this field with the following actions:

- studied the technological aspects and market for qualified website authentication certificates (QWACs);
- reviewed and evaluated the standards related to TSPs and eIDs (also developed under mandate M-460 and in light of the new Regulation), and made a mapping to the requirements of eIDAS;
- ENISA in collaboration with the Commission launched the creation of a forum bringing together three communities, namely: trust service providers from the EU Trusted List, conformity assessment bodies and supervisory authorities. This action will be followed up in 2016 and further.

Finally, ENISA collaborated with FESA in the area of exchange of information on the supervision of TSPs.

1.3.2 WPK 3.2: Assist EU MSs and Commission in the implementation of EU NIS regulations

ENISA focussed its efforts on assisting regulatory authorities and the Commission in the implementation of EU regulations related to incident reporting. This effort built on successful work done in this area from previous years namely in the area of Article 13a.

The Agency provided support to:

- NRAs and EU MSs on the implementation of Article 13a (disruptions in the telecom sector) and Article 4 (personal data breach notification) and the developed synergies among the two;
- NRAs and EU MSs on the implementation of Article 19 of new Regulation on electronic identification and trusted services (eIDAS);
- the Commission and MSs on the implementation of the NIS Directive.

ENISA continued collecting and analysing annual, national reports of security breaches from 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. NIS Platform), analysed the reports, compared them with previous years, identified good practices and lessons learnt and made recommendations to NRAs and the private sector to mitigate these threats in the future. Also the Agency assessed the impact of incident reporting schemes (Article 13a) trying to identify the changes in outcome that can be attributed to the regulations. The results of the evaluation have served as input to the EC public consultation for the new telecom package. According to this assessment, 82 % of NRAs are currently satisfied with the work model of the Article 13a expert group and the role of ENISA. The Agency also identified lessons learnt, evaluated the value for money of these schemes and issued recommendations for stakeholders.

Additionally, ENISA continued its effort to bring NRAs, DPAs and the Commission together for the harmonisation and implementation of the security and data breach articles (Article 13a and Article 4). The Agency also further assessed the Article 4 incident reporting scheme by means of a survey that was executed with the support of the Commission, and the results presented in a workshop. In that survey, all relevant stakeholders had the opportunity to discuss the challenges and propose recommendations towards a more harmonised and cost efficient way of implementing the two articles so as to avoid overlaps. ENISA also organised a workshop on incident prevention and reporting in Bucharest (June 2015). The participants were from Member States, National Regulatory Agencies, solution providers and assets owners.

ENISA has already contributed to the area of electronic identification and trusted services (eIDAS) by providing recommendations on incident reporting by the trust service providers to the supervisory bodies. In 2015, ENISA continued its efforts to aggregate together all relevant stakeholders (Article 19 expert group) from MSs including the competent regulatory bodies of MSs and deliberated with them on the development of a consistent incident reporting framework for Article 19. With ENISA's support the scope and the parameters were defined as well as the thresholds for the summary reporting by the supervisory bodies to ENISA and the Commission. ENISA also considered conceptual synergies with Article 13a and supported the Article 19 expert group in developing the functional requirements by an automated tool for reporting incidents in the context of Article 19.

1.3.3 WPK 3.3: Assist EU MSs and Commission in the implementation of NIS measures of EU data protection regulation

In 2015, ENISA intensified its efforts in the field of privacy and trust in a number of areas.

Firstly, ENISA analysed the obstacles of the adoption and evolution of privacy technologies and clarified why in the current practice of web services PETs are rarely used. The report also studied the technical possibilities as well as the economic incentives that could be used to further increase the market penetration of such tools.

Secondly, due to the recognition of privacy enhancing technologies in several policy documents, e.g. the draft data protection regulation proposal, that are based on complex cryptographic building blocks, coupled with security of these building blocks being constantly challenged by new attacks, ENISA produced a report pointing to already established EU policies and processes to addresses these issues. The report was distributed to members of the ENISA MB.

Emerging technologies in the areas of online information sharing, data merging and data mining create new possibilities for the processing of personal data and, thus, new privacy risks. ENISA produced a state-of-the art analysis of the data protection threats, risks and protection measures in the emerging big and open data landscape. During the Annual Privacy Forum, ENISA brought together both policy-makers and the research community to address the lag between data protection legislation and technological protection mechanisms and the challenges of data protection and privacy.

The 2015 version of the ENISA report entitled 'Indicative list of appropriate cryptographic protection measures' was distributed to the members of the MB. The report will be used by the Commission as a main reference document for the publication of a list of appropriate technological protection measures pursuant to Article 4(3) of Commission Regulation (EU) No 611/2013. Based on the latest scientific evidence at the moment of publication, technological breakthroughs may occur that compromise the recommended protection measures, which is why the report was updated. As was the case in previous years, in the context of this work ENISA collaborated with well recognised experts in the field (also ensuring high quality peer reviews). In addition, ENISA involved experts in the field from National Authorities (BSI, ANSSI, etc.).

1.3.4 WPK 3.4: R & D, Innovation & Standardisation

Since its creation ENISA has tracked the development of standards in the area of Network and Information Security, maintaining close contacts and collaboration with International Standardisation Organisations. In 2015, the Agency monitored NIS standards across the EU and globally. This enabled ENISA to keep its activities up-to-date with the latest developments as well as inform its stakeholders on new NIS standardisation activities and flag opportunities and/or risks as they developed.

Since 2012 ENISA contributes actively to the creation and work of the ETSI CEN-CENELEC Cyber Security Co-ordination Group (CSCG). This collaboration with CSCG continued and ENISA further strengthened its synergies between CSCG and its work programme. In this context of the CSCG activities work was performed to analyse good practices within the governance framework of the European Union and proposing recommendations for stakeholders. A gaps and overlaps analysis of the standardisation of cybersecurity was also performed in separate report.

Finally a study was conducted to analyse the adoption of information security and privacy standards by SMEs in Europe. Despite rising concerns on information security risks the results of the analysis indicate that adoption is low due to a number of identified drivers and barriers.

In the areas of interest to the ENISA Work Programme the Agency continued to collaborate with and to support EU-funded R & D projects (H2020). The main aim of the activity was to align the objectives of policy initiatives in the area of NIS with that of the relevant EU-funded R & D projects (H2020). Collaboration was formed by way of a workshop organised by ENISA and representatives from MSs.

Copyright ©Shutterstock

1.3.5 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	**Achieved results**
WPK 3.1: Provide information and advice to support policy development	
Engage at least 5 key sector actors in launching and establishment of a forum that brings together 3 communities, namely: trust service providers from the EU Trusted List, conformity assessment bodies and supervisory authorities. The degree of activity of the relevant key sector actors in the forum is of importance to its success.	The 1st TSP Forum was organised at the end of June 2015. The forum was attended by more than 100 participants and by representatives from all key sector actors from many EU MSs.
Validations by at least 5 representatives from different MSs of the contribution to the implementation of the Regulation on electronic identification and trusted services for electronic transactions.	The participants of the eIDAS TF were involved throughout this work and also contributed at all stages of the peer review.
WPK 3.2: Assist EU MSs and Commission in the implementation of EU NIS regulations	
By 2017, 12 MSs make direct use of the outcomes of Article 13a work by explicitly referencing it or by adopting it at nationally level.	By 2015, a study on the impact assessment of Article 13a in EU was published. 23 countries have responded that they have implemented the Article 13 requirements (although the real number is greater than this), and on average 15 of them (more than 60 %) declared that they have used different work produced by the group in their national implementation and work. More than this, 19 (82 %) NRAs are currently satisfied with the current work model of Article 13a expert group, drafting and agreeing on common technical guidelines and sharing experiences.
By 2017, 10 MSs implement recommendations by ENISA on implementing and enforcing Article 4.	12 MSs participated in ENISA's survey on Article 4 data breaches. Workshop organised by EC on data breaches of Article 4 and more than 20 MSs participated.
By 2017, 10 MSs implement ENISA's recommendations on Article 19.	3 workshops of Article 19 expert group organised in 2015. This working group of experts consists of national regulatory authorities and ministries from across Europe: the Article 19 Expert Group. On average, more than 15 MSs participated in each one of them.
WPK 3.3: Assist EU MSs and Commission in the implementation of NIS measures of EU data protection regulation	
At least 5 representatives from different MSs contributing to ENISA guidelines and best practice recommendations regarding Privacy Enhancing Technologies.	6 EU MSs representatives contributed to the report and also supported ENISA in the peer review stages.
At least 10 actors in the field validating the results of the studies.	12 representatives of different sector actors contributed to the various peer review stages of the work.
More than 80 participants in APF'15 (researchers, policy-makers and industry participants).	APF'2015 was attended by more than 100 participants. The conference gathered increased interest.
WPK 3.4: R & D, Innovation & Standardisation	
Support at least 10 key sector actors involved in EU funded R & D programs (H2020) in the area of NIS in defining priorities.	4 meetings of the respective expert group were organised in 2015. On average, more than 10 sector actors' representatives' participated in each one of them.
Engage at least 5 MS representatives from at least 3 MSs in the work of the ETSI CEN CENELEC Cyber Security Coordination Group (CSCG).	5 representatives from 3 MSs' national standardisation authorities contributed to this work and the various meetings of the expert group.
Engage at least 5 MS representatives through at least 1 workshop organised in collaboration with the research (H2020) and standardisation communities.	ENISA organised 1 workshop in October 2015 attended by over 20 participants. On average more than 5 MS representatives attended the workshop.

1.3.6 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, Impact Indicators	**Achieved results**
WPK 3.1: Provide information and advice to support policy development	
D1: Analysis of standards related to eID and/or TSPs (report, Q4, 2015)	Analysis of standards related to Trust Service Providers — Mapping of requirements of eIDAS to existing standards, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp_standards_2015
D2: Report analysing the terminology and definitions used by eIDAS (including recommended technological means used by TSPs) (report, Q4, 2015)	Qualified Website Authentication Certificates, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/qualified-website-authentication-certificates/
WPK 3.2: Assist EU MSs and Commission in the implementation of EU NIS regulations	
D1: Analysis of Annual 2014 Incident Reports (report, Q3, 2015)	Annual Incident Reports 2014, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2014
D2: Recommendations on addressing root causes of specific incidents (report) (Q3, 2015)	(1) Guideline on Threats and Assets. Technical guidance on threats and assets in Article 13a, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/technical-guideline-on-threats-and-assets (2) Security incidents indicators — measuring the impact of incidents affecting electronic communications, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/studies/security-incidents-indicators
(Security incidents indicators — measuring the impact of incidents affecting electronic communications)	This deliverable was postponed according to the decision MB/2015/6 WP where WP15 is amended.
D3: Guidelines on Minimum Security Measures for Trusted Service Providers (workshops, report, Q4, 2015)	Impact evaluation on the implementation of Article 13a incident reporting scheme within EU, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/studies/impact-evaluation-article13a
D4: Impact assessment on the effectiveness of incident reporting schemes (e.g. Art. 13a); (Q4, 2015)	Proposal for Article 19 Incident reporting. Proposal for an Incident reporting framework for eIDAS Article 19, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/article19/technical-guideline-for-incident-reporting
WPK 3.3: Assist EU MSs and Commission in the implementation of NIS measures of EU data protection regulation	
D1: Readiness analysis for the adoption and evolution of privacy enhancing technologies (Q4, 2015)	Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pets
D2: Building blocks for PETs update (Q4, 2015)	Deliverable Approved. Following agreement with the ENISA MB the deliverable will not be published but only be distributed to the members of the ENISA MB.
D3: Annual Privacy Forum 2015, APF'2015 (Q4, 2015)	APF2015 was successfully organised in October 2015, https://www.enisa.europa.eu/media/news-items/2015-annual-privacy-forum-focusing-on-privacy-enhancing-technologies. The post proceedings are in print with Springer.
D4: State-of-the-art analysis of data protection in big data architectures (Q4, 2015)	Privacy by design in big data, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/big-data-protection
D5: 2015 edition of the annual report on 'Indicative list of appropriate cryptographic protection measures' (Q4, 2015)	Deliverable approved. Following agreement with the ENISA MB the deliverable will not be published but only be distributed to the members of the ENISA MB.

WPK 3.4: R & D, Innovation & Standardisation	
D1: Good Practice Guide for aligning Policy, Industry and Research (Q4, 2015)	Governance framework for European standardisation, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/policy-industry-research
D2: Standardisation Gaps in Cyber Security (Q4, 2015)	Definition of Cybersecurity — Gaps and overlaps in standardisation, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/standardisation-gaps-in-cybersecurity
D3: Guide to standardisation for the SME Community (Q4, 2015)	Information security and privacy standards for SMEs, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/standardisation-for-smes

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

In 2015, ENISA continued in its efforts to build up targeted NIS communities to meet policy goals. In some cases (e.g. The NIS Platform, as referenced by the EU Cyber Security Strategy), ENISA supported other institutions in creating such communities, whilst in other areas sought to build such communities itself when requested to do so by the Commission or the MSs.

ENISA built on the work it had carried out in the area of the pan-European exercise and supported the TRANSITS training in the area of CSIRTs in order to build communities through a 'learn by doing' approach.

The following work packages constitute this Strategic Objective:

WPK 4.1 — Support for EU cooperation initiatives amongst NIS –related communities in the context of the EU CSS
This WPK is aimed at leveraging the positive experience of ENISA in supporting CSIRTs, the CSIRT communities and Law Enforcement communities to come up with mutually satisfactorily ways to collaborate in NIS.

WPK 4.2 — European cybercrisis cooperation through exercises
This WPK sought to facilitate the planning of the next pan-European Cyber Exercise in 2015-2016. ENISA further enhanced its methodology, training outreach and technical capability to organise large-scale cybercrisis exercises.

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

ENISA leveraged its experience in supporting the CSIRTs, the CSIRT communities and Law Enforcement communities to enhance collaboration between these actors.

As such, ENISA developed and provided guidance based on good practice for cooperation between key stakeholder communities (CSIRTs, CIIP community, Law Enforcement, Financial Services; Data Protection, etc.). 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 leveraged its experience in supporting the CSIRTs, the CSIRT communities and Law Enforcement communities to enhance collaboration between these actors.

ENISA also continued its support to the collaboration between CSIRT and law enforcement communities, which were based on the recent policy and technical developments in this area in MSs. This work also included a close collaboration with other institutions active in the 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 more operational and systematic flows of information between CSIRTs and law enforcement communities, the exchange of specific knowledge and expertise, the elaboration of general situational reports, reports resulting from strategic analyses and good practice, strengthening capacity building through training and awareness raising in order to safeguard network and information security at the EU level.

For better coordination and in order to avoid overlaps ENISA was engaged in the EC3 programme board. The well-established and jointly organised ENISA-EC3 workshop continued during 2015.

1.4.2 WPK 4.2: European cybercrisis cooperation through exercises

The activities of 2015 were focused on the following areas:

- pan-European cyber-exercises management;
- enhance the capacity to support and organise cyber-exercises;
- promote maintain and improve EU cybercrisis cooperation plans and procedures, e.g. the EU Cyber Standard Operational Procedures (EU-CSOPs), and bring closer the cybercrisis cooperation community.

Pan-European cyber-exercises management

In 2015 ENISA performed an in-depth analysis of the evaluation data gathered from the Cyber Europe 2014 exercise. This resulted in a detailed evaluation report with 33 discrete follow up actions that was shared with the participating countries.

In addition, in 2015 ENISA kicked off the planning of the next pan-European cyber-exercise, Cyber Europe 2016. The lessons learned from Cyber Europe 2014 were used to drive the plan for the new exercise in 2016; in particular the upcoming exercises will include an enhanced programme of different learning opportunities, including training and small-scale focused exercises, in addition to the main large-scale exercise event.

Enhance the capacity to support and organise cyber-exercises

ENISA further improved its methodology as well as seminar and trainings hand-outs, as well as its technical capabilities for the organisation and management of large-scale cybercrisis exercises.

The Agency built yet further its capability to organise and manage complex, distributed exercises. New tools and methods were introduced while the Agency also facilitated strategic partnerships. The development of an advanced tool for managing exercises, the Cyber Exercise Platform (CEP), was one of the main achievements in 2015.

International cybersecurity exercises

In 2015, ENISA analysed the options for a potential joint cyber-exercises with non-EU countries and international organisations. ENISA discussed with the EU and EFTA countries the options for such joint initiatives in order to plan the roadmap of future exercises. The strategic decision for joint initiatives with non-EU or international organisations will be taken by ENISA's Management Board. The report on the potential, future, joint exercises was submitted to ENISA's Management Board as the one of the input documents in this strategic decision-making process.

Promote, maintain and improve EU cybercrisis cooperation plans and procedures, e.g. EU Cyber SOPs, including bringing closer the cybercrisis cooperation community.

ENISA continued to support EU countries in the maintenance and training of operational procedures for cybercrisis cooperation. ENISA analysed the EU cross-border cybercrisis cooperation procedures and plans, with inputs from previous efforts, such as cyber-exercises, and other related reports. Also ENISA continued to work with all EU MSs on the actions, plans and tools needed for improving the cross-border cooperation and proposed mechanisms for a possible implementation, closely involving MSs.

ENISA continued its efforts to bring the cybercrisis cooperation community closer in order increase the trust building to increase synergies. To that end in 2015 ENISA studied the EU-level structures on crisis management in different sectors, such as aviation, health, etc., in order to learn from their good practices. The report published identifies recommendations with which the ICT sector (cyber) can improve at an EU-level the response to major cyber-incidents (also known as cybercrises).

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: Support for EU cooperation initiatives amongst NIS-related communities in the context of the EU CSS	
At least 2 new operational communities will be identified and contacted for the purpose of identifying mutually satisfactory ways to collaborate (CSIRTs, LEA, EU Financial service, Data Protection, CIIP community, etc.)	In 2015, Aviation and ATM communities were identified and contacted to set up cooperation in the incident response area. In addition, LEA and CSIRT communities were involved in a project to address a common taxonomy for those communities in order to advance the mutual way of collaboration.
By 2016, at least 15 MSs are familiar with practices in addressing different sector regulation challenges of managing cybersecurity issues.	In 2015 the first step was taken — ENISA published a report on Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches. The contribution to the report was done in cooperation with the ENISA NLO network from all 28 MSs.
WPK 4.2: European cybercrisis cooperation through exercises	
At least 25 EU MSs and EFTA countries confirm their support for pan-European Cyber Exercises.	In total 29 EU and EFTA countries are participating in the planning process of Cyber Europe 2016.
At least 25 MSs are familiar with and use the cross-border cybercrisis EU Standard Operational Procedures by 2016.	All countries involved in the Cyber Europe series of exercises are familiar with the cybercrisis cooperation SOPs.

Copyright ©Shutterstock

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, Impact Indicators	**Achieved results**
WPK 4.1: Support for EU cooperation initiatives amongst NIS–related communities in the context of the EU CSS	
D1: Develop and provide guidance based on best practice for cooperation between key stakeholder communities (Trust building for and reaching out to new communities) (CSIRTs, CIIP community, Law Enforcement, Financial Services; Data Protection, etc.) (Q4, 2015)	1. Information sharing and common taxonomies between CSIRTs and Law Enforcement, https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement/at_download/fullReport; 2. Update on CSIRT baseline capabilities,https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/csirt-capabilities/at_download/fullReport
D2: Identify practices of Member States in addressing different sector regulation challenges of managing cybersecurity issues (Q4, 2015)	Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches, https://www.enisa.europa.eu/activities/cert/support/information-sharing/cybersecurity-information-sharing/at_download/fullReport
WPK 4.2: European cybercrisis cooperation through exercises	
D1: Evaluation Analysis and Actions from CE2014 (restricted report) (Q2, 2015)	The restricted version shared with EU MSs includes lessons learned from the 2014 pan-European Exercises, including 33 actions to follow up on, in order to improve the cybersecurity preparedness in the EU. A public version is available online at ENISA's website: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014
D2: Pan-European Cyber Exercises Roadmap for CE2016 (restricted report) (Q4, 2015)	The deliverable is limited, shared with ENISA MB on November 2015.
D3: Joint exercises with non-EU-EFTA countries and International Organisations (restricted report) (Q4, 2015)	The deliverable is limited, shared with ENISA MB on November 2015.
D4: Evaluation and recommendations for improved communication procedures between EU Member States (public/restricted report) (Q4, 2015)	Common practices of EU-level crisis management and applicability to cybercrises, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/eu-level-crisis-man/at_download/fullReport

1.5 HORIZONTAL ACTIVITIES. ACTIVITIES AND KEY RESULTS

1.5.1 Management Board, Executive Board & PSG Secretariat

This section addresses activities that are required to support ENISA's formal bodies, the Management Board (MB) and the Permanent Stakeholders Group (PSG) as well as Executive Board in their functions.

For the MB, 1 ordinary meeting was organised in 2015. Also, 5 informal meetings were held with the MB members who volunteered to contribute to the drafting of the annual work programme. The existing electronic newsletter continued throughout 2015 as support for the MB Portal. For the PSG also, 2 formal meetings were organised. To facilitate the exchange of views, 3 PSG members were nominated by the Group to be present at the informal meetings with the MB members.

For the Executive Board, formal meetings were organised during 2015, also by using the teleconferencing facilities.

1.5.2 National Liaison Officer Network

Since 2014, ENISA initiated a number of activities with the aim to strengthen cooperation within the National

Liaison Officers' (NLO) Network. NLOs are key actors for the Agency's daily work and interaction, assuring in terms of outreach effective liaison to the MSs and dissemination of ENISA activities. It expands the NLO-Network with contact points from governmental and public agencies/organisations (e.g. CSIRTs and Regulatory Bodies/Agencies, etc.).

In 2015, ENISA built upon these efforts and improved its cooperation with the NLO Network, the first Point of Contact for ENISA in the MSs. In particular, the Agency continued working on the following actions:

- an NLO meeting was organised on 4 March 2015, in which improvements of the collaboration were discussed;
- the NLO terms of reference were published on the ENISA website, clarifying the role of NLOs;
- information was sent to the members of the NLO network at regular intervals on upcoming ENISA project related tenders, vacancy notices, and events organised by ENISA or where the Agency contributes (e.g. co-organiser, etc.);
- organisation of 1 ad hoc meeting on a specific topic was identified in collaboration with the NLOs (visit of Dutch Delegation from NCSC);
- all relevant information on active ENISA projects (e.g. unit responsible for the project, relevant tender results, etc.) was sent to the network;
- a new section on the ENISA website, called 'Events from the Member States' was created in 2015. This section provides information on NIS events of international interest, taking place in EU and EFTA Member States. This section is based on information sent by NLOs.

1.5.3 Stakeholders' engagement: Key ENISA Events

Throughout 2015, ENISA restructured its engagement with its stakeholders, focusing on two important lines addressed to NIS Industry leaders and high level policy and business representatives. Additionally, ENISA explored the possibility of presenting compelling NIS-related themes in a different format by organising a thematic conference. Activities in this area included:

1.5.3.1 Industry Event 2015

Among ENISA's strategic goals is to enhance community and capacity building in Europe (1). For this reason, ENISA organised a workshop with the European IT security industry, on 8 July, in Brussels.

The primary goal of this event was to engage industry in a dialogue on how to best serve their needs in a rapidly changing threat environment, while focusing on policy implementation issues.

This event brought together key industry decision-makers in order to (a) explain the strategic vision of ENISA and how the Agency works with the private sector to achieve impact and (b) get industry feedback on their expectation and on how to create impact and continuously improve the Agency's output.

The workshop was structured around several information exchange sessions and a panel debate. In the information exchange sessions, ENISA informed EU industry representatives of the work it is doing and solicited their opinion on how well this meets their requirements. The debate evolved around the topic of how the Agency could help industry to be more secure in an economically optimal fashion.

Due to the success of the event, a follow up event will be organised in 2016 around two key themes of interest for Industry.

1.5.3.2 ENISA High Level Event 2015

In 2015, the ENISA's High Level Event (HLE) was the main networking event of the Agency and it took place in Brussels, on 9 November.

The ENISA HLE seeks to bring together key stakeholders of the Network and Information Security field, policy-makers and subject experts, including top-level representatives from the Commission, Member States, Industry and Academia. By interacting with the C-layer of its stakeholders, ENISA seeks to collect input to improve and expand its delivery and outreach. By bringing together representatives from all of ENISA's stakeholder communities, HLE15 provided an appropriate platform for discussing the key challenges that the Agency is likely to face in the next 5-year period and for defining the first set of priorities.

Panel discussions explored three themes which are widely being discussed among policy and NIS circles: 'Cybersecurity at the Service of Industry', 'Aligning Cybersecurity Goals with Democratic Principles', and 'Identifying Challenges and Priorities for NIS in Europe'. Key participating figures included Commissioner Günther H. Oettinger who gave the keynote speech on the EU Perspective on key cybersecurity policy objectives, representatives from the Luxemburgish Presidency, DG Justice, European Cyber Crime Centre, eu-LISA, ANSSI and Digital Rights Ireland, among others.

1.5.3.3 Cyber Security & Privacy Challenges for Law Enforcement (CySPLE15)

On 18-19 May 2015, ENISA and the Heraklion Chamber of Commerce and Industry (HCCI) jointly organised a 2-day conference on the theme of Cyber Security and Privacy Challenges for Law Enforcement. This conference brought together experts from policy, industry and academia on a unique opportunity to exchange views on current EU policy issues and initiatives that intersect cybersecurity, privacy and law enforcement. Current and emerging technologies were analysed from an application, organisational and legal view point in the wake of new compliance requirements. Cross-border cooperation, exercising rights, and exchanging information, in the EU and beyond, was emphasised throughout this conference. In addition the Agency featured in the HCCI publication providing its recommendations to SMEs on cloud services. Beyond operational goals, CySPLE15 was a good example of the Agency collaborating with a local authority in its Seat.

1.5.4 EU Relations

Part of the Agency's horizontal activities include its relations within the sphere of EU institutions and bodies notably with the European Commission, the European Parliament, as well as contacts within Member States to promote NIS policy. ENISA's Executive Director and Head of Core Operations led the activities at the political and industry level respectively, with the support of the relevant departments. The press-media office also contributes actively by providing communication support, input and the appropriate vehicles to disseminate the Agency's work in cybersecurity to the relevant stakeholders and citizens. This includes its work on:

- supporting the Commission initiatives n the Digital Single Market (DSM) for Europe;
- supporting the first EU wide cybersecurity Directive (NIS);
- support for the European Commission Public Consultation on 'Contractual PPP' launch of a public consultation, around the Public-Private Partnership as an important step towards securing the Digital Single Market, by welcoming the initiative and inviting its stakeholders to contribute.

Within this framework, activities in field included the Executive Director participating in the following events:

- the EPP Hearing on data driven security, on the 1st July 2015, at the European Parliament in Brussels;
- on 23 June 2015, at the IMCO Committee meeting in Brussels, in an exchange of views on the public interest information platform of the Universal Service Directive;
- the SEDE (Security and Defence) subcommittee meeting in Brussels, on 16 March 2015 in an exchange of views on cybersecurity and defence;
- the 4th meeting of the Working Group on Digital Union of the ITRE Committee on cybersecurity at the European Parliament (EP) in Brussels. Prof. Helmbrecht spoke to the Working Group about ENISA's role in 'securing and enabling Europe's information society', focusing on the Agency's work with Europe's Computer Security Incident Response Teams (CSIRTs) and the facilitation of pan-European cyber-exercises;
- the European Parliament high-level conference in Brussels, jointly organised by the Civil Liberties Committee (LIBE) and the Luxemburg Presidency of the Council of the EU, co-chaired by the IMCO and ITRE Committees, which debates the protection of online privacy by enhancing IT security and strengthening EU IT capabilities. ENISA welcomed the separately discussed policy areas of stimulating the adoption of privacy enhancing technologies (PETs), addressing software and hardware vulnerabilities and the internet infrastructure as well as developing the EU potential for a strong and vital IT industry. ENISA hopes for a stimulating effect of the conference in the political debate on these closely linked policies;
- the Chatham House Cyber 2015 meeting on 'Security, Privacy and Competing interests';
- the 2nd High Level Conference on EU Cybersecurity, organised by the European Commission, on 28 May 2015, in Brussels. The event focused on making the EU an industrial leader in trustworthy ICT; building capacity to fight cybercrime and strengthen cybersecurity in the EU and beyond; and achievements of the EU Cybersecurity Strategy, the challenges and opportunities ahead;
- the 10th Future Security Conference. The event hosts high-level panellists mainly from ministries, institutions and academia. ENISA's Executive Director Prof. Helmbrecht delivered the keynote address on 'Privacy and Data protection: an EU Perspective', where he mentioned the latest developments in the area and spoke about how the Agency has become a point of reference on eIDAS;
- the 19th Security Conference on Telecommunications and IT Security in Warsaw on the 14-15 October 2015, at the Copernicus Science Centre, Warsaw. ENISA was an honorary patron of this year's event. Prof Helmbrecht spoke about cybersecurity standards giving an insight from the EU perspective and ENISA's role;
- the Cyber Cooperation Summit in New York. Along with representatives from the public and private sectors, Prof. Helmbrecht spoke on the panel 'Is Cooperation Possible in Cyberspace?' discussing the challenges to protecting critical assets from cyber-attacks at a global level while minimising threats to IT security;
- the panel discussion on 'Accelerating Digital Innovation for Social Impact' at ITU. Prof. Helmbrecht spoke on the need for a close collaboration between policy initiatives and technology innovation, providing notable examples of areas which offer such a potential, and elaborated on how the EU needs an industry policy approach to create a competitive EU based ICT industry which can be based on a variety of different tools;
- talking to decision-makers at the Deutschland sicher im Netz e.V event on 3 November 2015, referencing ENISA's multi-stakeholder approach. Helmbrecht recommended cooperating with public authorities at the state level in order to 'create synergies between existing programs and objectives', for example with national data protection authorities, regulatory bodies and academia.
- At the main forum at the Omnicard event in Berlin on 21 January, 2015, on the panel on 'Secure identities — an effective tool to increase information security?'. ENISA's work 'Framework on how to evaluate National Cyber Security strategies' also featured on the Omnicard website. The report, addressed to policy experts and government officials who design, implement and evaluate an NCSS policy, is strongly aligned with the EU Cyber Security Strategy (EU CSS) aiming to assist Member States in developing capabilities in the area of NCSS.
- the agency also hosted visits at its premises, including a 2-day visit by an EP ITRE (Industry, Research and Energy) delegation, Michal Boni MEP, and Eva Kaili MEP, at its premises in Heraklion on 24-25 September 2015. The programme of their visit included a: (i) brief presentation on ENISA and the agency's mission and scope of its activities; (ii) presentation on flagship and major agency projects including secure and smart infrastructures, cloud computing, national cybersecurity strategies, incident reporting, threat landscape, certification, privacy and data protection, and supporting EC policy processes. In each case, emphasis was placed on the impact of the work; (iii) demonstration and overview of ENISA's training activities for the EU CSIRT community and cyber-exercises; (iv) meeting with ENISA staff for an exchange of views on the upcoming challenges in the field of cybersecurity within the European context and activities.

1.5.5 Corporate Communication

Year 2015 was a challenging one for the Agency in view of the agreements on the NIS Directive, the General Data Protection Regulation (GDPR) and the announcement of the Digital Single Market (DSM) initiative by the Commission, as these are areas in which the Agency is particularly active. These landmark agreements make the Agency's work even more important within the EU in cybersecurity, and its stimulus to the internal market growth. The Agency also engaged itself this year more at the EU level, communicating on cybersecurity challenges and efforts — such as CSIRTS cooperation and training, privacy-by-design (PbD), the need for standards, for cybercooperation, awareness raising, incident reporting, data protection and privacy issues, data breach reporting, IoT security, support to private-public partnerships (PPPs) and the trending developments both at the industry and policy level. ENISA also got engaged more by participating at targeted events for the first time with its own booth at the Bitkom #hub15 event, thus establishing new platforms for dialogue and networking, while providing support and recommendations to the involved communities.

1.5.5.1 Dissemination activities

ENISA Press Office has sought to enhance its outreach in the EU increasing its presence mainly in Belgium and Germany, and also the United Kingdom and France. The result was increased coverage, editorials, articles and interviews published in top-tier online press and media outlets with the major expert media in Europe. Special emphasis was placed on messages tailored to the specific audiences for ENISA's events, projects, activities, deliverables and press presence.

In the following subsections some of the activities, events, and statistics associated with our communication activities are presented.

Publications

ENISA is active in publishing the results of its work through its reports, studies, info notes, papers and opinions, enhancing its communication and reach with various stakeholders. Additionally, ad hoc technical or policy reports, papers, and studies were produced. In 2015 the Agency published 53 deliverables as Work Programme deliverables and produced various other reports, papers and studies — including the Annual Activities Report 2014 and ENISA's Work Programme 2016.

ENISA is active in publishing the results of its work through its reports, studies, info notes, papers and opinions, enhancing its communication and reach with various stakeholders.

In 2015, ENISA's main templates were redesigned and relaunched improving significantly the look and feel and functionality. In addition, ENISA's publication process was supported with professional graphic designs, images and illustrations. In 2015 ENISA continued to identify its deliverables using the EU Publication's Office Identification numbers (e.g. ISBN, DOI) so that all deliverables are simultaneously published on the EU bookshop.

The Agency strives to make the Executive Director and select staff members available to communicate publically and provide their expertise externally to the relevant communities and to the press and media, promoting best practices and developing synergies towards a smooth cyber EU environment. Along these lines, through the press office, a large number of interviews, editorials, and articles have been made available to leading publications, media outlets and other counterparts, and the Agency is present at high level events, promoting cybersecurity from an official, respected EU

source. Furthermore a number of interviews are given in various official languages. A multilingual approach to communication remains a priority for the Agency.

1.5.5.2 Media outreach

ENISA's impact, outreach and media programme gives the Agency the opportunity to extend its reach. The Agency expanded its actions, further enhancing its media distribution and outreach, and promoting a culture of tailored targeting and cross-referencing aspects of its work and multipliers.

In 2015, ENISA:

- produced 40 press releases (doubling, compared 23 media releases in 2014) and 75 news items on the ENISA website;
- simultaneously published media releases and news items on ENISA's social media channels on Facebook, Twitter, and LinkedIn.

Cross media impact

ENISA generated 3 383 mentions in EU media maintaining its reach and impact across the EU. Directly, media releases on the ENISA website received 220 000 unique page views showing an increase, and individual news stories received around 64 183 direct hits. Figures continue to show a clear correlation between peaks in web visitors and the distribution of media releases in multiple channels, demonstrating the beneficial effect of the communication and media activity. Total readership includes an online reach of 2 378 448, 110 and 15 393,097 in print. In addition ENISA extended its reach (2) to millions of citizens — to and through key EU expert media — enhancing its reputation as experts and dialogue partners in cybersecurity.

Social media

ENISA continues its prominent engagement with the online community through its social media outlets. All ENISA activities and deliverables are communicated via social media channels, and generate increasing traffic towards the Agency website, activities, events and deliverables. In addition, they are incorporated in the Agency's communications (publications, presentations, emails, brand material, etc.). In particular, social media monitoring reports show an increased reach through ENISA's channels. Key accomplishments for 2015, include:

- The ENISA Twitter channel features 9 300 followers (6 000 in 2014), generating over 4 000 tweets.
- The ENISA LinkedIn page features 5 800 followers.
- The ENISA YouTube channel contains 51 videos posted.

Digital media

The ENISA website continues to be the Agency's main communication channel, enhancing its presence. In 2015, the website received more than 3 000 000 unique page views.

Technical improvements in 2015 include initiating the development of a new online environment for ENISA's website with the joint collaboration of staff members across all ENISA's units.

The Agency is making continuous efforts for the improvement of its website with usability studies and regular updates in order to make it more user friendly and reach citizens more effectively. Against this background the Agency's website layout and information architecture have been redesigned to further improve ease of navigation, usability and end-user experience. The new site is contemporary, responsive and has a dynamic fast-paced architecture providing access to ENISA's Work Programme, latest reports, events, projects, publications and audiovisual material. The new website is expected to go live early in 2016.

ENISA Portals — used by specialist expert communities — have also been redesigned to improve end-user experience, while a number of new web tools have been introduced or updated to support ENISA's activities.

Furthermore, the structure of the Agency's three mini-sites in French, German and Greek continue to support and attract visitors. In addition, the dedicated portal for the European Cyber Security Month was redesigned and enhanced further with new content and functionalities promoting the ECSM initiative and its growing community.

Audio-visual material

In 2015, 3 videos were produced to communicate the Agency's activities.

- ENISA's Cyber-exercise team created a video providing a peek into Europe's biggest cyber-exercise;
- ENISA's CSIRT team created a 'train the trainers' video introducing and demonstrating the teams' work and training resources for the Member States.

Additionally, 3 videos were produced for internal communication purposes.

In addition the Agency's departments produced infographics and posters on the topics of their work, aiming to improve the visibility of the Agency's work and key facts and disseminate messages. These include:

- ENISA PETs (privacy enhancing technologies) poster;
- Posters and infographics on ENISA's work on Critical Information Infrastructure protection;
- National Cyber Security Strategies Infographic;
- ENISA Cyber Security Exercises and Training posters;
- ENISA Threat Landscape 2015 Infographic;
- 4 new posters on cybersecurity education and awareness.

1.5.5.3 Additional outreach activities

ENISA actively continued its participation in events, increasing visibility, involvement, recognition and awareness at a local, national or EU level through:

- Europe Day activities with ENISA staff members visiting schools in Athens and Heraklion for a 'Back to school' session, giving the opportunity to students to learn more about the Agency's work in cybersecurity for Europe. The Agency also hosted an interactive seminar session on trending cybersecurity topics for representatives of embassies, the Hellenic Authority for Communication Security and Privacy (ADAE), local authorities, academia and educators. The press office for the occasion collected awareness-raising material on cybersecurity which as available online on ENISA's website including posters, videos, recommendations, infographics and games. Relevant branding material was also produced and distributed.
- The European Cyber Security Challenge initiative with organisations from six countries. The competition is an opportunity for participants, who are not IT professionals, to test and put their digital skills at work, and also acts as a platform for the exchange of good practices among contestants, and to motivate young people to enhance and further develop their skills to tackle online threats. In 2016 the event is supported by ENISA.
- Hosting visits from EU schools, providing the opportunity to meet with staff and experts, bringing educators and students closer to the EU activities on cybersecurity and seeing the EU Agency from within, meet staff and follow presentations on ENISA's work and awareness on cyberthreats.
- An event for the presentation of the new — to be — School of European Education (SEE) in Heraklion hosted at its premises on 30 April a welcoming party of around sixty participants including teachers and parents from the SEE, and representatives from Heraklion Municipality, of the School Buildings Organisation and of the new Regional Director of Education in Crete.
- Supporting NIS experts in the production of the successful series of 'Info Notes' activities where short, expert reports provide a pragmatic analysis on trending security issues and themes. The activity has proven to be an important tool which stakeholders turn to for reliable information on security issues.
- The News from the Member States activity, a request of the NIS community, covering the latest technical cybersecurity updates from EU Member States aiming at increasing interaction within the specific community.
- The organisation of an information security workshop (Infosec) in Athens in September 2015. This invitation-only event welcomed participants from EU Agencies such as Europol, CEPOL, BEREC, ECHA, eu-LISA, Cedefop, EFCA, OHIM, ERA, EEA, EMSA, FRONTEX, FRA, IMI, EIGE, the Translation Centre of the European Bodies, and FCH. The workshop aimed at providing valuable insights on information security at the highest operational level. ENISA experts gave an overview on the cyberthreat landscape, risks and considerations for cloud platforms, as well as an inside look at ENISA's technical trainings and the Cyber Europe Exercises.
- Hosting workshops and visits such as that of the: (i) German Ministry of Interior on areas of shared interest, such as critical information infrastructure protection, threat landscape, data protection and others. The discussion revealed opportunities for further cooperation between the two organisations especially in policy implementations where ENISA has significant experience at an EU level;

(ii) COINS Research School of Computer and Information Security summer school;

(iii) E-CODEX representatives, a Europe-wide project aiming at improving the cross-border access of citizens and businesses to legal means, as well as increasing the interoperability between legal authorities within the EU; (iv) ENCYSEC, a pilot project with the overall objective to increase the security and resilience of information communication technologies networks in the beneficiary countries by building and training local capacities to adequately prevent, respond and prosecute cyber-attacks and/or accidental failures; (v) a joint workshop with the European Banking Authority (EBA) on the use of cloud computing in the finance sector in London in October 2015; (vi) a joint workshop with EC3 between CSIRTs and law enforcement.

- An array of varying activities was organised that included the EU Agencies Network coordination, ENISA Christmas activities for staff and families, and various internal coordination activities in such areas as strategy, organisational culture and team building.

1.5.6 Quality Management System and Project Office

The Quality Management System (QMS) of the Agency aimed at responding to a mix of regulatory and stakeholder requirements for operations mostly, in an effort to improve organisational performance and compliance. Scheduled annual activities have aimed at the promulgation and maintenance of standard operating procedures (SOPs) and a methodology that supports the operational processes of the Agency. The primary goal of the documented QMS in 2015 was to improve performance across the Agency, while reducing operational costs and enhancing stakeholder satisfaction. Implementing SOPs has been a priority in order to increase operational efficiency. Good examples of SOPs that had a tangible impact in improving efficiency and effectiveness include: the SOP on the Review and Publication of Deliverables, the SOP on handling Article 14 requests, etc.

The ENISA Project Office supported the smooth promulgation of the annual work program of the Agency coordinating an array of contributors among Agency staff and its MB, PSG and the Commission. Additionally the Project Office's work entailed responding to about 150 individual requests for ad hoc contributions to management work such as briefings on cross-cutting themes, coordinating the coherence of recommendations across the Department, etc. In 2015, the editing and production of the Annual Activity Report 2014 was coordinated by the Project Office team.

1.5.7 Article 14 Requests

Article 14 requests are an instrument that allows the MSs or EU institutions to make direct requests to ENISA for carrying out particular activities. This mechanism has become increasingly valuable and it has grown in significance to the extent that the Agency believes that it needs to be explicitly planned for in the annual work programme.

The following table provides an overview of the Article 14 requests in 2015 compared to those in 2014.

	2014	2015	% Change
Number of new requests	12	23	+92 %
Number of requests in progress	19	19	-
Number of requests completed	15	14	-7 %
Number of requests received 2015 to be initiated 2016	3	10	+233 %
Effort in person days	408	278	-32 %
Effort in Euros (FTE [1] including overhead) [2]	EUR 252 054	EUR 156 684	-38 %
Direct Cost [3]	EUR 65,583	EUR 54 273	-17 %
Total Cost	**EUR 317 637**	**EUR 210 957**	**-34 %**

1 Mean full time equivalent (FTE) costs are calculated on the basis of the total budget consumption over 201.6 actual working days p.a., to support salaries and overhead for staff in service in the reference year (64.7 staff in 2015 and 59.6 FTEs in 2014 including TA, CA and SNE).
2 Based on statistical analysis at the end of 2015 the use Cost of a person-day in 2015 (including overheads) is EUR 564 and for 2014, EUR 618.
3 Mission costs and other direct expenses linked to request are included in this budget estimate.

The table of requests outlines all current ongoing requests. The relevant requests for 2015 report (10 requests that will be covered during 2016, 14 completed requests, 4 ongoing requests and 1 declined request).

	Origin	Institution	Title	Due Date
1	Belgium	CERT.BE	CERT.BE training request	To be initiated in 2016
2	Cyprus	Cyprus — Office of the Commissioner for Electronic Communications and Postal Regulation	Participating in the pilot step-by-step guide, best practices of national risk assessments for cybersecurity	Complete
3	Czech Republic	Czech CERT Team	Request for training Czech national CSIRT team	To be initiated in 2016
4	Estonia	The Estonian Information System Authority	Request for training	To be initiated in 2016
5	Estonia	Information System Authority of Estonia	Request for training course Estonia	Complete
6	European Union	CEPOL European Police College	Request for CEPOL	Complete
7	European Union	Council of the European Union	Request for assistance under Article 14 of Regulation (EU) No 526/2013; policy framework for the Council's Public key Infrastructure	Complete
8	European Union	European External Action Service	Request from EEAS for ENISA to participate in various NATO exercises	In progress
9	European Union	European External Action Service	Cyber Capacity Building	To be initiated in 2016
10	European Union	European Commission	Contribution and advice on revising the regulatory framework on electronic communication	To be initiated in 2016
11	FYROM	FYROM Agency for Electronic Communications	Request for cooperation	Declined
12	Germany	Klinikum Munich	Request for follow up Article 14 — eHealth security project	In progress
13	Germany	Federal office for Information Security (BSI)	BSI request for workshop on Security Certification	To be initiated in 2016
14	Germany	Federal office for Information Security (BSI)	Co-operation in the area of privacy	In progress
15	Greece	Hellenic National CERT	Hellenic National Cert training request	To be initiated in 2016
16	Greece	Hellenic Ministry of Interior	Request for training Hellenic Ministry of Interior	To be initiated in 2016
17	Greece	Centre for Security Studies	Request for training KEMEA	Complete
18	Greece	The Hellenic Authority for Communication Security and Privacy	ADAE Training courses	Complete
19	Latvia	University of Latvia	Request for training from University of Latvia	Complete

20	Latvia	Ministry of defence	Workshop on Legal Aspects of Cloud Computing Security	Complete
21	Lithuania	Ministry of defence CSTS	Training request	To be initiated in 2016
22	Luxembourg	Presidency of the Council of EU	Support & Cooperation on Responsible disclosure and EU /International cyber-exercises calendar	Complete
23	Malta	Cabinet office of the Prime Minister	Request to enhance capabilities of Malta's CIP Directorate	Complete
24	Malta	Malta Information Technology Agency	Request assistance in establishment of Malta National Cyber Security Strategy	Complete
25	Poland	Polish National Police	Training Polish National Police	To be initiated in 2016
26	Poland	NASK	Polish government request to build cybersecurity governance model	Complete
27	Spain	National Security Department — Spanish Prime Minister's Office	Request for seminar on NCPs and National Exercises	In progress
28	Spain	National Security Department — Spanish Prime Minister's Office	Request from Spain, study on Cyber Security Exercises	Complete
29	United Kingdom	British Embassy in Athens	Training request	Complete

1.5.8 Data Protection Officer

The main tasks of the Data Protection Officer (DPO) included:

- informing and advising ENISA of its obligations pursuant to Regulation 45/2001/EC;
- monitoring the implementation and application of ENISA's policies in relation to the protection of personal data;
- monitoring the implementation and application of Regulation 45/2001/EC at ENISA, including the requirements for data security, information of data subjects and their requests in exercising their rights under the Regulation, as well as the requirements for prior check or prior consultation with EDPS;
- monitoring the documentation, notification and communication of personal data in the context of ENISA's operations;
- acting as ENISA's contact point for EDPS on issues related to the processing of personal data; cooperating and consulting with EPDS whenever needed.

On top of these tasks, in 2015 the DPO contributed to the organisation and follow up of the EDPS visit at ENISA, which supported the Agency's compliance with Regulation 45/2001/EC, as well as its cooperation with EDPS on operational matters. Moreover, the ENISA's DPO organised the 38th meeting of the EU agencies DPOs & EDPS network (approximately 70 participants), which was hosted by ENISA in Athens in November 2015.

II.

SECTION II.

MANAGEMENT OF RESOURCES

2.1 MANAGEMENT OF FINANCIAL RESOURCES

2.1.1 Budget Execution of EU subsidy (C1 funds)

In terms of budget execution, the expenditure appropriations of ENISA Budget 2015 of EUR 10 064 274, were committed at a rate of 100.00 % on 31 December 2015.

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 92.89 % in 2015 compared to 85.61 % in 2014. 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 (2014) and enabled the launch of projects related to the Work Programme in early 2015, 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 Nos 1 to 7, approved by the Executive Director (ED) of ENISA, and the Amending Budget (AB) 1/2015, approved by the Management Board, on the initial Budget 2015:

Table 1. Summary of transfers and AB 1/2015 effect:

	Initial Budget	Transfers 1-7 B2015 approved by ED	Amending Budget 1/2015	New Appropriations 2015 (AB 01/2015)
Title 1	6.039.794,90	-222.050,00	65.718,11	5.883.463,01
Title 2	1.497.600,00	-18.053,20	-68.732,65	1.410.814,15
Title 3	2.558.554,10	240.103,20	-28.660,93	2.769.996,37
Total	**10.095.949,00**	**0,00**	**-31.675,47**	**10.064.273,53**

The table below summarises the effect of the Budget transfers Nos 8 and 9, approved by the ED after the adoption of the AB 1/2015 to the final budget execution:

Table 2. Summary of transfers' effect on final budget execution:

	New Appropriations 2015 (AB 01/2015)	Transfers 8-9 B2015 approved by ED	Final Budget Execution 2015
Title 1	5.883.463,01	40.462,79	5.923.925,80
Title 2	1.410.814,15	16.682,97	1.427.497,12
Title 3	2.769.996,37	-57.145,76	2.712.850,61
Total	**10.064.273,53**	**0,00**	**10.064.273,53**

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 2015, were carried forward (automatic carry forward) to 2016 (C8 appropriations).

All commitment appropriations corresponding to the subsidy from the Greek Government for the lease of ENISA premises in Greece (external assigned revenue — R0 appropriations) were paid by 31 December 2015, therefore no commitment appropriations were automatically carried over to 2016 (R0 appropriations).

The funds carried forward to 2016 (C8 appropriations) are detailed below:

Title	Total C1 appropriations carried forward to 2016
Title 1 – Staff	335.988,15
Title 2 – Administration	181.037,92
Title 3- Operations	157.494,47
Total	**674.520,54**

The total cancelled appropriations carried forward from 2014 to 2015 (C8 appropriations of 2015) but finally not paid in 2015, was EUR 80 675.08 (representing 6.05 % of the total appropriations carried forward from 2014 to 2015).

2.1.4 Types of Procurement Procedures

In 2015, a total of 47 Procurement procedures were launched, resulting in 50 contracts (19 framework contracts, 11 service contracts and 20 specific contracts awarded under Re-Opening of Competition) and 301 Purchase Orders (143 of which were issued under pre-existing framework contracts) were signed.

2.1.5 Interest charged by suppliers

During 2015, 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 2015, 69 statutory staff were employed in the Agency.

During 2015, 4 staff left the Agency, 7 vacancy notices were published and 17 staff were recruited or took up new duties within the Agency. ENISA still experiences significant challenges in attracting and holding 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) and the low coefficient factor which applies to salaries of ENISA employees in Greece.

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.

In 2015, 4 implementing rules prepared by the Commission (Appraisal of CA's, Appraisal of TA's, Working Time and Teleworking) were considered by ENISA and were sent to the Management Board for approval. These approved implementing rules provide clarification and detail on the application of the Staff Regulations which provide the legal basis for the obligations and rights of Staff members.

In 2015, ENISA engaged consultants to complete a report on cost of living and quality of life in Athens for all the years from 2011 up to 2015. Also, a number of team building activities with staff were held throughout the year to improve team spirit and the working environment. These exercises proved to be very well received by the staff and also helped to bridge the barrier created from the operation of two offices in a small agency and improved the day-to-day work through new projects which are running

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

2.2.2 Results of screening

The Agency performed the job screening benchmarking exercise for the second time for 2015. The result of the exercise, which is a snapshot of the staffing situation on end December 2015, appears in Annex A.4. It is relevant to mention that the 'Overhead', support functions, is only 21.35 % of the total statutory staff count, which is below the maximum value accepted for the Agencies that is estimated at 25 %.

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 multi-annual 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 of the financial year 2014. The recommendations issued on the report were addressed during the year.

The ex post controls of the financial year 2014 were quiet extensive. A total of 174 financial transactions were sampled and controlled representing 9.22 % of all financial transactions of the Agency and representing 70.99 % of the 2014 Agency's budget.

As a result 1 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)

At the beginning of 2015, the Agency had 1 open recommendation. During the end of January 2015, the Agency closed it. In 2016, the IAS will perform the Risk Assessment for the Agency.

2.5.2 European Court of Auditors (ECA)

The annual report of ECA on the accounts of ENISA for 2014 contained 1 important recommendation, which was open in 2012, when the Court noted a delay in performance of a physical inventory count.

The recommendation concerning the physical inventory was completed in 2014. However the asset de-classifica-

tion and disposal process, which was launched following the physical inventory count, is still ongoing.

In detail:

- the declassification exercise was done in 2014 as well as the donation of goods to public institutions in need;
- the auction exercise was completed in 2015;
- the process regarding the physical destruction/recycling of the remaining declassified items is estimated to be completed in April 2016.

The ECA's report on 2015 accounts is expected in the third quarter of 2016. The Agency expects that the Court's opinion on the true and fair presentation of the accounts as well as on the legality and regularity of the transactions underlying the accounts will be unqualified as it has been for the past 8 years.

2.5.3 Follow up of audits plans, audits and recommendations

The Agency has only 1 open recommendation regarding the workflows of financial transactions.

This recommendation was closed in the beginning of 2015 when the tool 'Paperless' was implemented (January 2015).

2.5.4 Follow up of observations from the Discharge authority

Regarding the European Parliament decision of 29 April 2015, the Executive Director of the Agency was granted the discharge in respect of the implementation of the Agency's budget for the financial year 2013.

Regarding the European Parliament decision of 29 April 2015, the closure of the accounts of the Agency for the financial year 2013 was approved.

2.5.4.1 Follow up of the 2012 discharge

The Discharge authority notes from the Court's report that regarding one comment made in the Court's 2011 report and marked as 'Ongoing' in the Court's 2012 report, corrective actions were taken and the comment is now marked in the Court's report as 'Completed'.

The Discharge authority notes furthermore that the comment made in the Court's 2012 report is now marked in the Court's report as 'Ongoing'.

The Discharge authority acknowledged that the information on the impact of its activities on Union citizens is provided on the Agency's website through the yearly publication of strategic documents including the Annual Report, as well as new communication channels such as social media.

The Discharge authority acknowledged that the Agency performed a comprehensive physical inventory count in 2013; notes that the results of the inventory count were reported within the Annual Accounts of 2013 and that the corresponding comment of the Court marked the action as 'Ongoing' because the declassification procedure for the items out of use was still pending at the time of the Court's audit.

2.5.4.2 Budget and financial management

The Discharge authority noted that budget monitoring efforts during the financial year 2013 resulted in a budget implementation rate of 94.41 % and that the payment appropriations execution rate was 86.46 %; points out that in November 2013, additional funds were approved by the Commission for the financing of the Agency's new office in Athens; notes that in this context, a total of EUR 500 000 was not committed at year-end and was carried over, following a decision by the Management Board.

The Discharge authority acknowledged that during 2013, the Agency's operational staff were relocated to Athens while its administrative staff remained in Heraklion; agrees with the Court's opinion that administrative costs could be reduced if all the Agency's staff were to be centralised in one location and encourages the Agency to prepare a strategy that would resolve this issue effectively.

2.5.4.3 Commitments and carryovers

The Discharge authority notes that the total amount of committed appropriations carried over was EUR 1 200 000, representing 13.5 % of total appropriations; is concerned that out of this amount, EUR 800 000 are Title II carry-overs, representing 59 % of Title II total appropriations; acknowledges that the EUR 500 000 referred to in paragraph 3 as well as an additional EUR 300 000 carried over for the financing of furniture and network equipment for the new office in Athens, explain the high level of carry-overs for Title II.

2.5.4.4 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 2013 have remained within the limits of the financial rules.

2.5.4.5 Procurement and recruitment procedures

The Discharge authority noted that that for the year 2013, neither sampled transactions nor other audit findings have led to any comments on the Agency's procurement procedures in the Court's report.

The Discharge authority noted that the Court made no comments in its report as regards the Agency's recruitment procedures.

2.5.4.6 Prevention and management of conflicts of interests and transparency

The Discharge authority acknowledged that the Management Board approved and signed the decision on practical arrangements for implementing transparency and confidentiality rules in October 2013 and acknowledged from the Agency that CVs, declarations of interest of the Executive Director, the Directors and the Heads of Department were fully published on the Agency's website as requested by the Discharge authority on the Agency's discharge 2012.

2.5.4.7 Comments on internal controls

The Discharge authority noted that in September 2013 the Internal Control Coordinator role (ICC) was fully deployed and addressed as a priority the implementation and subsequent closure of several recommendations made by the Commission's Internal Audit Service (IAS).

2.5.4.8 Internal audit

The Discharge authority noted that during 2012, a risk assessment exercise was conducted by the IAS in order to determine the audit priorities for the following 3 years; notes that the IAS submitted its final strategic audit plan of 2013-2015 for the Agency on 3 December 2012.

The Discharge authority acknowledged that the IAS performed a desk review audit on 'Project Management in Operations' during 2013, which resulted in a total of 5 recommendations; notes that 4 of these recommendations have already been closed while the fifth one is to be reviewed by the IAS.

The Discharge authority noted that no critical recommendations from previous IAS reports were open as of 31 December 2013; notes furthermore that the only 'Very Important' rated recommendation open at the year-end has been implemented and was awaiting to be reviewed by the IAS; points out that this recommendation relates to the application of ex post controls; calls on the Agency to inform the Discharge authority when the ex post controls are validated by the IAS.

2.5.4.9 Other comments

The Discharge authority acknowledged that 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; is concerned by the constant late payment of rent, delayed by several months, which presents business continuity and financial risks for the Agency; takes note that the Agency has commenced discussions with the interested parties in this regard; notes furthermore that to date, the landlord has accepted the delays attributed to the procedures of the Greek Government without imposing any penalty on the Agency; calls on the Agency to continue its efforts in order to mitigate the risks brought by this situation and to inform the Discharge authority on the progress.

The Discharge authority noted with concern that the Agency failed to answer the question on the cost-effectiveness and environment-friendliness of its working space; calls on the Agency to inform the Discharge authority on the measures in place.

III.

SECTION III.

ASSESSMENT OF THE EFFECTIVENESS OF THE INTERNAL CONTROL SYSTEMS

3.1 RISK MANAGEMENT

The Agency is actually using the Risk Assessment done by the Internal Audit Service in 2012.

The Risk Self-Assessment procedure was adopted in 2015. The Risk Self-Assessment will be done in 2016.

Regarding fraud prevention and detection, the Management Board adopted the Agency's Anti-fraud strategy and action plan in 2014 a specific procedure for whistle-blowing will be done in 2016.

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.

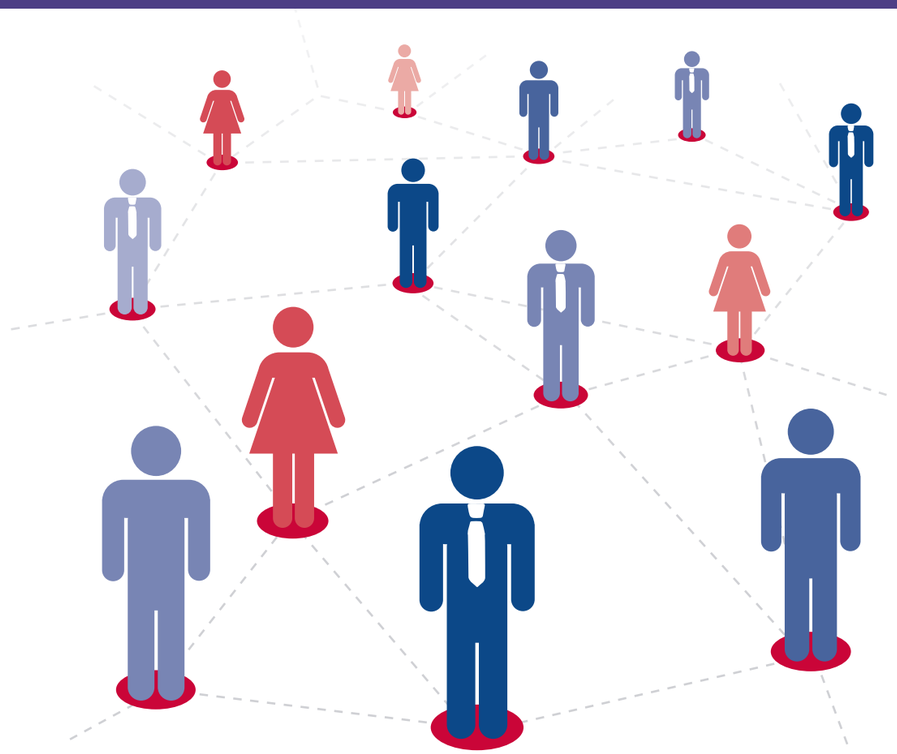
In 2014, the Agency focused on compliance with the standards that were identified as areas of concern during the risk assessment exercise, as well as on the recommendations raised by the auditing bodies (ECA and IAS). During 2015, the Agency achieved compliance with the internal control standards listed 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 2015. 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 is 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)

Work Programme and budget preparation procedures were developed in 2009 and revised in 2014. The Annual Work Programme (WP) of the Agency is developed by the Agency services, with continuous input and guidance from its two governing bodies, the Management Board and the Permanent Stakeholders Group. The WP 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 WP 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.

The Agency's Work Programmes are annual and multi-annual. The MB and the PSG give orientation and input on a regular basis throughout the WP development process as well as during the year of implementation.

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 5 consecutive years. The commitment rate of budget appropriations available for the year 2015 (C1) reached 100 %, another consecutive year in which the total Agency budget was consumed.

3.2.6 Risk management process (ICS 6)

The IAS performed a risk assessment of the Agency in 2012. Risks identified as very important during the previous audits were addressed by the Agency and actions were planned and communicated to the IAS accordingly. In 2014, effort and resources were devoted to addressing and mitigating the risks that had been identified. This satisfactorily addressed the recommendations of both the ECA and IAS, as noted in their annual reports.

The Risk Self-Assessment procedure was adopted in 2015. The Risk Self-Assessment will be done in 2016. Moreover, the Internal Audit Service will conduct their Risk Assessment in September 2016.

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.

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. This document emphasises the role and responsibilities of the Financial Verifying Agent.

The Agency proceeded in 2015 with the full 2014 ex post control exercise and will deliver the 2015 ex post control report in the first semester of 2016.

Importantly in 2014, a Quality Management System was implemented strengthening the performance management of the Agency.

The Agency has based the measurement of its performance on Key Performance Indicators (KPIs) that are applied to all areas of activity.

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 weekly and sets priorities for the actions to be taken in order to achieve the short- and medi-

um-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. Management supervision covers both legality and regularity aspects (i.e. set up and compliance with applicable rules) and operational performance (i.e. achievement of Annual WP 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.

The implementation of the project management tool MATRIX has enhanced the planning, implementation, monitoring and reporting of operational projects, and has enabled the establishment of a common project management framework across different organisational units of the Agency.

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.).

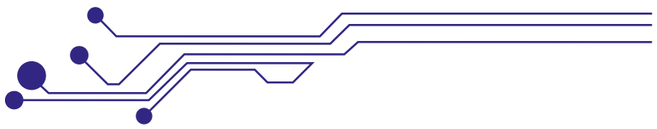
An IT Business Continuity Plan (BCP) has been developed and implemented. An Agency-wide BCP, designed to cover crisis response and recovery arrangements with respect to major disruptions, has been developed and fully implemented. The latter BCP identifies the functions, services and infrastructure that 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.

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 new application, 'Paperless', which routes documents to staff involved in preparation, review and approval of all kinds of work related documents and transactions.



As regards the financial and administrative workflows, ENISA adopted in January 2015 a new 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.

The application 'Paperless' was a breakthrough in ENISA day-to-day operations, as it heavily contributed to streamlining processes, reducing paper circulation (green office), reducing courier costs between the two offices (Athens and Heraklion), reducing time needed for repetitive administrative tasks and significantly reducing archive space and management.

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 Administration and Support 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.

3.2.16 Internal Audit Capability (ICS 16)

The Head of the Administration and Support 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.

In line with the Strategic Audit Plan 2014-2016, in 2014 the Internal Audit Service (IAS) carried out a control 'on the spot'. Out of 25 open recommendations in 2014, the Agency has only 1 remaining open which was closed in February 2015. 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: (1) staff that have the requisite knowledge and skills; (2) systems and procedures designed and implemented to manage the key risks effectively; and (3) no instances of ineffective controls that have exposed the Agency to substantial risk.

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

IV.

SECTION 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 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 annual work programme 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 on the next page.

	Systemic process	Activity	Performance indicator
1	Activity	Update of documents and activities reporting.	Feedback by auditors in the next application period and overall improvement of performance.
2	Performance indicator	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.

4.2 EXCEPTIONS

In 2015, the Agency recorded 21 exceptions. Only 3 are with high materiality. For one of these cases, the root of the problem was the late opening of the financial tool ABAC and one case is regarding the Greek Authorities for the payment of the rent of the Athens building (delay in receiving the funds from the Greek Authorities to pay the rent leaded to an a posteriori commitment). The last one concerned an error of encoding in ABAC which was spotted by the Financial Verifying Agent. By the time that the workflow was redone the commitment had become a posteriori.

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.

V.

SECTION 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 [1].

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, 27. 5. 2016

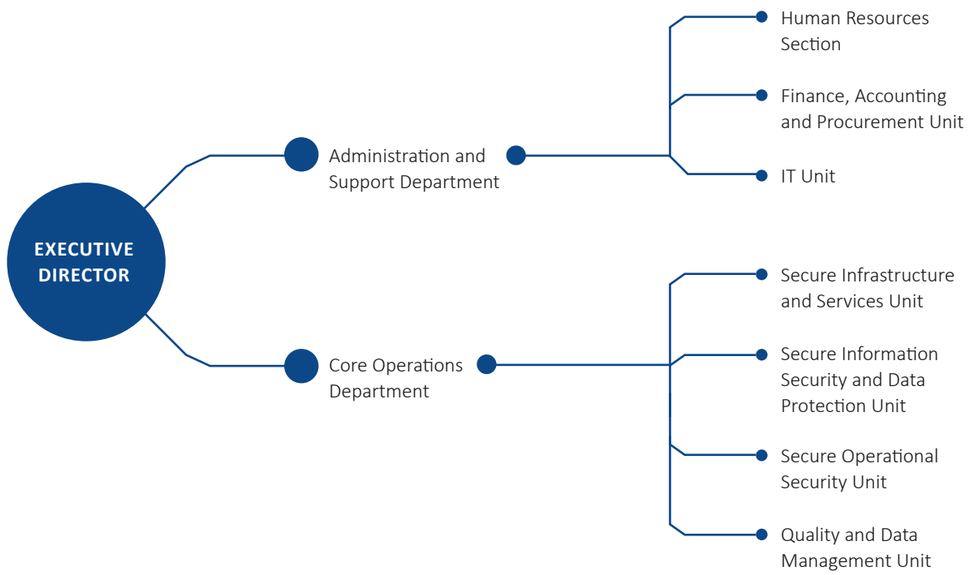
Udo Helmbrecht
Executive Director

1 True and fair in this context means a reliable, complete and correct view on the state of affairs in the service.

ANNEXES

ANNEX A.
HUMAN RESOURCES

A1 ORGANISATIONAL CHART



A2 ESTABLISHMENT PLAN 2015

Function group and grade (TA/AST)	Posts 2015 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		7
AD 7		6
AD 6		
AD 5		1
AD Total:		**32**
AST 11		
AST 10		
AST 9		
AST 8		
AST 7		
AST 6		2
AST 5		6
AST 4		3
AST 3		3
AST 2		2
AST 1		
AST Total:		16
Grand Total:		**48**
Total Staff:		**48**

A3 INFORMATION ON ENTRY LEVEL FOR EACH TYPE OF POST

Job title	Type of contract (Official, TA or CA)	Indication whether the function is dedicated to administrative support or operations
Executive Director	TA	top operations
Head of Administration and Support Department	TA	administrative
Head of Core Operations Department	TA	operations
Head of Finance, Accounting and Procurement Unit	TA	neutral
Head of Information and Technology Unit	TA	administrative
Head of Information Security and Data Protection Unit	TA	operations
Head of Operational Security Unit	TA	operations
Head of Secure Infrastructure and Services	TA	operations
Head of Quality and Data Management	TA	operations
Expert in Network and Information Security	TA	operations
Expert in Network and Information Security	TA	operations
Expert in Network and Information Security	TA	operations
Expert in Network and Information Security	TA	operations
Expert in Network and Information Security	TA	operations
Expert in Network and Information Security	TA	operations
Expert in Network and Information Security	TA	operations
Expert in Network and Information Security	TA	operations
Expert in Network and Information Security	CA	operations
Expert in Network and Information Security	CA	operations
Expert in Network and Information Security	CA	operations
Expert in Network and Information Security	CA	operations
Expert in Network and Information Security	CA	operations
Expert in Network and Information Security	CA	operations
Expert in Network and Information Security	CA	operations
Expert in Network and Information Security	CA	operations
Expert in Network and Information Security	CA	operations
Expert in Network and Information Security	CA	operations
Expert in Network and Information Security	CA	operations
Expert in Network and Information Security	CA	operations

Expert in Network and Information Security	CA	operations
Expert in Network and Information Security	TA	operations
Expert in Network and Information Security	TA	operations
Expert in Network and Information Security	TA	operations
Network and Information Security — Research and Analysis Expert	TA	operations
Network and Information Security — Research and Analysis Expert	TA	operations
Network and Information Security — Research and Analysis Expert	TA	operations
ICT Solutions Architect Expert	TA	operations
Expert in Network and Information Security	SNE	operations
Expert in Network and Information Security	SNE	operations
Facilities Management, Safety and Security Officer	SNE	administrative
Expert in Security Tools and Architecture	TA	operations
Expert in Security Tools and Architecture	TA	operations
Senior ICT Systems Officer	TA	administrative
Senior Procurement Officer	TA	neutral
Senior Safety and Security Officer	TA	administrative
Security and Resilience of Communication Networks Officer	CA	operations
Security and Resilience of Communication Networks Officer	CA	operations
ICT Systems Officer	CA	administrative
Software Developer Officer	CA	administrative
Legal Officer	TA	coordination
Corporate Communications Officer and Spokesman	TA	coordination
Administrative Officer to the Management Board	TA	top operations
Senior Financial Assistant	TA	neutral
Financial Assistant	TA	neutral
Financial Assistant	CA	neutral
Financial Control Assistant	TA	neutral
Finance and Procurement Assistant	CA	neutral
Project Assistant	CA	operations
NIS Assistant	TA	operations
HR Assistant	TA	administrative
HR Assistant	TA	administrative
HR Assistant	CA	neutral
Administrative Assistant	TA	operations
Administration and Internal Communications Assistant	CA	coordination
Administrative Assistant	TA	administrative
Administrative Assistant	TA	operations
Administrative Assistant to the Core Operations Department	TA	operations
Assistant to the Head of Administration and Support Department	TA	administrative
Personal Assistant to the Executive Director	TA	top operations
Facilities Management Assistant	CA	administrative
Corporate Communications Assistant	CA	operations
IT and Facilities Support Assistant	TA	administrative

A4 INFORMATION ON BENCHMARKING EXERCISE

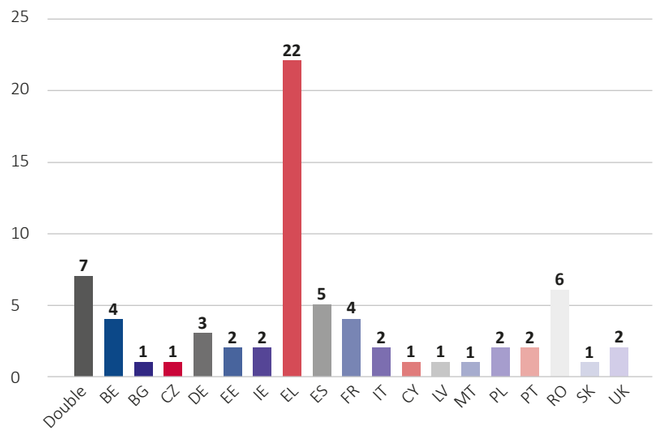
Job type	2015	2014
Total Administrative support and Coordination	**21.35 %**	**22 %**
Administrative support	17.98 %	18 %
Coordination	3.37 %	4 %
Total Operational	**66.29 %**	**68 %**
Top operational coordination	8.99 %	5 %
General Operational	57.30 %	63 %
Total Neutral	**12.36 %**	**10 %**
Finance and Control	12.36 %	10 %

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 %).

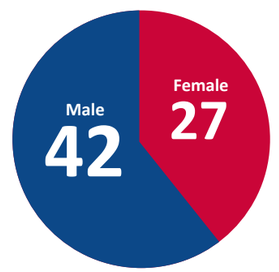
A5 HUMAN RESOURCES STATISTICS

As of 31. 12. 2015, ENISA counts 69 staff members: 45 TAs (30 ADs and 15 ASTs), 22 CAs and 2 SNEs.

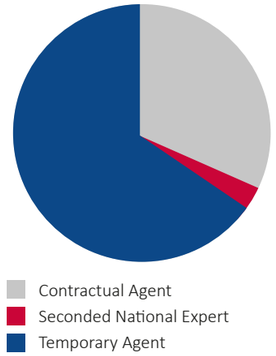
Staff members by Nationality



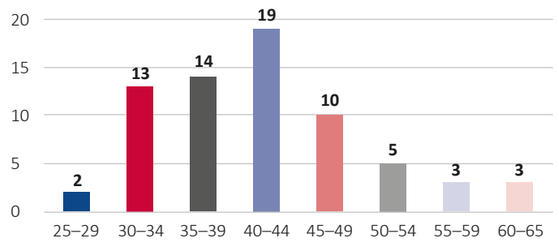
Gender Balance



Staff members by Category



Age Analysis



A6 HUMAN RESOURCES BY ACTIVITY

Core Operational Activities: Strategic Objectives 1-4		Operational Activities (FTE)	Total Cost of Activities ABB (EUR)
SO1	**ActivitiesABBSO1To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network & Information Security (NIS)**		
WPK 1.1	NIS Threats Analysis	2.3	245 806
WPK 1.2	Improving the Protection of Critical Information Infrastructures	6.6	688 253
WPK 1.3	Securing emerging Technologies and Services	5.3	486 603
WPK 1.4	Short- and mid-term sharing of information regarding issues in NIS	2.7	183 301
Total SO1		**16.8**	**1 603 963**
SO2	**To assist the Member States and the Commission in enhancing capacity building throughout the EU**		
WPK 2.1	Assist in public sector capacity building	6.6	788 253
WPK 2.2	Assist in private sector capacity building	2.4	185 971
WPK 2.3	Assist in improving awareness of the general public	2.0	167 476
Total SO2		**11.0**	**1 141 700**
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**		
WPK 3.1	Provide information and advice to support policy development	2.7	233 301
WPK 3.2	Assist EU MS and Commission in the implementation of EU NIS regulations	5.3	506 603
WPK 3.3	Assist EU MS and Commission in the implementation of NIS measures of EU data protection regulation	4.0	404 952
WPK 3.4	R&D, Innovation & Standardisation	2.7	248 301
Total O3		**14.6**	**1 393 157**
SO4	**To enhance cooperation both between the Member States of the EU and between related NIS communities**		
WPK 4.1	Support for EU cooperation initiatives amongst NIS –related communities in the context of the EU	4.6	439 777
WPK 4.2	European cyber crisis cooperation through exercises	6.0	617 428
Total SO4		**10.6**	**1 057 205**

Horizontal Operational Activities		Operational Activities (FTE)	Total Cost of Activities ABB (EUR)
	ActivitiesStakeholder Relations, Corporate Communication, Project Support Activities		
SR1	MB & PSG Secretariat	1.3	271 651
SR2	National Liaison Officers Network	0.7	77 825
SR3	EU Relations	0.7	45 825
SR4	Stakeholders Communication	1.3	91 651
CC1	Corporate Communication	1.3	329 651
PS1	Quality control & Project Office	7.3	735 079
PS2	Article 14 requests	0.7	45 825
PS3	Data Protection Officer	0.7	45 825
Total SO1		**13.9**	**1 643 332**
Total Operational Activities		**67.0**	**6 839 357**

Administration and Support Activities		Operational Activities (FTE)	Total Cost of Activities ABB (EUR)
ASA	**Administration and Support Activities**		
ASA 0	Executive Director's office and General Management activities	1.1	83 985
ASA 1	General Administration activities	0.7	131 840
ASA 2	Finance, Accounting & Procurement activities	2.6	180 538
ASA 3	HR Activities (excluding salaries)	1.6	976 836
ASA 4	IT Activities	1.5	514 353
ASA 5	Facility Management Activities	0.5	930 651
Total ASA	**Administration and Support Activities**	**8.0**	**2 818 203**

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 2015.

ANNEX B.
FINANCIAL RESOURCES

B1 PROVISIONAL ANNUAL ACCOUNTS 2015

Balance Sheet 2015 (in EUR)

	2015	2014
NON-CURRENT ASSETS	**878 678**	**813 993**
Intangible Assets	1 409	1 954
Property, plant and equipment	877 269	812 039
CURRENT ASSETS	**1 065 148**	**1 652 400**
Short-term Receivables	280 069	270 320
Cash and Cash Equivalents	785 079	1 382 080
ASSETS	**1 943 826**	**2 466 393**
NON-CURRENT LIABILITIES	**-**	**-**
Provisions (long term)	-	-
CURRENT LIABILITIES	**686 251**	**1 026 144**
EC Pre-financing received	80 397	105 318
EC Interest payable	-	17 323
Accounts Payable	289 761	234 179
Accrued Liabilities	316 093	469 324
Short-term provisions	-	200 000
LIABILITIES	**686 251**	**1 026 144**
NET ASSETS (ASSETS less LIABILITIES)	**1 257 575**	**1 440 249**

Statement of Financial Performance 2015 (in EUR)

	2015	2014
OPERATING REVENUES	**10 062 303**	**9 664 900**
Revenue from the European Union Subsidy	9 345 552	9 035 189
Other revenue	83 089	10 131
Revenue from Administrative operations	633 662	619 580
OPERATING EXPENSES	**-10 243 489**	**-9 427 471**
Administrative Expenses	-8 062 292	-7 735 138
Operational Expenses	-2 181 197	-1 579 833
Adjustments to provisions	-	-112 500
OTHER EXPENSES	**-1 487**	**-1 948**
Financial Expenses	-1 118	-1 171
Exchange rate loss	-369	-777
ECONOMIC RESULT FOR THE YEAR	**-182 673**	**235 481**

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 2016).

B2 FINANCIAL REPORTS 2015

Outturn on Commitment Appropriations in 2015

Chapter		Commitment appropriations authorised *	Commitments made	%
		1	2	3=2/1
Title A-1 STAFF				
A-11	Staff in Active Employment	4 515 299.70	4 515 299.70	100.00 %
A-12	Recruitment Expenditure	356 508.46	356 508.46	100.00 %
A-13	Socio-medical Services and Training	140 980.28	140 980.28	100.00 %
A-14	Temporary Assistance	911 137.36	911 137.36	100.00 %
Total Title A-1		**5 923 925.80**	**5 923 925.80**	**100.00 %**
Title A-2 FUNCTIONING OF THE AGENCY				
A-20	Buildings and Associated Costs	923 342.25	923 342.25	100.00 %
A-21	Movable Property and Associated Costs	22 550.57	22 550.57	100.00 %
A-22	Current Administrative Expenditure	56 951.50	56 951.50	100.00 %
A-23	Information and Communication Technologies	430 184.52	430 184.52	100.00 %
Total Title A-2		**1 433 028.84**	**1 433 028.84**	**100.00 %**

Title B-3 OPERATING EXPENDITURE				
B-30	Group Activities	837 097.61	837 097.61	100.00 %
B-32	Horizontal Operational Activities	408 266.62	408 266.62	100.00 %
B-36	Core Operational Activities	1 467 761.04	1 467 761.04	100.00 %
Total Title B-3		**2 713 125.27**	**2 713 125.27**	**100.00 %**
TOTAL ENSA		**10 070 079.91**	**10 070 079.91**	**100.00 %**

* 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 2015

Chapter		Payment appropriations authorised *	Payments made	%
		1	2	3=2/1
Title A-1 STAFF				
A-11	Staff in Active Employment	4 515 299.70	4 515 299.70	100.00 %
A-12	Recruitment Expenditure	382 788.00	359 569.67	93.93 %
A-13	Socio-medical Services and Training	246 075.28	149 327.18	60.68 %
A-14	Temporary Assistance	1 164 712.98	904 635.71	77.67 %
Total Title A-1		**6 308 875.96**	**5 928 832.26**	**93.98 %**
Title A-2 FUNCTIONING OF THE AGENCY				
A-20	Buildings and Associated Costs	1 016 381.78	929 250.25	91.43 %
A-21	Movable Property and Associated Costs	42 939.89	41 012.60	95.51 %
A-22	Current Administrative Expenditure	59 702.61	55 601.92	93.13 %
A-23	Information and Communication Technologies	926 985.60	832 299.64	89.79 %
Total Title A-2		**2 046 009.88**	**1 858 164.41**	**90.82 %**
Title B-3 OPERATING EXPENDITURE				
B-30	Group Activities	1 001 378.21	926 009.72	92.47 %
B-32	Horizontal Operational Activities	498 239.19	435 861.66	87.48 %
B-36	Core Operational Activities	1 547 997.47	1 498 437.04	96.80 %
Total Title B-3		**3 047 614.87**	**2 860 308.42**	**93.85 %**
TOTAL ENSA		**11 402 500.71**	**10 647 305.09**	**93.38 %**

* 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. 2015

Chapter		2015 Commitments to be settled			
		Commitments 2015	Payments 2015	RAL 2015	% to be settled
		1	2	3=1-2	4=1-2/1
Title A-1 STAFF					
A-11	Staff in Active Employment	4 515 299.70	-4 515 299.70	0.00	0.00 %
A-12	Recruitment Expenditure	356 508.46	-344 129.81	12 378.65	3.47 %
A-13	Socio-medical Services and Training	140 980.28	-58 527.09	82 453.19	58.49 %
A-14	Temporary Assistance	911 137.36	-669 981.05	241 156.31	26.47 %
Total Title A-1		**5 923 925.80**	**-5 587 937.65**	**335 988.15**	**5.67 %**
Title A-2 FUNCTIONING OF THE AGENCY					
A-20	Buildings and Associated Costs	923 342.25	-840 378.93	82 963.32	8.99 %
A-21	Movable Property and Associated Costs	22 550.57	-21 629.65	920.92	4.08 %
A-22	Current Administrative Expenditure	56 951.50	-52 888.13	4 063.37	7.13 %
A-23	Information and Communication Technologies	430 184.52	-337 094.21	93 090.31	21.64 %
Total Title A-2		**1 433 028.84**	**-1 251 990.92**	**181 037.92**	**12.63 %**
Title B-3 OPERATING EXPENDITURE					
B-30	Group Activities	837 097.61	-785 206.45	51 891.16	6.20 %
B-32	Horizontal Operational Activities	408 266.62	-345 889.09	62 377.53	15.28 %
B-36	Core Operational Activities	1 467 761.04	-1 424 535.26	43 225.78	2.95 %
Total Title B-3		**2 713 125.27**	**-2 555 630.80**	**157 494.47**	**5.80 %**
TOTAL ENSA		**10 070 079.91**	**-9 395 559.37**	**674 520.54**	**6.70 %**

* 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 2015

Title	Description	Year of Origin	Revenue and Income recognised	Revenue and Income cashed in 2014	Outstanding Balance
9000	Subsidy from the eu general budget	2015	9 425 949.00	9 425 949.00	0.00
9200	Other contributions	2015	616 378.68	616 378.68	0.00
9300	Revenue from administrative operations	2015	21 945.85	26 952.44	0.00
TOTAL ENSA			**10 064 273.53**	**10 069 280.12**	**0.00**

Average Payment Time for 2015

Average Payment Time for 2015 (Days)	Total number of payments	Within Time Limit	Percentage	Average Payment Time (Days)	Late Payment	Percentage	Average Payment Time (Days)
19.07	2 084	1 758	84.36 %	12.65	326	15.64 %	53.68

ANNEX C.
MATERIALITY CRITERIA

ENISA is not using any materiality criteria. Indeed 100 % of the financial transactions are submitted to the ex ante control (verification before the authorisation).

In order to further strengthen the controls, ENISA executes a yearly ex post control exercise (verification after authorisation).

The exercise methodology for sample selection is a judgmental (non-statistical) method designed to demonstrate bias in the selection of transactions for ex post control taking into account the potential for error identified by the Agency, either through the value of the transaction, the initiating procedure used and the Agency's risk assessment, their documentation or through discussion.

ANNEX D.

INTERNAL CONTROL TEMPLATES FOR BUDGET IMPLEMENTATION (ICT)

D1 STAGE 1: PROCUREMENT

D.1.1 Planning

Main control objectives: Effectiveness, efficiency and economy. Compliance (legality and regularity).

Main risks It may happen (again) that…	Mitigating controls	How to determine coverage frequency and depth	How to estimate the costs and benefits of controls	Possible control indicators
The needs of the Agency are not well defined (operationally and economically) and that the decision to procure was inappropriate to meet the operational objectives. Interruption or delay of the services provided due to late contracting (poor planning and organisation of the procurement process)	Publication of intended procurements / Work Programme.	100 % of the forecast procurements (open procedures published in OJEU and website) are justified in a note addressed to the AO(D).	**Costs:** Estimation of cost of staff involved and the related contract values (if external expertise is used). **Benefits:** Amount of rejections of unjustified purchases. Estimation of litigation avoided and eventual discontinuation of the service provided.	**Effectiveness:** Number of projected tenders cancelled, Number of contracts discontinued or underutilised due to poor planning. **Efficiency:** For consultancy based tenders for operations: average person day cost per tender.
	Validation by AO(S)D of justification (economic, operation) for launching a procurement process.	100 % of the forecast procurements.		
	Decisions discussed/ taken at Management Team meeting.	All key procurement procedures (> amounts and/or having significant impact on the objectives of the Agency) are discussed at management meetings.		

D.1.2 Needs assessment & definition of needs

Main control objectives: Effectiveness, efficiency and economy. Compliance (legality and regularity).

Main risks It may happen (again) that…	Mitigating controls	How to determine coverage frequency and depth	How to estimate the costs and benefits of controls	Possible control indicators
The best offer(s) are not DG if it goes wrong submitted due to the poor definition of the tender specifications.	AOSD supervision and approval of specifications.	100 % of the specifications are scrutinised **Depth:** May be determined by the amount and/or the impact on the objectives of the Agency	**Costs:** Estimation of cost of staff involved and the related contract values (if external expertise is used). **Benefits:** Limit the risk of litigation, limit the risk of cancellation of a tender. Amount of contracts for which the approval and supervisory control detected material error.	**Effectiveness:** Number of 'open' or procedures where only one or no offers were received. Number of requests for clarification regarding the tender. **Efficiency:** Estimated average cost of a procurement procedure.
	Additional supervisory verification by specialised expert actor or entity.	100 % of the tenders above a financial threshold (e.g. > EUR 60 000) are reviewed. **Depth:** Risk based, depends on the sensitivity.		

D.1.3 Selection of the offer & evaluation

Main control objectives: Effectiveness, efficiency and economy. Compliance (legality and regularity). Fraud prevention and detection.

Main risks It may happen (again) that…	Mitigating controls	How to determine coverage frequency and depth	How to estimate the costs and benefits of controls	Possible control indicators
The most economically advantageous offer not being selected, due to a biased, inaccurate or 'unfair' evaluation process.	**Formal evaluation process:** Opening committee and Evaluation committee.	100 % of the offers analysed. Depth: All documents transmitted.	**Costs:** Estimation of costs involved. **Benefits:** Compliance with FR. Difference between the most onerous offer and the selected one.	**Effectiveness:** Number of 'valid' complaints or litigation cases filed. **Efficiency:** Cost of successful tender minus cost of the most onerous one (or average cost). Average cost of a tendering procedure.
	Opening and Evaluation Committees' declaration of absence of conflict of interests.	100 % of the members of the opening committee and the evaluation committee.	**Costs:** Estimation of cost of staff involved. **Benefits:** Amount of contracts for which the control prevented the risk of litigation or fraud.	
	Exclusion criteria documented.	100 % checked. **Depth:** Required documents provided are consistent.	**Costs:** estimation of cost of staff involved. **Benefits:** Avoid contracting with excluded economic operators.	
	Standstill period, opportunity for unsuccessful tenderers to put forward their concerns on the decision.	100 % when conditions are fulfilled.	**Costs:** estimation of cost of staff involved. **Benefits:** Amount of procurements successfully challenged during standstill period.	

D2 STAGE 2: FINANCIAL TRANSACTIONS

Main control objectives: Ensuring that the implementation of the contract is in compliance with the signed contract.

Main risks It may happen (again) that…	Mitigating controls	How to determine coverage frequency and depth	How to estimate the costs and benefits of controls	Possible control indicators
The products/services/ works foreseen are not, totally or partially, provided in accordance with the technical description and requirements foreseen in the contract and/or the amounts paid exceed that due in accordance with the applicable contractual and regulatory provisions. Business discontinues because contractor fails to deliver.	Operational and financial checks in accordance with the financial circuits. Operation authorisation by the AO For riskier operations, ex ante in-depth verification.	100 % of the contracts are controlled, including only value-adding checks. Riskier operations subject to in-depth controls. The depth depends on risk criteria.	**Costs:** Estimation of cost of staff involved. **Benefits:** Amount of irregularities, errors and overpayments prevented by the controls	**Effectiveness:** % error rate prevented (amount of errors/ irregularities averted over total payments); Number of control failures; Number/ amount of liquidated damages. **Efficiency:** Average cost per open project. % cost over annual amount disbursed. **Time-to-payment:** Late interest payment and damages paid (by the Agency).
	For high risk operations, reinforced monitoring on deliverables timing. Management of sensitive functions.	High risk operations identified by risk criteria. Amount and potential impact on the Agency operations of late or no delivery.		

ANNEX E.

THE PERMANENT STAKEHOLDERS' GROUP, TERM OF OFFICE 2015-2017

Nominated members

Authority	Nominated representative	Alternate
Art. 29 Working Party	Mr Gwendal Le Grand Director of technology and innovation Commission nationale de l'informatique et des libertés (CNIL)	
Body of European Regulators for Electronic Communications (BEREC)	The Chairperson of the BEREC	To be nominated on an ad hoc basis
Europol	Mr Olivier Burgersdijk, Head of Strategy of the European Cybercrime Centre (EC3) at Europol	Mr Benoit Godart, EC3

Experts appointed ad personam

Name	Nationality	Sector
Rainer Baumgart	German	Industry
Marcus Berglund	Swedish	Consumer
Ilias Chantzos	Double (Greek/Belgian)	Industry
Nick Coleman	British	Industry
Corrado Giustozzi	Italian	Consumer
Marcos Gomez Hidalgo	Spanish	Consumer
Luke Thomas Herbert	British	Academia
Tom Koehler	German	Industry
Mika Lauhde	Finnish	Industry
Katerina Mitrokotsa	Greek	Academia
Jan Neutze	German	Industry
Bart Preneel	Belgian	Academia
Kai Rannenberg	German	Academia
Christine Runnegar	Swiss	Consumer
Ingrid Schaumüller-Bichl	Austrian	Academia
Margarita Starkeviciute	Lithuanian	Consumer
Marc Vael	Belgian	Industry
Franck Veysset	French	Industry
Alain Viallix	French	Industry
Claire Vishik	Double (British/American)	Industry

ANNEX F.

LIST OF ENISA MANAGEMENT BOARD REPRESENTATIVES AND ALTERNATES

This annex includes the list of ENISA Management Board Representatives and Alternates as of 9. 12. 2014.

Commission representatives

Representative	Alternate
Paul TIMMERS Director in charge for Sustainable and Secure Society DG Communications Networks, Content and Technology Paul.Timmers@ec.europa.eu	**Jakub BORATINSKI** Head of Trust and Security DG Communications Networks, Content and Technology Jakub.Boratinski@ec.europa.eu
Ken DUCATEL Chief Information Security Officer DG DIGIT Ken.DUCATEL@ec.europa.eu	**Grzegorz MINCZAKIEWICZ** Head of Unit, Information Technology Unit DG DIGIT Grzegorz.MINCZAKIEWICZ@ec.europa.eu

Member States representatives in alphabetical order

Member State	Representative	Alternate
Austria	**Reinhard POSCH** Chief Information Officer reinhard.posch@cio.gv.at	**Herbert LEITOLD** A-SIT, Secure Information Technology Center – Austria Institute for Applied Information Processing and Communication, IAIK Graz herbert.leitold@iaik.at
Belgium	**Daniel LETECHEUR** Information Security Analyst Fedict daniel.letecheur@fedict.belgium.be	**Dr Stéphane VAN ROY** Engineer-Advisor BIPT Stephane.Van.Roy@bipt.be

Bulgaria	**Krasimir SIMONSKI** Executive Director of the Executive Agency 'Electronic Communication Networks and Information Systems' ksimonski@esmis.government.bg	**Vasil GRANCHAROV** Director of Network and Information Security Directorate Executive Agency 'Electronic Communication Networks and Information Systems' vgrancharov@esmis.government.bg
Croatia	**Zeljko TABAKOVIC**	
Cyprus	**Antonis ANTONIADES** Senior Officer of Electronic Communications and Postal Regulation antonis.antoniades@ocecpr.org.cy	**Costas EFTHYMIOU** Officer of Technical Affairs at Office of the Commissioner of Electronic Communications and Postal Regulation costas.efthymiou@ocecpr.org.cy
Czech Republic	**Jaroslav SMID** Deputy Director National Centre for Cyber Security National Security Authority of the Czech Republic j.smid@nbu.cz	**Roman PACKA** Assistant Director of NSA r.packa@nbu.cz
Denmark	**Flemming FABER** Senior Adviser Ministry of Defense Centre for Cyber Security ff@govcert	**Thomas KRISTMAR** Head of Unit Danish Ministry of Defence Centre for Cyber Security thokri@cfcs.dk
Estonia	**Toomas VAKS** Director of Cyber Security Information Systems Authority	**Karoliina AINGE** Head of Estonian Cyber Security Policy Department of State Information Systems Ministry of Economic Affairs and Communications
Finland	**Timo KIEVARI** Ministerial adviser Ministry of Transport and Communications timo.kievari@lvm.fi	**Piia NYSTROM** Senior Officer Ministry of Transport and Communications Communications Policy Department Communications Data piia.nystrom@lvm.fi
France	**Jean-Baptiste DEMAISON** Agence nationale de la sécurité des systèmes d'information (ANSSI) international.enisa-mb@ssi.gouv.fr	**Yann SALAMON** Agence nationale de la sécurité des systèmes d'information (ANSSI) international.enisa-mb@ssi.gouv.fr
Germany	**Michael HANGE** President of the Federal Office for Information Security (BSI) michael.hange@bsi.bund.de	**Roland HARTMANN** Head of International Relations Federal Office for Information Security (BSI) SIB@bsi.bund.de
Greece	**Dimosthenis VATIKIOTIS**	**Theodoros KAROUBALIS** Hellenic Ministry of Transport and Communications t.karoubalis@yme.gov.gr
Hungary	**Ferenc SUBA** VICE-CHAIR OF ENISA MANAGEMENT BOARD Senior Advisor National Cybersecurity Coordination Council Prime Minister's Office ferenc.suba@cybersecurity.me.gov.hu	**Bela Ferenc VERECKEI** President National Information Security Authority Ministry of Interior ferenc.bela.vereckei@bm.gov.hu
Ireland	**Kevin FOLEY** National Cyber Security Unit Department of Communications, Energy & Natural Resources Kevin.foley@dcenr.gov.ie	**Paul CONWAY** Head of Compliance and Operations Commission for Communications Regulation paul.conway@comreg.ie
Italy	**Rita FORSI** Director General of Instituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI) Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, Department of Communications, Ministry of Economic Development rita.forsi@mise.gov.it	**Alessandro RIZZI** Ministry of Economic Development Department of Communications alessandro.rizzi@mise.gov.it
Latvia	**Leva KUPCE** Adviser of State Secretary Ministry of Defence ieva.kupce@mod.gov.lv	**Viktors LIPENITS** Head of transport and communications division Ministry of Transport and Communications viktors.lipenits@sam.gov.lv
Lithuania		**Dr Rytis RAINYS** Head of Network and Information Security Department of the Communication Regulatory Authority of Lithuania rytis.rainys@rrt.lt
Luxembourg	**François THILL** Accréditation, notification et surveillance des PSC francois.thill@eco.etat.lu	**Pascal STEICHEN** Ministry of the Economy and Foreign Trade Department for electronic commerce and information security pascal.steichen@eco.etat.lu
Malta	**John AGIUS** Director (Critical Infrastructure Protection) Malta Critical Infrastructure Protection (CIP) Unit, Cabinet Office, Office of the Prime Minister john.f.agius@gov.mt maltacip@gov.mt	**George CHETCUTI**
Netherlands	**Mr H.L. (Hans) de VRIES** Head NCSC and Deputy director Cyber Security Ministry of Security and Justice hans.devries@ncsc.nl	**drs. J.C. (Hans) Oude ALINK** Senior coordinating advisor National Cyber Security Centre (NCSC) Ministry of Security and Justice hans.oudealink@ncsc.nl
Poland	**Krzysztof SILICKI** Technical Director Research and Academic Computer Network (NASK) krzysztof.silicki@nask.pl	**Piotr DURBAJŁO** Deputy Director of the IT Security Department The Internal Security Agency p.durbajlo@abw.gov.pl
Portugal	**José Carlos BARREIRA MARTINS** Coordinator of the National Centre for Cybersecurity	**Manuel PEDROSA DE BARROS** Diretor da Direção de Segurança das Comunicações da ANACOM 2730-216 Barcarena manuel.barros@anacom.pt
Romania	**Augustin JIANU** Director, CERT-RO augustin.jianu@cert-ro.eu	
Slovakia	**Ján HOCHMANN** Director Information Society Division Ministry of Finance of the Slovak Republic jan.hochmann@mfsr.sk	

Slovenia	**Gorazd BOZIC** Head ARNES SI-CERT gorazd.bozic@cert.si gorazd.bozic@arnes.si	**Denis TRCEK** Laboratory of e-media, Head Faculty of Computer and Information Science University of Ljubljana denis.trcek@fri.uni-lj.si
Spain	National Security Department, Spanish Prime Minister´s Office dsn@dsn.presidencia.gob.es	National Security Department, Spanish Prime Minister´s Office dsn@dsn.presidencia.gob.es
Sweden	**Jörgen SAMUELSSON** CHAIR OF ENISA MANAGEMENT BOARD Deputy Director Division for Information Technology Policy Ministry of Enterprise, Energy and Communications jorgen.samuelsson@gov.se	**Annica BERGMAN** Network Security Department Swedish Post and Telecom Agency (PTS) annica.bergman@pts.se
United Kingdom	**Rachael BISHOP** BIS Assistant Director of Cyber EU and International Policy Rachael.bishop@bis.gsi.gov.uk	**Colin WHORLOW** Head of International Relations CESG colin.whorlow@cesg.gsi.gov.uk

EEA-country representatives (observers)

Member State	Representative	Alternate
Iceland	**Björn GEIRSSON** Director of Legal Division Post and Telecom Administration in Iceland bjorn@pfs.is	
Liechten-stein	**Kurt BÜHLER** Director Office for Communications Kurt.buehler@ak.llv.li	
Norway	**Jörn RINGLUND** Deputy Director General Ministry of Transport and Communications Department of Civil Aviation, Postal Services and Telecommunications jorn.ringlund@sd.dep.no	**Martin KJELLSEN**

ANNEX G.
LIST OF POLICY DOCUMENTS

	Policy document	Complete title and link (Links available as of April 2016.)
1	The new ENISA Regulation (EU) No 526/2013	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, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0526 Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.
2	Cybersecurity strategy of the EU	Joint communication on the cybersecurity strategy of the European Union: 'An open, safe and secure cyberspace', JOIN(2013) 1 final of 7 February 2013, available from: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.
3	The proposal for an NIS directive	Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final of 7 February 2013, available from: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.
4	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
5	Digital agenda	Commission communication — 'A digital agenda for Europe', COM(2010) 245 final of 19 May 2010. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245&from=EN
6	Directive on European critical infrastructures (ECIs)	Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:jl0013

7	Critical information infrastructure protection (CIIP) action plan	Commission communication on critical information infrastructure protection, 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience', COM(2009) 149 final of 30 March 2009, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF.
8	Commission communication on critical information infrastructure protection	Commission communication on critical information infrastructure protection, 'Achievements and next steps: towards global cyber-security' adopted on 31 March 2011 and the Council conclusion on CIIP of May 2011. http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf
9	Electronic communications regulatory framework	Telecommunications regulatory package (Article 13a amended Directive 2002/21/EC framework directive).
10	Review of the data protection framework	Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation), COM(2012) 11 final of 25 January 2012, available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.
11	Regulation on electronic identification and trusted services for electronic transactions in the internal market (eIDAS)	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. http://eur-lex.europa.eu/legal-tent/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
12	Commission regulation 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. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF
13	Framework to build trust in the digital single market (DSM) for e-commerce and online services	Commission communication — 'A coherent framework for building trust in the digital single market for e-commerce and online services', COM(2011) 942 final of 11 January 2012. http://ec.europa.eu/internal_market/e-commerce/communication_2012_en.htm
14	Directive on attacks against information systems (IS)	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, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-:32013L0040.
15	Communication on Europol's European cybercrime centre (EC3)	Commission Communication — 'Tackling crime in our digital age: Establishing a European cybercrime centre', European Commission, COM(2012) 140 final of 28 March 2012, available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/communication_european_cybercrime_centre_en.pdf.
16	Council resolution of December 2009 on a collaborative approach to network and information security (NIS)	Council resolution of 18 December, 2009 on a collaborative approach to network and information security (2009/C 321 01), available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:C:2009:321:TOC.
17	Council conclusion on CIIP of May 2011	Council conclusion on CIIP of May 2011, available at: http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf.
18	Action plan for an innovative and competitive security industry	Commission communication on security industry policy, 'Action plan for an innovative and competitive security industry', COM(2012) 417 final of 26 July 2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF
19	Single Market Act	Single Market Act: Twelve levers to boost growth and strengthen confidence, 'Working together to create new growth', COM(2011) 206 final of 13 April 2011. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0206:FIN:en:PDF
20	Internet of things — An action plan for Europe	Commission communication — 'Internet of things — An action plan for Europe', COM(2009) 278 final of 18 June 2009. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF
21	European cloud computing strategy	Commission communication — 'Unleashing the potential of cloud computing in Europe', COM(2012) 529 final of 27 September 2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF
22	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
23	Telecom ministerial conference on CIIP	Telecom ministerial conference on CIIP organised by the Presidency in Balatonfüred, Hungary, 14-15 April 2011.
24	Data protection directive	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
25	Digital single market (DSM) strategy	Commission communication — 'A digital single market strategy for Europe', COM(2015) 192 final of 6 May 2015, available at: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf.
26	Communication on thriving data-driven economy	Commission communication — 'Towards a thriving data-driven economy', COM(2014) 442 final of 2 July 2014, available at: https://ec.europa.eu/digital-agenda/en/news/communication-data-driven-economy.
27	ENISA Work Programme 2015 and Amendment	ENISA Work Programme 2015: https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2015. Amending Work Programme 2015: https://www.enisa.europa.eu/publications/programmes-reports/amending-work-programme-2015.

NOTES

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

Catalogue number: TP-AB-16-001-EN-N
ISBN: 978-92-9204-167-0
ISSN: 2314-9434
DOI: 10.2824/698162

enisa.europa.eu