European Union Agency for Network and Information Security

ENISA
ANNUAL REPORT

2013

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*):

00 800 6 7 8 9 10 11

(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

More information on the European Union is available on the Internet (http://europa.eu).

Cataloguing data can be found at the end of this publication.

Luxembourg: Publications Office of the European Union, 2014

ISBN 978-92-9204-084-2

ISSN 01/2+7212

doi / .,0602-1/2/4

Printed in Greece

PRINTED ON ELEMENTAL CHLORINE-FREE BLEACHED PAPER (ECF)

A MESSAGE FROM THE EXECUTIVE DIRECTOR

Securing our cyber-future

It is my pleasure to present ENISA's Annual Report 2013, which provides a comprehensive overview of the Agency's activities for this year.

This has been a year of changes, largely characterised by two major events:

- Firstly, the EU's cyber security strategy was published. This pushed cyber security to the political level, where three European commissioners joined forces to conduct a comprehensive analysis of the situation and propose remedies for Europe as we move ahead.
- Secondly, in this new political landscape, the successful final negotiation and consequent adoption of our new mandate occurred on 18th June 2013. One of its effects is that the "General Report" will be called the "Annual Activity Report" in the future.

In 2013, we also welcomed a new Chair of the Management Board, Mr Jörgen Samuelsson of Sweden, while at the same time thanking the outgoing Chair from Finland, Mrs Mari Herranen for her excellent work.

The message underlying this report is that ENISA continues to be a recognised player and trusted partner for the Member States of the European Union and globally. Our experience, insight, expertise and added value have become increasingly acknowledged and appreciated among all cyber security actors; Member states, EU institutions, policy makers and practitioners in industry, academia, as well as citizens. In all, 2013 has probably been ENISA's most challenging year and at the same time its most successful year to date. Our Work Programme tasks were completed on time and within budget. The level of financial performance that ENISA achieved was very high, especially given the challenges that we faced. Not the least of these challenges was the transfer of ENISA's operational staff from Heraklion to Athens, which happened without any disruption to our planned activities.

For an agency in the field of cyber security, which faces a constantly evolving threat environment, our success is measured by the accuracy of our insight and the value of our recommendations rather than by how well we performed in the past. The borders between the virtual and real worlds are dissolving, as new technologies, services and business models push existing concepts and regulation to their limits. The organisational structures and physical barriers that ensured security in the past are now largely obsolete, and in some cases, have been breached by cyber threats that are continually evolving. Taking positive, concrete steps to manage these challenges requires that we acknowledge the risks and costs of not addressing the challenges. It requires increased cooperation between all actors at all levels. Whilst cooperation will not happen overnight, ENISA will continue to bring communities together and to encourage information exchange that is based on concrete goals. This will lay the foundation for a more effective collaboration model in the years to come. As part of this approach, ENISA signed a Memorandum of Understanding with CEN/CENELEC and initiated preparations to renew with Europol and ETSI in 2014.

Whilst the following are just a few of the highlights of this year's work, they perfectly illustrate the contribution that the Agency is making to a more secure Europe:

- The ENISA Cloud Report.
- The ENISA annual Threat Landscape Report.
- In terms of the development of ENISA's activities, the Agency followed up on last year's success as the principal player in Europe's Cyber Incident Reporting framework, under Article 13a of the EU's Telecommunications Framework Regulation.
- In the area of Computer Emergency Response Teams (CERTs), the Agency continued to strengthen cooperation within the CERT community.
- We hosted the 2nd cyber security crisis cooperation conference as well as the ENISA annual conference for stakeholders in Brussels at the end of the year.
- The first fully fledged European Cyber Security Month (ECSM) took place in October and involved several Member States and other stakeholders.

In addition to the above planned activities, ENISA responded swiftly and professionally to an increasing number of requests for assistance (the so-called 'Article 14 Requests') from the Member States.

Looking to the future, it is clear that the new ENISA Regulation, adopted by the European Parliament and the Council of Ministers in 2013, will allow the Agency to support the Member States more effectively in the future. Although there is still a significant amount of work to be done to achieve the vision of a harmonised approach to cyber security across the EU, it is encouraging to note that significant progress has been made in collaborating across communities and across national boundaries. ENISA is proud to have contributed to these improvements.

Finally, I would like to say that I am grateful for the hard work, dedication and support of all of the Agency's staff, the members of its Permanent Stakeholders Group, as well as guidance received from the Management Board. All of these actors enabled the Agency to meet its commitments to Europe successfully, despite the challenging new conditions and increased workload throughout the year.

Udo Helmbrecht
Executive Director, ENISA

TABLE OF CONTENTS

1

INTRODUCTION

1.1 EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA) IN BRIEF

ENISA was established in 2004 by Regulation (EC) No. 460/2004 of the European Parliament and the Council. This regulation was subsequently amended by Regulation (EC) No. 1007/2008 of the European Parliament and the Council and Regulation (EC) No. 580/2011 of the European Parliament and the Council, extending ENISA's mandate until 13 September 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 and repealing Regulation (EC) No. 460/2004 ("Regulation (EU) No. 526/2013") further extended ENISA's mandate until 19 June 2020.

The Agency is governed by a **Management Board (MB)** composed of one representative from each EU Member State and EEA country (Iceland, Liechtenstein, and Norway), and two representatives from the European Commission. On 17 October 2013, the MB established the **Executive Board** to enhance the effectiveness and efficiency of the operations of the Agency.

ENISA is managed by its **Executive Director**, who is appointed by the Management Board from a list of candidates proposed by the European Commission and following a hearing in the European Parliament. The Agency's headquarters is in Heraklion, Crete, Greece, with a branch office in Athens, Greece.

The ENISA Management Board (MB) and the **Permanent Stakeholders Group (PSG)**, the latter consisting of 30 leading experts in network and information security acting independently of Member States and companies, assists ENISA by providing advice to extend the Agency's networking and information gathering capabilities.

In line with established practice, two Management Board meetings and one Permanent Stakeholders' group meeting were held as planned during the 2013.

ENISA Management Board meeting in Crete

European Cyber Security Month - ENISA ED Austrian media briefing

In 2013, the MB adopted a number of administrative, management and budgetary decisions to implement Regulation (EU) No. 523/2013. The MB also adopted the Work Programme for 2014. Minutes and decisions of the Management Board are available on the ENISA website (http://www.enisa.europa.eu/about-enisa/structure-organization/management-board).

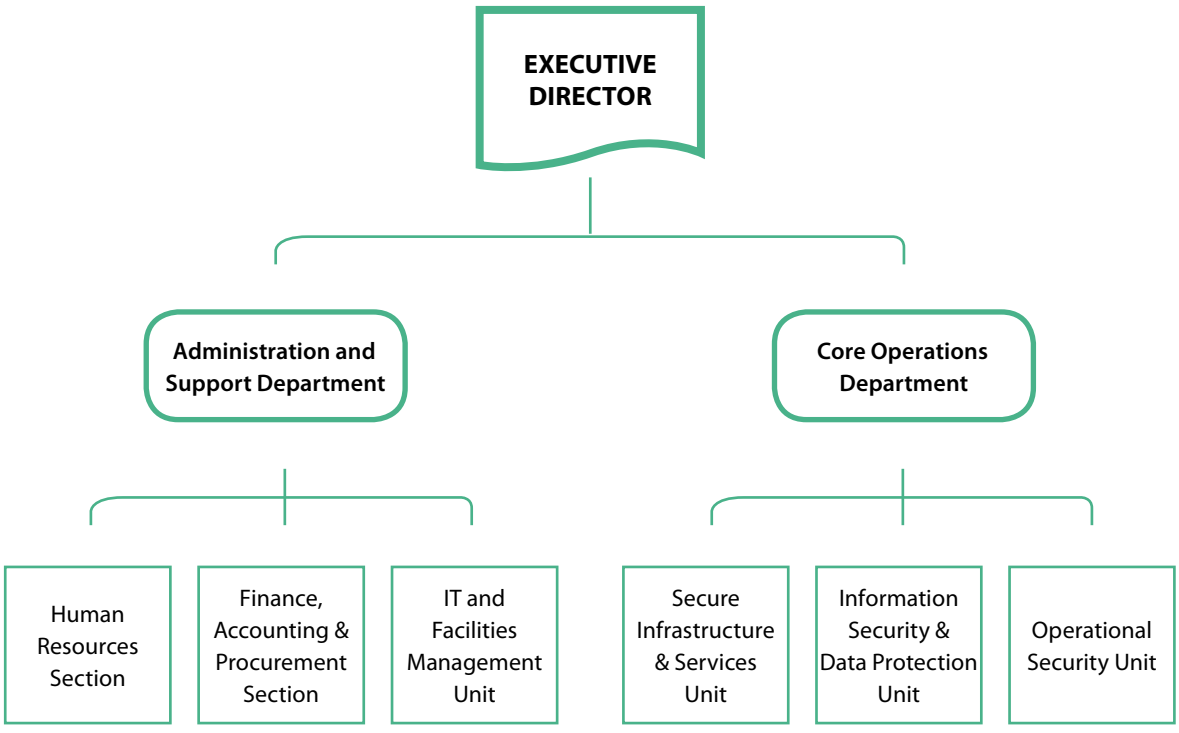
Furthermore, an informal joint meeting between the Management Board and the Permanent Stakeholders Group took place in February 2013 in Greece. The meeting focused on setting the priorities and themes of the Work Programme 2014. In addition, an informal Management Board meeting on strategic guidance for Work Programme 2015 was held in Brussels in November 2013.

The network of National Liaison Officers (NLO) was created as a partnership network of ENISA and its member countries. Although not a formal body, this network is of great value to ENISA, serving as the point of contact with Member States. The NLO consists of experts in national entities involved in network and information security at the national level. As ENISA's contact points with Member States, throughout 2013 and before, the NLOs have been asked to provide feedback and assistance in disseminating information as well as in providing relevant contacts to ENISA to support implementation of the ENISA work programme.

In line with the operational and horizontal objectives of the Agency, ENISA's **organisational structure** (see Figure 1) was reorganised by the Executive Director in December 2013. The organisational structure shows two departments divided in three units/sections each. The Agency's organisational structure is dictated by the new challenges identified by its two locations and its stakeholders and the consequent need to address the rapidly changing operating environment with the limited number of human resources at the Agency's disposal.

As a knowledge-based organisation, ENISA relies on its personnel to deliver its services to its stakeholders and ensure compliance with the regulatory framework. As an EU Agency, ENISA benefits from having a diverse, multi-national workforce.

In 2013, there was an increased focus on communicating ENISA's work and concepts to the European Commission, the Council and the European Parliament as well as other EU agencies and regional organisations. Regular meetings with various Commission services, and **DG CONNECT** in particular, took place during the year.



Pict.1 ENISA organisational chart (as of December 2013.)

1.2 EXECUTIVE SUMMARY

This Annual Activity Report reflects the outstanding achievements of ENISA in 2013, which was probably the most successful year in the history of the Agency.

Two pivotal points marked 2013: the transfer of staff to the Athens office and promulgation of the new "ENISA II" Regulation. In 2013, the Agency successfully supported the Greek government in selecting suitable premises in Athens and then set up its new branch office in record time. This involved transferring staff without disrupting operations and with minimal impact on their work. With end of the year establishment of the new Athens office, ENISA also needed to work hard to obtain a supplementary budget. The Agency successfully achieved this with help from our partner DG CONNECT. ENISA's supplementary budget was disbursed at the very end of 2013, a situation that challenged our management and planning capabilities to their maximum.

The second pivotal point was promulgation of the new "ENISA II" Regulation, (EU) No. 526/2013.[1] The new Regulation provides the Agency with a new and extended seven year mandate, and expands its scope and tasks. Both the transfer of staff to the Athens office and promulgation of the new Regulation represent turning points in the history of the Agency.

Green light for new regulation for EU Cyber Security Agency ENISA given by the European Parliament

With regards to the Work Programme 2013, the Agency successfully delivered all 30 deliverables agreed with the ENISA Management Board. Everything was delivered on time and within budget, corresponding to a delivery rate of 100%. "ANNEX 7: A list of ENISA's Work Programme publications" provides links to these deliverables. Several "extra miles" reports were also delivered. As far as operations, three major accomplishments standout. The first was the 'Second ENISA International Conference on Cyber Crisis Cooperation and Exercises', a high-level event hosted by ENISA in Brussels at the end of 2013. The conference aimed to directly support the EU's new cyber security strategy by bringing together more than 200 stakeholders to establish a more coherent cyber security policy. The event helped to significantly raise the Agency's visibility with its stakeholders. Another major accomplishment was ENISA's annual report on major incidents in the telecoms sector. The report was highly appreciated and represented a milestone in that it provided more material to analyse the trends and patterns. A third major accomplishment was the release of ENISA's annual report on the threat landscape. The report was released at the high-level event in Brussels to our key stakeholders, and received wide acclaim.

As regards project planning and related calls for tender (EU public procurement procedures), 10 calls for tender for 2014 (including several Lots) were already launched during the period November-December 2013, thereby successfully committing 70.5% of the annual budget for core operations for next year. Four tenders leading to multiannual framework contracts with 'Re-opening of Competition' have also been launched. They have helped to streamline the procurement process in thematic areas that are fundamental to ENISA's Regulation.

1 Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA), Brussels, 30.09.2010., COM(2010) 521 final

1.3 KEY PERFORMANCE INDICATORS

KPI1: improved non-governmental Computer Emergency Response Teams (n/g CERTs) collaboration capabilities (continuation of 2012 work) should be adopted by a minimum of four Member States in 2014.

Status KPI1: already adopted by 19 Member States during the two ENISA CERT Workshops in 2013.

KPI2: improved n/g CERT operational capabilities (continuation of 2012 work) should be adopted by a minimum of four Member States in 2014.

Status KPI2: already adopted by 19 Member States during the two ENISA CERT Workshops in 2013.

KPI3: at least 20 Member States should contribute to the work facilitated by ENISA on implementing and enforcing article 13a and should make use of the outcomes of this work.

Status KPI3: all EU National Regulatory Authorities (NRAs) now contribute to ENISA's work on incident reporting.

KPI4: five NRAs and 10 Cloud Computing Providers should support ENISA's work in the area of cloud computing.

Status KPI4: more than 20 different private stakeholders and more than five NRAs contribute to ENISA's work on cloud computing (e.g. governmental cloud, incident reporting, etc.).

KPI5: ENISA should support the European Commission Directorate General for Communications Networks, Content and Technology (DG CONNECT) regarding its proposal for a Regulation on electronic identification and trusted services for electronic transactions in the internal market. In doing so, ENISA should involve at least five relevant stakeholders from public and private sectors.

Status KPI5: ENISA has supported DG CONNECT by providing recommendations on maintaining an acceptable level of security at trust service providers. The study was written by five experts from different sectors and involved 57 organisations from within the EU. Nearly 80 stakeholders from various sectors validated the studies at the Trust Service Provider workshop in September 2013.

1.4 KEY CONCLUSIONS ON RESOURCE MANAGEMENT AND INTERNAL CONTROL EFFECTIVENESS

1.4.1 Resource management

In 2013 the Agency committed its appropriations at a rate of 99.99% (100% in 2012) in order to carry out the operational activities specified in the Work Programme 2013, as well as administrative tasks that are necessary to ensure compliance to the regulatory framework and the provision of services by the Agency. Payments reached the level of 86.46% of the total appropriations received from the Union Budget 2013. The commitment and payment rates demonstrate an increased efficiency in utilisation of the Budget, reconfirmed in the last 4 years.

The outturn of contracts awarded as a result of procurement procedures completed in 2013, is as follows:

- 25 contracts were signed: including 18 service contracts and 7 framework contracts.
- 162 purchase orders were signed: 78 were issued under a framework contract.
- 25 procurement procedures were issued: including 15 open procedures consisting of 19 separate tenders.

As regards project planning and related call for tenders (EU public procurement procedures), ten calls for tenders for 2014 (including several Lots) were already launched during November-December 2013, thereby committing 70.5%[2] of the Core Operations Department's annual budget for 2014. This included the launch of four tenders leading to multiannual framework contracts with 'Re-opening of Competition'. The issuance of multiannual framework contracts has helped to streamline the procurement process in thematic areas that are fundamental to ENISA's Regulation.

2 This is a continuous improvement compared to 34.8% in 2010, 46.5% in 2011, and 64.4% in 2012.

The outturn of contracts awarded as a result of procurement procedures completed in 2013, is as follows:

- 25 contracts were signed: including 18 service contracts and 7 framework contracts.
- 162 purchase orders were signed: 78 were issued under a framework contract.
- 25 procurement procedures were issued: including 15 open procedures consisting of 19 separate tenders.

1.4.2 Internal control effectiveness

In accordance with the governance statement of the European Commission, staff of the Agency conducts operations in compliance with all applicable laws and regulations, working in an open and transparent manner to meet the high level of professional and ethical standards that is expected.

The Agency 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 required by the Financial Regulation, the Executive Director of the Agency has put in place the organisational structure and the internal control systems suited to the achievement of the policy and control objectives, in accordance with the standards and having due regard to the risks associated with the environment in which ENISA operates.

The Agency assessed the effectiveness of its key internal control systems during the reporting year and concluded that the internal control standards have been effectively implemented. In addition, the Agency systematically examined the available control results and indicators, including those designed for monitoring entities to which it has entrusted budget implementation tasks (e.g. subcontractors). The Agency also took into account the observations and recommendations issued by internal auditors and the European Court of Auditors. These have been assessed to determine their impact on management regarding the achievement of control objectives. Please refer to Part 2 for further details

In conclusion, management is confident that, overall, suitable controls are in place and working as intended; risks are being monitored and mitigated; and the required improvements and reinforcements are being implemented. The Executive Director, in his capacity as Authorising Officer, has signed the Declaration of Assurance.

2

POLICY ACHIEVEMENTS

2.1 ACHIEVEMENT OF GENERAL AND SPECIFIC EFFORTS

2.1.1 Policy area Work Stream 1: Evolving risk environment & opportunities

Evolving risk environment & opportunities focuses on informing policy makers and private sector companies on how risks are evolving and on deploying strategies to mitigate these risks. The level of detail of the analysis should be sufficient to support strategic and policy decisions. In addition to informing policy makers, the objective is to mobilise stakeholder communities so that they can achieve common goals and align their strategies and methods. This work stream focuses on the areas of critical information infrastructure and trust infrastructure.

2.1.1.1 General Objective - WPK 1.1: Identification and mitigation of threats affecting Critical Information Infrastructure (CIIP)

Impact Indicator 1: an independent source of information for risks, threats and threat trends, and corresponding mitigation measures should be developed for use by private sector companies for enhancing their security systems and controls.

ENISA lists top cyber-threats in this years Threat Landscape Report

Result achieved: as of this writing, more than 20 different organisations are using the conclusions of ENISA's Threat Landscape report. ENISA Threat Landscape 2013 has been listed in the Authoritative Reports and Resources on Cybersecurity prepared for US Congress (http://www.fas.org/sgp/crs/misc/R42507.pdf). Several hundred references to ENISA Threat Landscape 2013 have been made via the main cybersecurity web pages and blogs.

Impact Indicator 2: policy makers should be provided with an independent and consistent approach to the identification of threats and risks.

Result achieved: more than five EU Member States and the European Commission have expressed interest in using ENISA's Threat Landscape report as a basis for developing their policies.

Studies and reports:

ENISA Threat Landscape mid-year 2013

http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-mid-year-2013/at_download/fullReport

ENISA Threat Landscape 2013

http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport

2.1.1.2 General Objective Work Package 1.2: Identification & mitigation of threats affecting Trust Infrastructure

Impact indicator 1: at least 10 different organisations should be using the conclusions of these analyses by 2014 and the produced material should be recognised as a neutral source of information (Source: Work Programme 2013).

Current situation: 57 organisations took part in the survey on trust service providers. They were all interested in using the conclusions of the analysis. The material was validated at the Trust Service Providers workshop in Brussels in September 2013 by nearly 80 participants from various sectors.

Impact indicator 2: at least five policy makers in cyber security should use the produced information (Source: Work Programme 2013).

Current situation: the papers (Trusted e-ID infrastructures and services in the EU, Trusted provision of e-government services in the EU and eID Authentication methods in e-Finance and e-Payment services) were broadly distributed. The recipients declared interest in using the information. Further results are to be observed.

ENISA conducted a survey[3] that addressed several issues of the services that are being offered: security practices, standards implemented and risk analysis. The survey was complemented by a study about the security mechanisms and interoperability issues specific to the new regulated trust services. Several specific recommendations to e-Government service providers were made. These encourage the use of Trusted Third Party service providers to implement trust services. Such services are required to give citizens confidence in the trustworthiness of services.

Apart from this, in 2013 ENISA launched a survey to collect information about the electronic IDentity and Authentication Systems (eIDAS) used in e-Finance and e-Payment systems and to analyse the risks associated with each eIDAS mechanism. A report documenting best practices was created for the main actors in this sector: financial institutions, merchants and payment service providers.

Studies and reports:

Trusted e-ID infrastructures and services in the EU: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/trusted-eid

Trusted e-ID Infrastructures and services in the EU: Recommendations for trusted provision of e-Government services - https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/trusted-egov

eID Authentication methods in e-Finance and e-Payment services: Current practices and recommendations https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/eIDA-in-e-finance-and-e-payment-services

2.1.1.3 Other Work Stream 1 actions

ENISA Smart Grid Threat Landscape

The objective of this work was to "deepen" the generic risk assessment by taking into account the specificities of smart grids and the appropriate security measures. This was done by providing the threat environment and demonstrating the effect of the selected security measures in reducing threat exposure.

Studies and reports:

ENISA Smart Grid Threat Landscape

http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/sgtl/smart-grid-threat-landscape-and-good-practice-guide/at_download/fullReport

3 The survey came under the scope of the proposed new Regulation on electronic identification and trust services for electronic transactions in the internal market, which will supersede the current Directive 1999/93/EC on a Community framework for electronic signatures.

2.1.2 Policy area Work Stream 2: Improving pan-European CIIP & resilience

Improving pan-European CIIP & Resilience addresses the security of electronic communications and information systems used in the operation of critical infrastructures. The results of this work stream address the managers of the ICT systems using those infrastructures. The beneficiaries of the work achieved in this work stream will be the providers of the services critical for society.

2.1.2.1 General Objective Work Package 2.1: Cyber crisis cooperation

Impact indicator 1: at least 15 Member States should take part in the study on National Risk Management by 2013 (Source: Work Programme 2013).

Result achieved: 22 Member States participated in the study.

Impact indicator 2: at least 15 Member States should request training on ENISA's NCP Good Practice Guide and Cyber Exercises Methodologies by 2014 (Source: Work Programme 2013).

Result achieved: 20 Member States already requested the training in 2013.

Impact indicator 3: at least 90% of EU Member States and EFTA countries should confirm their support for Cyber Europe 2014 (Source: Work Programme 2013)

Result achieved: already in 2013 over 90% of EU Member States and EFTA countries confirmed their support and willingness to participate in Cyber Europe 2014.

Impact indicator 4: at least 80% of Member States should have established or be in the process of establishing National Contingency Plans by 2016 (Source: Work Programme 2013).

Result achieved: ENISA doesn't yet have clear signals from the Member States. Situation is to be observed.

Impact Indicator 5: at least 80% of Member States should have established or be in the process of establishing National Cyber Exercises by 2016 (Source: Work Programme 2013).

Result achieved: over 80% of Member States were in the process of establishing National Cyber Exercises in 2013.[4]

In 2011 ENISA studied the National Cyber Contingency Plans (NCPs) in several countries and prepared the good practice guide on this subject. In 2013, the Agency deepened its understanding of the lifecycle of National Network Information Security Contingency Plans (NCP) by focusing on the National-level Cyber Risk Assessment. ENISA aimed to develop a relevant methodology with an emphasis on 'how-to'. This would help Member States to further improve their national-level contingency planning and their national-level risk assessments for ICT services and infrastructures.

ENISA hosted the "Second ENISA International Conference on Cyber Crisis Cooperation and Exercises" on 23–24 September 2013 in Athens, Greece. The conference was a unique, high-profile international event that directly supported the EU's new cyber security strategy by helping stakeholders to establish more coherent cyber security policies. In addition, the conference was a key knowledge-sharing platform for national and regional cyber security practitioners, both technical experts and executives.

Cyber exercises are recognised as an essential part of the EU's cyber crisis cooperation and response improvement lifecycle. ENISA is a key facilitator of these exercises and is organising the fourth exercise of its kind, Cyber Europe 2014. Cyber Europe 2014 is a multi-level pan European exercise that will take place throughout 2014. Twenty-nine countries from the EU and EFTA will participate in Cyber Europe 2014.

Studies and reports:

National-level Risk Assessments: An Analysis Report

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/nlra-analysis-report

Report on Second International Conference on Cyber-Crisis Cooperation and Exercises

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/2nd-enisa-conference/report

4 In just a few cases, ENISA has not received any indication of the Member State's intentions.

2.1.2.2 General Objective Work Package 2.2: Facilitating Public-Private cooperation

Impact Indicator 1: ENISA should produce three position papers (one for each Task Force by the end of the fourth quarter of 2013); at least three national Public Private Partnerships, five pan-European associations and 15 key private companies should be actively involved in EP3R by end of the fourth quarter of 2013.

Result achieved: all of these impact indicators were achieved despite the closure of EP3R and the establishment of the NIS Platform.

Impact Indicator 2: five National Regulatory Authorities (NRAs) and 10 Cloud Computing Providers should support ENISA's work in the area of cloud computing

Result achieved: more than 20 different private stakeholders and more than five NRAs contribute to ENISA's work on cloud computing (e.g. governmental cloud, incident reporting, etc.)

ENISA supported the implementation of the EU Cloud Strategy and more specifically participated in the Cloud Certification and Cloud Standards working group. The result was to create a list of cloud computing certification schemes, currently including 5 schemes, which will be updated regularly to guide the customers through the security requirements each certified provider offers.

Impact Indicator 3: seven Member States and 10 Private stakeholders should take part in the development of the "cyber security strategy" constituency.

Result achieved: more than 12 different Member States and more than 12 private sector companies actively contribute to ENISA's work on cyber security strategy and are members of this constituency creating the ENISA NCSS experts group.

Impact Indicator 4: to cover as many of the Member States as possible and surpass the number of Member States (8) involved in 2012 (Source: agreements at the beginning of 2013, no KPI in the Work Programme).

Result achieved: 60 stakeholders from 27 European countries in total (including some non-EU countries) participated in the European Cyber Security Month activities.

The European Cyber Security Month (ECSM) is an EU advocacy campaign that takes place in October. The main objective is to promote cyber security awareness among citizens, to modify their perception of cyber threats and to provide updated security information through education, the promotion of good practices and competitions. ECSM 2013 took place in October in 27 countries. The event was coordinated by the European Commission (DG CONNECT) and ENISA. A large number of NIS stakeholders participated in it.

Studies and reports:

EP3R Task Forces paper on terminology definitions and categorisation of assets

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/tf-tdca

EP3R Task Forces paper on incident management and mutual aid strategies

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/tf-masim

EP3R Task Forces on trusted information sharing

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/tf-tis

Roadmap for European Cyber Security Month

http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2013

2.1.2.3 General Objective Work Package 2.3: Improving the transparency of security incidents

Impact Indicator 1: at least 20 Member States should contribute to the work facilitated by ENISA on implementing and enforcing article 13a, and make use of the outcomes of this work. **In 2013 ENISA organised 3 meetings for the Article 13a Expert group. In spring 2013 ENISA also set up a reference group consisting of experts from the electronic communications industry. ENISA uses this group to get direct feedback on its work.**

Result achieved: all EU NRAs now contribute to ENISA's work on incident reporting. ENISA also makes recommendations on national roaming for resilience, for example to discuss possible national roaming schemes with providers and to support the establishment of mutual aid agreements between providers in case of severe incidents. In parallel, a study on power supply dependencies for the communication sector was conducted.

New major incidents in 2012 report by EU cyber security

Impact indicator 2: 10 NRAs and/or Member State competent authorities and 10 Cloud Computing Providers should take part in the study on incident reporting for cloud providers. ENISA has setup an expert group with representatives from the private and public sector, to exchange knowledge and information on the several studies on Cloud Security.

Result achieved: more than 20 different private stakeholders contribute to ENISA's work on incident reporting for cloud computing. They are active members of our expert group.

Impact indicator 3: 10 NRAs and/or Member State competent authorities and 10 Internet Service Providers (ISPs) should take part in the consultation process about both Article 13a and Article 4.

Result achieved: more than 20 NRAs and more than 15 ISPs took part in ENISA's work on Article 13a and Article 4 harmonisation. The dialogue has identified a number of important issues. ENISA is now working with both constituencies to address them.

Studies and reports:

Article 13a Annual Report

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports

National Roaming for mitigating mobile network outages

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/national-roaming-for-resilience

Power Supply Dependencies in the Electronic Communications Sector

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies

National Roaming for resilience

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/national-roaming-for-resilience

Incident reporting for Cloud computing

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/incident-reporting-for-cloud-computing/

2.1.2.4 General Objective Work Package 2.4: Enhancing the security of Governmental Clouds, Smart Grids and Interconnected Networks

Impact indicator 1: 10 NRAs or other relevant government bodies and 10 Cloud Computing Providers should take part in the study on governmental cloud infrastructures.

Result achieved: more than 20 different private stakeholders contribute to ENISA's work on governmental clouds. It presents information from a total of 23 European countries (20 EU countries). The result is a set of recommendations on how to securely deploy cloud services in the public sector. The stakeholders are active members of our expert group.

Launch of ENISA report on Governmental clouds

Impact indicator 2: seven Member State NRAs and 10 Smart Grid providers should take part in the development of the Smart Grid community.

Result achieved: more than five NRAs and 30 different private stakeholders contribute to ENISA's work on minimum security measures for Smart Grids. The European Commission has recognised that smart grids – the blending of the energy (power) and telecommunication critical infrastructures – should operate securely and respect end-users' privacy. In order for European smart grid service providers to improve the security and the resilience of their infrastructures and services, they first have to assess risks and then take appropriate measures to mitigate these risks. In this light, EG2[5] has decided to organise consultations with industry and national cyber security authorities regarding minimum security requirements.

Impact indicator 3: 10 NRAs and 10 ISPs and Internet Exchange Points (IXPs) should take part in the study on priority data communications.

Result achieved: more than 20 NRAs and 15 different private stakeholders (IXP providers, ISPs, Telcos, etc.) have contributed to ENISA's work on internet interconnection.

Deliverables:

Good practice guide for securely deploying governmental clouds

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds

Proposal for a list of security measures for smart grids

https://resilience.enisa.europa.eu/security-and-resilience-of-communication-networks-and-information-systems-for-smart-grids/eg2-minimum-security-measures-for-smart-grids/conference-calls/3rd-conference-call/final-document/view

Good practices for an EU ICS testing coordination capability

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/good-practices-for-an-eu-ics-testing-coordination-capability

Window of exposure… a real problem for SCADA systems?

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/window-of-exposure-a-real-problem-for-scada-systems

Guidelines for enhancing the Resilience of eCommunication Networks

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/guidelines-for-enhancing-the-resilience-of-ecommunication-networks

5 Expert Group 2 formed by European Commission's Smart Grid Task Force and it aims at making regulatory recommendations for data safety, data handling and data protection.

2.1.2.5 Other Work Stream 2 actions

Aside from the activities planned in the Work Programme, ENISA performed actions in the framework of Work Stream 2.

2.1.2.5.1 Methodology of severity assessment of data breaches

In previous years, the Agency developed specific technical recommendations for the implementation of Article 4 of the e-Privacy Directive. Based on this work, in 2013 the Data Protection Authorities of Greece and Germany, in collaboration with ENISA, developed an updated methodology for data breach severity assessment. The methodology can be used both by Data Protection Authorities (DPAs) as well as by data controllers. A working document is a first result of the co-operation between experts of the DPAs and ENISA. The methodology will ultimately be developed into a practical tool for data breach severity assessment.

Studies and reports:

Recommendations for a methodology of the assessment of severity of personal data breaches https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn-severity

2.1.2.5.2 Brokerage model of NIS in Education

With publication of the Brokerage model for Network & Information Security (NIS) in education report, ENISA aimed to provide content and promote digital education on network and information security at all levels. The target group is composed of educators such as trainers, teachers and peers involved in formal education and non-formal education, including lifelong learning. ENISA tries to connect the stakeholders in the best way possible by presenting different countries' perspectives via three case studies: the Czech Safer Internet Centre (NCBI)'s Strategy of community education in project — Prague safe online, the German Federal Office for Information Security (BSI)'s 10th anniversary of the Safer Internet Day provides an opportunity to increase awareness, and Norwegian partners' Norwegian Centre for Information Security.

Studies and reports:

Brokerage model for Network and Information Security in education

https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/brokerage-model-for-network-and-information-security-in-education/

2.1.2.5.3 Supporting the implementation of the EU Cloud Strategy

ENISA is involved in almost all EU activities implementing the Cloud Strategy. In this light ENISA has been supporting the Certification Special Interest Group (SIG) and in detail: ENISA published a paper summarising all activities of the SIG since its establishment, putting forward all the reasoning in favour of a common certification scheme for Europe. In parallel ENISA has been asked to support other activities of the strategy (e.g., the ETSI Standardization working group, the SLA SIG).

Studies and reports:

Certification in the EU cloud strategy

https://resilience.enisa.europa.eu/cloud-computing-certification/certification-in-the-eu-cloud-strategy

2.1.2.5.4 Ex-post analysis and learning capability for ICS SCADA

This report proposes a set of recommendations for developing a proactive environment at an appropriate level of preparedness with respect to ex post incident analysis and learning capability. ENISA identified several key activities that can contribute to this goal. They include facilitating the integration of cyber and physical response processes with a greater understanding of where digital evidence may be found and what would be the appropriate actions to preserve it; designing and configuring systems in a way that enables digital evidence retention; and complementing the existing skills base with ex post analysis expertise and understanding overlaps between cyber and physical critical incident response teams.

Studies and reports:

What can we learn from SCADA incidents?

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/can-we-learn-from-scada-security-incidents

2.1.3 Policy area Work Stream 3: Enabling communities to improve NIS

Enabling communities to improve NIS is a work stream that addresses the security of underlying internet communications. It does so not from the viewpoint of service providers, but from the viewpoint of the users of the internet services. The results of this work stream will be provided to network and internet security managers, as well as other communities that are responsible for implementing or validating security mechanisms. Results take the point of view of the "implementer". The beneficiaries of these activities are Information Security Officers in organisations, i.e. the "internal" security service providers.

2.1.3.1 General Objective Work Package 3.1: Application of good practice for CERTs

Impact Indicator 1: ENISA should improve the level of communication, response (appropriate to the threat level) and information exchange between European national/governmental (n/g) Computer Emergency Response Teams (CERTs) and other bodies (governmental organisations, industry and academia). Its recommendations should be adopted by a minimum of four Member States in 2014 (Source: Work Programme 2013).

Result achieved: improved levels of communication, response and information exchange were already adopted by 19 Member States during the two ENISA CERT Workshops in 2013.

Impact Indicator 2: ENISA should provide training to improve the operational practices of CERTs (on-going support with best practice development) to a minimum of 20 participants from different organisations (Source: Work Programme 2013).

Result achieved: ENISA CERT training was rolled out on request and on the Agency's initiative at more than 10 events, each attended by more than 20 participants, for a total participation of 200 people.

Impact Indicator 3: the improved collaboration capabilities of n/g CERTs (continuation of 2012 work) should be adopted by a minimum of four Member States in 2014 (Source: Work Programme 2013).

Result achieved: already adopted by 19 Member States during the two ENISA CERT Workshops in 2013.

Studies and reports:

D1	Secure communication's platform for European n/g CERTs (Requirements & stocktaking)	*Detect, SHARE, Protect - Solutions for Improving Threat Data Exchange among CERTs* https://www.enisa.europa.eu/activities/cert/support/data-sharing/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs
D2	EISAS – deployment in Europe (a feasibility study)	https://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas-deployment-feasibility-study
D3	Good practice guide on Alerts, Warnings and Announcements (including an inventory of Incident Response Methodologies)	*Best practice guide on Alerts, Warnings & Announcements* https://www.enisa.europa.eu/activities/cert/support/awa
D4	CERT Inventory; an extended overview (inventory and interactive map)	https://www.enisa.europa.eu/activities/cert/background/inv

D1 (Detect, SHARE, Protect): the focus of the report is on the threat and incident information exchange and sharing practices used among CERTs. It examines existing communication solutions and practices among European CERTs, identifying the functional and technical gaps that limit the exchange of threat intelligence between n/g CERTs and their counterparts in Europe, as well as other CERTs within their respective countries. The report also defines basic requirements for improved communications that are interoperable with existing solutions.

D2 (EISAS): the final report that concludes ENISA's activities in the area of European Information Sharing and Alerting System (EISAS).

D3 (Alerts, Warnings, Announcements): the guide describes good practices and provides practical information and guidelines on the process of preparing and issuing alerts, warnings and announcements to a CERT's constituencies (customers). Informing CERTs and their constituencies about threats and ways to contain threats typically involves the use of a reliable set of indicators and a well-structured process for assessing and processing the incoming information. This enables the CERT to get the right information to the right places in a timely fashion.

D4 (CERT Inventory): the inventory aims to provide an overview of the actual situation concerning CERTs in Europe. It provides a list and an interactive map of CERT teams and similar facilities by country, and also contains a catalogue of co-operation, support and standardisation activities related to them.

Example of value added:

In 2013, ENISA extended its good practice material for CERTs with a special emphasis on obstacles to information sharing. Currently, CERTs face not so much a lack of information (about incidents, vulnerabilities, threats, etc.) as difficulty in extracting useful, actionable pieces of information out of the abundance of available information (Netflow data, logfiles, etc.). At the end of 2013 (and continuing in 2014), ENISA actively participated in a project, led by governmental CERTs from Austria, Portugal and Belgium, designed to tackle this problem. A tool, "Abusehelper", was developed to help CERTs to extract actionable information from their data sources. The tool will be made available to all CERTs.

2.1.3.2 General Objective Work Package 3.2: Enabling collaborative communities

Impact Indicator 1: improved operational capabilities of n/g CERTs (continuation of 2012 work) should be adopted by a minimum of four Member States in 2014.

Result achieved: improved operational capabilities already adopted by 19 Member States during the two ENISA CERT Workshops in 2013.

Impact Indicator 2: ENISA will identify at least 20 key actors who can act as intermediaries in the dissemination of the outcomes of the work package. Together they should cover at least 12 Member States by the end of 2013.

Result achieved: 19 national/governmental CERTs in the EU acted as multipliers or intermediaries for the dissemination of work page results, including two n/g CERTS from EEA countries. The Forum of Incident Response and Security Teams (FIRST) and the Task Force for Computer Security and Incident Response Teams (TF-CSIRT) acted as additional multipliers, with 24 key actors disseminating results to at least 500 CERTs worldwide (members of FIRST, members of TF-CSIRT, teams on the national level, and teams in the start-up phase not yet registered anywhere).

Impact Indicator 3: pan-European cooperation shall be improved between CERTs and Law Enforcement Agencies (LEA) in the area of fighting cybercrime, with the commitment of a minimum of four Member States in 2013.

Result achieved: cooperation agreed upon by 19 Member States during the two ENISA CERT Workshops in 2013. The workshop series will be continued in 2014.

ENISA attending the FIRST international incident response conference

Studies and reports:

D1	Good practice guide on the practical implementation of the Directive on attacks against information systems	*A Good Practice Collection for CERTs on the Directive on attacks against information systems* https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/the-directive-on-attacks-against-information-systems
D2	8th Annual CERT workshop report (public version)	*8th ENISA Workshop 'CERTs in Europe' report* https://www.enisa.europa.eu/activities/cert/support/files/8th-enisa-workshop-certs-in-europe-report
D3	CERT exercise material - extended – cybercrime scenarios (handbook and toolset)	*ENISA CERT exercise material extended with cybercrime scenarios* http://www.enisa.europa.eu/activities/cert/support/exercise
D4	New version of Baseline capabilities framework – international harmonisation (Status report on capabilities harmonisation with worldwide stakeholders) and appropriate ICS-CERT capabilities	*Good practice guide for CERTs in the area of Industrial Control Systems* https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/ics-cerc/good-practice-guide-for-certs-in-the-area-of-industrial-control-systems *CERT communities - Recognition mechanisms and schemes* https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/cert-community-recognition-mechanisms-and-schemes/
D5	CERT training support (TRANSITS and ENISA training portfolio activities)	*No deliverable*

D1 (Good practice on Directive[6]): the report serves two major goals, both of which aim to support CERTs. Firstly, it aims to provide an analysis of the legal framework created by the Directive, coupled with a stock taking of existing national activities and good practices which may be relevant. Secondly, it aims to identify key areas and, when appropriate, guidelines and recommendations for CERTs derived from good practices. The document provides background information mainly for members of CERTs in the EU Member States. It explains the potential outcomes and implications raised by the new Directive. While it stops short of giving direct guidance for the implementation process, it will hopefully enable key players to take sound decisions.

D2 (Workshop report): the document is a brief ENISA report on the annual workshop for Computer Emergency Response Teams in Europe: *CERTs in Europe*. The first part of the workshop focused on hands-on technical training for n/g CERTs in Europe. The second part of the workshop, the ENISA/EC3 workshop, was a follow up event to last year's workshop with Europol. It had the same focus on enhancing cooperation between n/g CERTs in Europe and their national law enforcement counterparts.

D3: (CERT exercise material): ENISA CERT exercises and training material were introduced in 2008, and in 2012 and 2013 these were complemented with new exercise scenarios containing essential material for success in the CERT community and in the field of information security. The ENISA CERT training material contains a handbook for teachers, a toolset for students and virtual images to facilitate hands on training sessions.

D4: (Harmonisation and ICS CERT capabilities): the "harmonisation" document provides an overview of existing mechanisms that help CERTs to deploy capabilities necessary for their operations and appropriate to their level of maturity. It introduces each mechanism according to the CERT maturity level that it addresses, based on eight predefined criteria. The criteria include mandatory requirements for CERTs, their focus, the type of CERT or its region of operation, and the definitions and terminology used.

The Industrial Control System Computer Emergency Response Capabilities (ICS-CERC) guide builds upon the current practice of CERTs responsible for industrial control system (ICS) networks, as well as on earlier work by ENISA regarding baseline capabilities for n/g CERTs. The document is an initial attempt to provide a good practice guide for the entities that have been tasked to provide ICS-CERC. The guide does not, however, attempt to prescribe to the EU Member States which entities should be entrusted with provision of ICS-CERC services.

D5 (CERT training support): ENISA continues to support the successful TRANSITs[7] training programme for CERT staff members, which usually takes place twice a year in Europe. TRANSITs training programmes for CERTs evolved out of a European Commission funded project (IST-2001-39118, 1 July 2002-30 September 2005) to promote the establishment of CERTs by addressing the shortage of skilled staff. To complement this effort, in 2013 ENISA started to provide in-house technical training for CERTs and other operational communities (i.e. ICS administrators) based on requests from EU Member States. Tailored training programmes are based on ENISA exercises and training materials that have been developed by ENISA since 2008. ENISA's training portfolio complements our effort to strengthen CERT capabilities and to foster cooperation amongst teams throughout Europe.

6 European Commission. 2010. Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA. COM(2010) 517: http://ec.europa.eu/dgs/home-affairs/policies/crime/1_en_act_part1_v101.pdf [Last accessed 0ctober 14, 2013]

7 http://www.terena.org/activities/transits/transits-i/

Example of value added:

In 2008, ENISA decided to develop CERT training programmes as a more direct way of disseminating its CERT good practice material. Since then the number of available training scenarios has reached 23, and the programmes are highly regarded. In 2013, we received several requests from Member States for specialised training for their CERT teams, and this trend has continued in 2014. This is a strong contribution to the state of NIS in Europe that builds upon our work in defining baseline capabilities for national and governmental CERTs. The quality of our training programmes is high: participants typically give our programmes ratings of 4.5 out of 5 points. The real impact of the training, however, must be evaluated over the long-term.

2.1.3.3 General Objective Work Package 3.3: Enabling the information society

Impact indicator 1: ENISA should survey security certification practice in at least five Member States to identify best practices that could be applied for privacy certification/trustmarks (Source: Work Programme 2013).

Result achieved: the survey was conducted among 11 Member States, covering over 50% of the EU population.

ENISA has supported EU activities in the implementation of trustmarks by identifying best practice from security certification that can be deployed for privacy certification and trustmarks. Input was provided for the adoption of a framework on privacy certification, as well as for eGovernment certification in Europe. The conditions under which online security and privacy seals (OSPS) can be deployed to support users in making informed decisions about Web services and their providers with respect to the security and privacy provided were also analysed.

Studies and reports:

Security certification practice in the EU - Information Security Management Systems: A case study

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/security-certification-practice-in-the-eu-information-security-management-systems-a-case-study

On the security, privacy and usability of online seals

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/on-the-security-privacy-and-usability-of-online-seals/

Impact Indicator 2: ENISA should provide recommendations on best practice regarding the security of personal data and the use of cryptographic techniques for eGov services in Europe, based on inputs from at least five Member States (Source: Work Programme 2013).

Result achieved: input was gathered from five Member States, the US and other international stakeholders, and information was also provided by other Member States.

ENISA studied cryptographic techniques used in Europe, focusing on areas where data security is needed to protect the personal data of the citizens or on the new techniques required by new applications. The study addressed measures applied to safeguard sensitive and/or personal data, and discussed how information technology users with a basic knowledge of information security can employ cryptographic techniques to protect their personal data. It also addressed the need for a minimum level of cryptographic functionality across EU Member States, as part of their efforts to protect personal and/or sensitive data.

Studies and reports:

Recommended cryptographic measures – Securing personal data

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/recommended-cryptographic-measures-securing-personal-data

Algorithms, Key Sizes and Parameters Report

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report

Impact indicator 3: ENISA should support the proposal by DG CONNECT of the European Commission for a Regulation on electronic identification and trusted services for electronic transactions in the internal market, and involve at least five relevant stakeholders from public and private sectors (Source: Work Programme 2013)

Current situation (as achieved): ENISA has supported DG CONNECT by providing recommendations for maintaining acceptable levels of security at trust service providers (as agreed with the eIDAS Task Force). The study was written by five experts from different sectors and involved 57 organisations from within the EU. Nearly 80 stakeholders from various sectors validated the studies at the Trust Service Provider workshop in September 2013.

In 2013, ENISA developed guidelines for trust services providers, identifying the minimal security levels to be maintained by them. The study is divided into several sections. One section describes the framework for trust service providers (TPSs), drawing upon EU and other standards when relevant. A second section discusses the principles and concepts for defining and controlling the threats and vulnerabilities faced by TSPs. A final section recommends technical and organisational measures for mitigating the impact of security incidents on TSPs.

Studies and reports:

Guidelines for trust service providers - Part 1: Security framework

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp1-framework

Guidelines for trust service providers - Part 2: Risk assessment

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp2-risk

Guidelines for trust service providers - Part 3: Mitigating the impact of security incidents

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp3-incidents

2.1.3.4 Other Work Stream 3 actions

In addition to the activities planned in the Work Programme, ENISA performed actions in the framework of Work Stream 3.

2.1.3.4.1 Data retention

Data retention legislation has been adopted to address concerns related to national security and serious criminal activity. The legislation provides access to communication data for law enforcement purposes. However, the Data Retention Directive (DRD) requires that personal data collected, stored or in any way processed in most EU Member States be securely protected. In 2013, ENISA conducted a survey on the national implementation of the DRD in six selected Member States. The survey focused on technical and organisational security requirements and the implementation of the data security principles that are provided for in the Directive. It also provided a state-of-the-art analysis of the security measures proposed for the protection of personal data.

Studies and reports:

Securing personal data in the context of data retention

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/securing-personal-data-in-the-context-of-data-retention/

2.2 SPECIFIC EFFORTS TO IMPROVE THE 'ECONOMY' AND 'EFFICIENCY' OF SPENDING AND NON-SPENDING ACTIVITIES.

According to the financial regulation (art 30), the principle of economy requires that the resources used by the institution in the pursuit of its activities shall be made available in due time, in the appropriate quantity and quality and at the best price. The principle of efficiency entails finding the optimal balance between the resources employed and the results achieved.

These principles are upheld through the implementation of internal procedures and predefined practices. These procedures ensure that activities are executed in an efficient manner (e.g. different workflows contribute to efficient cooperation between staff, units, departments etc.) and according to the principle of economy (e.g. procurement rules ensure procurement on optimal terms).

The Agency continuously fine-tunes its internal arrangements in order to improve the efficiency and economy of its operations. The following two initiatives are examples that show how these principles are implemented at ENISA.

2.2.1 Example 1

To operate efficiently at two different locations, electronic workflows had to be designed and implemented. These workflows are more economical than sending large packages by post and more efficient because delays have been eliminated. The idea is to establish a fully digital organisation with lean procedures and optimal functionality.

2.2.2 Example 2

To operate efficiently at two different locations, IT tools such as videoconferencing were implemented. These types of tools are more economical than spending budget on travel and more efficient because issues can be resolved more quickly. This applies to several different core processes (management team meetings, tender procedures, etc.).

Other IT tools such as the Agency's intranet enable different actors to work simultaneously on the same document while storing all versions in a single location.

2.3 CORPORATE COMMUNICATIONS

2.3.1 Corporate Communications, media, outreach and impact

ENISA's impact, outreach and media programme gives the Agency the opportunity to reach many more of its stakeholders than it can through direct means. **Corporate communication activities in 2013 focused on five areas:**

1. Expanding and increasing media impact and coverage across Europe
2. Strengthening stakeholder relations
3. Strengthening digital communications
4. Ensuring coherence and consistency, i.e. communication planning
5. Strengthening the ENISA brand

Thus, in 2013, the Agency's corporate communications section continued to focus on communicating the Agency's results in its studies and reports, its core operations results. At the same time, in 2013, ENISA was reorganised so that the Public Affairs Unit (PAU) become a Corporate Communications team. The objective was to streamline activities and adapt to a new context, in view of other organisational developments, most notably the transfer of some Agency staff to Athens. Major achievements included the transition to and implementation of the new ENISA logo and new Agency name, in line with the new Regulation governing the Agency. In addition, the Agency web site and social media activities were further developed as the Agency's main communications channels. This year we also cooperated more closely with local and national media across Europe, resulting in TV coverage, editorials in the press and articles published in numerous media outlets. Corporate communications in particular gained Europe wide coverage for the ENISA Threat Landscape report, and the art13a annual incidents in the telecoms sector report.

As the focal point for Europe's cyber security information, corporate communications focus on communicating the results of ENISA's operational work. The communication objective is to reach diverse stakeholders and audiences, using the appropriate channels and with consistent messages that are tailored to each target audience. This approach is a key element of ENISA's mission to support a cyber-security culture, in order to promote a dynamic digital society and, ultimately, for the economy of Europe. ENISA's

corporate communication outreach channels include public relations campaigns, digital communications, external communications, and media activity and events across the EU.

ENISA High Level Event

Expanding and increasing communication and external relations by working with various audiences was, therefore, a pivotal point for corporate communications in 2013. To do so, the Agency co-organised or participated in joint events with other EU bodies and other organisations. The most outstanding example at corporate level was the annual High-Level Event in Brussels, which was organised in cooperation with an industry actor the European Security Round Table (ESRT), and a regional actor, the Hessen Representation. At this occasion, ENISA brought together representatives of the European Data Protection Supervisor (EDPS), the European Commission and industry. Under the umbrella of "Securing our cyber-future: risks, threats, challenges & opportunities for coordinating Europe's cyber security", topics discussed included:

- The new ENISA Regulation (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF) - what it actually means for improving Europe's cyber security
- The Cyber Security Strategy and NIS Directive (http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security) - the practicalities of implementation
- The implications of state surveillance revelations for IT security - what should be the technical response and what are the future needs?"

This generated unprecedented interest in the event, which was therefore a great success for the Agency stakeholder relations, in providing a platform for our stakeholders to meet.

Strengthening our external relations through communication with various audiences was a major part of the Agency's corporate communications work in 2013. To do so, the unit organised or participated in joint events with other EU bodies, such as the high-level cyber event in Brussels. This ENISA event brought together representatives of the European Parliament, the European Commission and industry. The Agency also engaged in outreach work, particularly with the local community, such as organising a Europe Day on 9 May, a celebration on Crete to highlight the benefits of information and communication technology for all of Europe's children. The corporate communications team has also worked to further strengthen ties with Greece's government, which hosts the Agency in Heraklion and Athens. Moreover, in 2013, ENISA engaged in strengthend relations with the Regional Governor of Crete and the Heraklion local authorities.

ENISA celebrated Europe Day

Media relations is the superior way to reach all Agency stakeholders. It articulates our results, and augments the cyber security debate. ENISA's impact, outreach and media programme enables the Agency to reach all its stakeholders, and influential policy makers, who follow the media. Through media relations ENISA can reach many more persons than, for example, at a conference. Today, in media relations there has been a blending between traditional, social media and digital relations with our stakeholders. All these channels are crucial to reach the media, who can act as multipliers of our message, as well as contribute to the open debate on cyber security in a democratic society.

In 2013, the Agency continued its outreach distribution and media monitoring process to assess the targeting, impact and reach of its media work. Major accomplishments include:

- Produced and issued 20 media releases
- Posted more than 115 individual news items on the ENISA web site
- All media releases and news items are simultaneously published in the Agency's social media channels and also generated hundreds of interviews throughout the year. Overall, the media coverage figures were around 2,500, which was an increase of about 25% in relation to 2012's figure.

2.3.2 Multilingual approach

An essential part of ENISA's work is to make its messages accessible to stakeholders across Europe and to overcome the "Tower of Babel", which is simultaneously a blessing of cultural diversity, but also a challenge. To tackle this challenge, the Agency issues media releases in five EU languages – English, German, French, Spanish and Greek – to press, radio, television and web-based news organisations. It also maintains online "landing pages" in German, French and Greek. ENISA media releases are distributed via general, financial, EU and social media outlets, as well as specialised ICT/Network and Information Security publications and web sites. In 2013, ENISA further developed and enhanced the three "landing pages" in Greek, German and French. More mini sites are planned for launch in 2014.

2.3.3 Cross media impact

Media monitoring analysis and in depth-evaluation of the Agency's media output shows that overall in 2013 the media work and translations generated more than 2,500 stories in European news media, and that stories appeared in all 24 EU languages. Statistics continue to display a clear correlation between peaks in web visitors, social media and the distribution of media releases in multiple channels. This demonstrates the beneficial effect of multiple media channels in spreading the results of the Agency. Overall, ENISA reached a combined potential audience of several million readers, listeners and viewers. Directly, media releases on the ENISA web site received more than 223,000 unique page views in 2013, a clear increase over the 171,000 unique page views received in 2012. Individual news stories on the ENISA website received more than 84,500 direct hits in 2013.

2.3.4 Additional media & outreach activities

Other dedicated topical press conferences and briefings targeted media in specific countries or around particular interest areas in network information security. As part of its media activities, the Agency also commenced the regular update of the Crisis Communication Strategy. In addition, the agency maintained and further developed its relations with other EU agencies, in the official Heads of Communications and Information Network (HCIN) of the EU agencies. The HCIN gives EU agencies the possibility of pooling their knowledge, benchmarking, learning and sharing best practices. This is a cost-effective way to continuously develop standards and learn for greater impact.

2.3.5 Digital communications and digital relations

ENISA's website continues to be the Agency's principal communications channel. In 2013, continuous development work was carried out to maintain and further improve the website for its users. The Agency social media channels – Facebook, LinkedIn, Twitter and YouTube – were expanded to include Slideshare and Pinterest in order to reach more stakeholders. Moreover, after analysis, a survey of the literature, and practical "lessons learned", we modified our tactics to increase our social media outreach further. These steps have enabled ENISA to better reach targeted NIS communities and the media, to increase our outreach, and to foster better digital stakeholder relations. This was a dedicated effort and new initiative in 2013 that helped us to better connect with new communities and to develop our ties with existing digital relations with our stakeholders and supporters.

Website development

Enhancing the website for users and helping visitors to navigate and find information with greater ease is an on-going process. To this end, the agency continued to improve the usability and design of the ENISA website. Further enhancements and improvements will be carried out on the website in 2014, including an improved content structure, and further development of the German and Greek mini-sites, and a new Spanish one.

Technical improvements in 2013 included the development of web tools for the Agency's website and portals (used by specialist expert communities) and the application of all the security patches to the Zope application and PLONE content management system used by the ENISA site.

A dedicated portal for the European Cyber Security Month (ECSM) was also launched during 2013, to better support the ECSM initiative and its constantly growing community.

2.3.6 Social Media

ENISA's social media channels (Facebook, Twitter, YouTube, LinkedIn) were launched in September 2012. The objective was to connect the Agency with new communities, deepen its ties with existing ones and generate traffic to ENISA's main site for increased visibility, impact and influence. The channels are accessible through the Agency's website (home page) and links to them were also added to all the Agency's communication channels (publications, presentations, e-mails, brand material, etc.)

During 2013, ENISA's social media presence was enhanced with two new channels - Pinterest and Slideshare – while new tools and methods were introduced to help ENISA to better distribute its work.

Social media monitoring reports have shown an increased reach for ENISA's channels. Main accomplishments include:

- More than 3,250 followers of the ENISA Twitter channel
- More than 1,260 tweets
- 2,400 followers of the ENISA LinkedIn page
- More than 600 Facebook fans
- 7,700 YouTube video views
- Hundreds of thousands of users reached by messages posted by ENISA

2.3.7 Video

In 2013, the Agency produced videos covering key areas of agency activity. For 2014, ENISA envisages further production of shorter video clips to promote the Agency's achievements and activities.

2.3.8 Quality, coherence and consistency

In 2013, the corporate communications team ensured that ENISA's corporate communications activity was fully aligned with ENISA's operational and policy development goals. Amongst other actions, this entailed maintaining and developing close links with the Management Board, the PSG, the European Parliament, the European Commission, the Council and Member States. All communications activity falls within the scope of five planned corporate communications areas of activity. This ensures that information forms part of a coherent and consistent narrative on the Agency's work. In addition, the continuing provision of high quality editorial, graphic design and printing services through contracts managed by corporate communications, has helped to ensure quality, coherence and consistency in ENISA's communications.

2.3.9 Brand and trust

Given the inherent nature of ENISA's mission, branding is an important aspect of Corporate Communication's work. A strong ENISA brand increases trust. Trust helps the Agency to achieve consistent and coherent results in all its communications, and is a precondition for its stakeholder relations. The ENISA brand was strengthened in 2013 through several means:

- **Visual identity:** the ENISA brand's visual identity was updated and implemented to reflect the new Agency name and logo.
- **Events:** to increase awareness and recognition of the ENISA brand, events were conducted across Europe.
- **Promotional material:** promotional material was produced for particular corporate and expert occasions and distributed at the High Level event and to visitors to ENISA's offices.

An effective brand strategy is key to connecting effectively with our audiences and stakeholders. Therefore, continuously updating the look and feel of ENISA material is paramount in the way the Agency communicates and to how it is perceived.

2.3.10 Publications

Publications are the 'face' of the ENISA brand and an important communication tool given ENISA's mission. Throughout 2013, the Agency published around 30 publications as work programme deliverables. In addition, ENISA went beyond by producing additional reports, papers and studies. Along with the writing and design of the Agency's General Report, in 2013, the Corporate Communications team produced a special corporate report for the ENISA high-level event in Brussels, EU *Cybersecurity cooperation - Defending the digital frontline* (http://www.enisa.europa.eu/media/key-documents/cybersecurity-cooperation-defending-the-digital-frontline). The report presented an updated and comprehensive overview of Europe's cyber security status, and examined areas where further cooperation can better secure digital economy of Europe.

In 2013, the Corporate Communications team worked with the Agency's NIS experts to step up the frequency of the Agency's Flash Notes – short expert reports published to provide an analysis or comment on a current cyber security topic not foreseen in the Work Programme. Notes included the topics of "Cyber-attacks – a new edge for old weapons", "Urgent action is needed to combat emerging cyber-attack trends", the Flash Note Can Recent Attacks Really Threaten Internet Availability? (http://www.enisa.europa.eu/publications/flash-notes/flash-note-can-recent-attacks-really-threaten-internet-availability) and "Internet Service Providers fail to apply filters against big cyber attacks".

Theses Flash Notes were extremely well received because of their timeliness. Thus, the Agency will continue this practice in 2014.

2.3.11 Conferences and events

Throughout the year, ENISA organised several conferences and events. In addition, the Agency took part in numerous external events and high-level European conferences. In addition to these activities, the Corporate Communications team provided support to the Executive Director for his participation in events across Europe.

ENISA Management Board Meeting in Vilnius

2.3.12 ENISA Stakeholder relations, media and corporate communications

ENISA's stakeholder relations are a key factor in the success of its overall mission of contributing to the security of the EU internal market. The Management Board (composed of the Commission, Member State and private sector representatives) and Permanent Stakeholders Group (composed of multiple stakeholders), as well as the Agency's informal networks and expert working parties, give ENISA unparalleled insights and access to public and private sector Network and Information Security (NIS) experts. This expertise and "checking point" also gives ENISA the opportunity to better and more rapidly identify emerging risks and gain new insights. This helps the Member States and private sector organisations to better prepare themselves for challenges in a proactive and professional manner, as well as to build novel public and private sector partnerships. Excellent relations with our stakeholders is also the flip side of the coin in relation to media, outreach and impact; good quality in our stakeholder relations depends on a genuine two way dialogue, attentiveness to and interest in our stakeholders' needs and priorities.

2.4 IT AND FACILITIES MANAGEMENT

New Branch Office in Athens

In March 2013, ENISA opened its new branch office in Athens. The new office was made operational in about five weeks using limited resources while waiting for additional budget approval. The move of all operational staff from Heraklion to Athens was completed without any interruption in functioning or any impact on productivity. In the meantime, planning went ahead regarding the refurbishment and furnishing of the office, including IT and facilities equipment and services.

A restricted call for tenders was launched in late 2013 for refurbishment work.

IP Telephony and Unified Communications

In early 2013, ENISA's telephony was integrated into the Lync system, which was already used for collaboration and online meetings. Thanks to this development, calling costs have decreased while additional functionality and flexibility have become available. For example, staff can make business calls from their desktop, even while travelling, as long as they have an Internet connection.

Align IT organisational structure and processes to ITIL standards

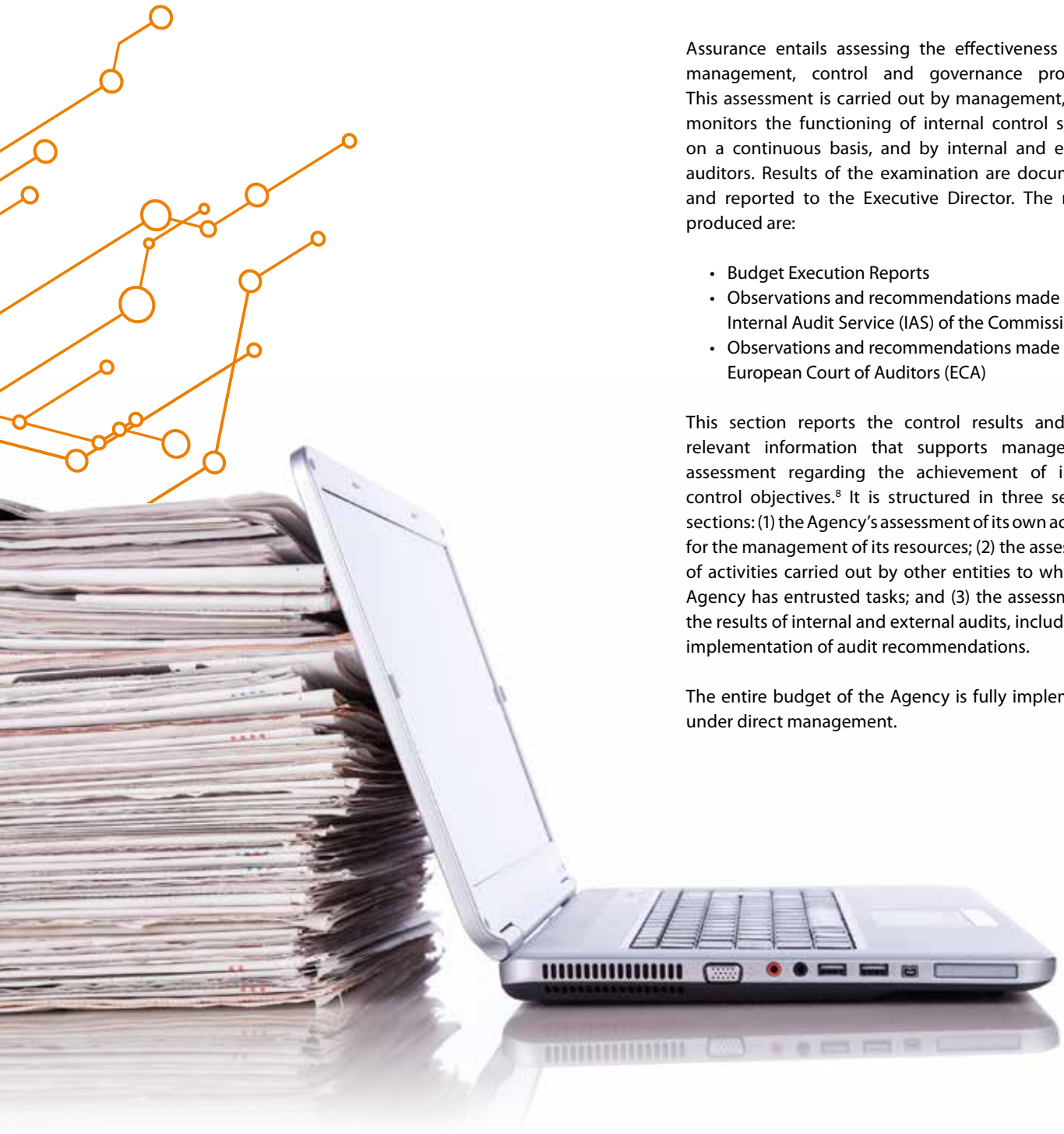
Changes to the structure of the IT budget were introduced in 2013 to better align it with IT service lifecycle stages. This approach will be finalised in 2014 and should provide better visibility on the maturity level of our IT organisation by comparing the time spent by the IT staff for development, evolution and business alignment versus the time spent for operating, supporting and recovering from failures.

Cyber Exercise Platform (CEP)

In 2013, IT contributed to ENISA's European Cyber Exercise. IT designed and delivered a complete infrastructure to run the Cyber Exercise campaigns. The pilot exercises were successfully conducted on this infrastructure. IT supports and continues to enhance this important platform in order to host future exercises. In 2014, about 500 users are expected to connect and use the platform during exercise sessions.

3

MANAGEMENT OF RESOURCES



Assurance entails assessing the effectiveness of risk management, control and governance processes. This assessment is carried out by management, which monitors the functioning of internal control systems on a continuous basis, and by internal and external auditors. Results of the examination are documented and reported to the Executive Director. The reports produced are:

- Budget Execution Reports
- Observations and recommendations made by the Internal Audit Service (IAS) of the Commission
- Observations and recommendations made by the European Court of Auditors (ECA)

This section reports the control results and other relevant information that supports management's assessment regarding the achievement of internal control objectives.[8] It is structured in three separate sections: (1) the Agency's assessment of its own activities for the management of its resources; (2) the assessment of activities carried out by other entities to which the Agency has entrusted tasks; and (3) the assessment of the results of internal and external audits, including the implementation of audit recommendations.

The entire budget of the Agency is fully implemented under direct management.

8 Effectiveness, efficiency and economy of operations; reliability of reporting; safeguarding of assets and information; prevention, detection, correction and follow-up of fraud and irregularities; and adequate management of the risks relating to the legality and regularity of the underlying transactions, taking into account the multiannual character of programmes as well as the nature of the payments (FR Art 32).

3.1 MANAGEMENT OF HUMAN AND FINANCIAL RESOURCES BY ENISA

3.1.1 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 exclusively on the verification of results before transactions are initiated ("ex-ante verification").

The European Court of Auditors (ECA) is responsible for implementing a second layer of controls. The ECA audits a sampling of all the transactions that have been conducted ("ex-post audit"). They then issue a report with their findings. For several consecutive years, the ECA has not found any issues that required it to issue findings on the Agency's transactions. This suggests that ENISA's 100% ex-ante verification strategy is very effective. Nevertheless, as soon as the Agency has more human resources available, bi-annual ex-post controls exercises will be instituted in order to strengthen controls regarding legality and regularity.

3.1.2 Fraud prevention and detection

The Agency is developing its anti-fraud strategy as foreseen in the Commission's overall anti-fraud strategy[9]. The strategy will be implemented before the end of 2014.

3.2 ASSESSMENT OF AUDIT RESULTS AND FOLLOW UP OF AUDIT RECOMMENDATIONS

3.2.1 Internal Audit Service (IAS)

In 2013, the Internal Audit Service (IAS) visited ENISA. The IAS carried out an audit on project management in ENISA's operations. At the end of the IAS visit, five recommendations were issued. The Agency took prompt action on these five recommendations. In fact, as of the first quarter of 2014, the IAS had already advised closure of four of the recommendations, while the last recommendation only requires further validation at the Agency's premises.

The Internal Control Coordinator role (ICC) was fully deployed by September 2013. Due to a lack of staff, the Agency uses resources shared across the Agency to ensure that all procedures are addressed. The implementation and subsequent closure of open recommendations was the first priority for the ICC, and the Agency was able to close several recommendations.

Some of the recommendations require validation at ENISA. The Agency and the IAS agreed that all of these recommendations were properly addressed and that they will be verified during the third quarter of 2014.

A schedule was agreed upon to assure that all recommendations are closed by the third quarter of 2014.

3.2.2 European Court of Auditors (ECA)

The European Court of Auditors (ECA) issued two important recommendations regarding ENISA in 2012. One recommendation concerned the need to improve the transparency of recruitment at ENISA's new office in Athens, while the other concerned the need to improve the management of fixed assets. After the first visit by the ECA in March 2013, the Agency took all necessary measures to assure completely transparent recruitment procedures, and the recommendation concerning the transparency of recruitment was closed by the ECA.

9 COM(2011) 376 24.06.2011.

The last recommendation concerning the management of fixed assets will be evaluated during the ECA's visit in April 2014. A full physical inventory was conducted, in line with the rules in practice, across both Agency premises in Heraklion and Athens. The retirement exercise, which included the reconciliation of fixed assets with the accounts, was successfully realised.

The ECA's visit of April 2014 will include the audit of the 2013 accounts. The ECA is expected to issue its final report in the third quarter of 2014. 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 last seven years.

4

ASSESSMENT OF THE EFFECTIVENESS OF THE INTERNAL CONTROL SYSTEMS

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 2013, 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 2013, the Agency achieved compliance with the internal control standards listed below.

Mission (ICS 1)

The Agency's mission and scope is described in the ENISA Regulation. Mission statements for departments and units were established based on the evolution of the organisation in 2013. The roles and tasks of each department and unit are clearly defined.

Ethical and organisational values (ICS 2)

The Agency has procedures in place – including updates and yearly reminders – to ensure that all staff 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.

Staff Allocation and Mobility (ICS 3)

Whenever necessary – at least once per year – management aligns organisational structures and staff allocations with priorities and workload.

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 Career Development Plan (CDP) 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.

Objectives and Performance Indicators (ICS 5)

Work Programme and budget preparation procedures were developed in 2009 and will be 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 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. 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 to rectify the budget under-spending highlighted by the IAS in 2009, by optimising budget execution in four following consecutive years. The commitment rate of budget appropriations available for the year 2013 (C1) reached 99.99%, another consecutive year in which the total Agency budget was consumed.

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 2013, 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.

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 five 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.

Processes and Procedures (ICS 8)

Several policies were developed to strength 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.

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 Executive Director's decision on the Register of Exceptions Procedure was updated.

As the Agency lacks the resources to execute ex-post control, a strategy of 100% ex-ante controls was decided upon and applied.

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 medium-term objectives of the Agency. A list of action items is compiled. It contains all agreed actions as allocated to specific departments or units. The list is published on a dedicated Intranet page and regularly reviewed by the Management Team. 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.

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.

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.

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.

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 has been used since 2011 for the management of ENISA's inventory.

Financial management information produced by the Agency, including financial information provided in the Annual Activity Report, complies with applicable financial and accounting rules.

Evaluation of activities (ICS 14)

Key performance indicators are used in order to measure the performance and assess the impact of the Agency's projects as provided for in its Annual Work Programmes. The General Report and the Annual Activity Report are the tools used by the Agency to report on performance and impact. The feedback of relevant stakeholders is taken into account.

Assessment of internal control systems (ICS 15)

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

Internal Audit Capability (ICS 16)

The Head of the 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, hierarchical controls and outsourced engagements, coordinated by the ICC.

In line with the Strategic Audit Plan 2013-2015, the Internal Audit Service (IAS) carried out an audit on Project Management in Operations at ENISA.

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 on-going effort, as part of the continuous improvement of management procedures. It includes taking into account any control weaknesses reported and exceptions recorded.

5

MANAGEMENT ASSURANCE

5.1 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 definitions

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 below:

	Systemic process	Activity	Performance indicator
1	Follow up on auditor's comments and recommendations regarding ADM practices and procedures as they are implemented in line with Financial Regulation (FR), Implementing Rules (IR) and Staff Regulations (SR).	Update of documents and activities reporting.	Feedback by auditors in the next application period and overall improvement of performance.
2	Opening and closing of the annual budget and preparation of budgetary statements.	Approved budget tree opened, appropriations posted properly.	Annual budget lines open and running by the end of the year with the anticipated budget, economic outturn account and supporting operations completed in time.
3	Implementation and consolidation of internal controls, as appropriate.	Annual review of internal controls.	Guidelines and checklists reviewed, annual risk assessment done. Controls updated accordingly. Staff participation and information.
4	Performance evaluation	Organise annual performance evaluation. Administer appeals	Number of evaluations carried out.
5	Annual training programme	Draft the generic training plan of the Agency.	Document presentation and implementation of programme.
6	Recruitment plan	Execute the Agency recruitment plan in line with the Establishment Plan.	Number of staff hired to cover new posts or make up for resignations.
7	Internal ICT networks and systems	Secure ICT networks and systems in place.	Results of external security assessment/ audit.
8	Public procurement	Regular, consistent observation of public procurement practices and appropriate assistance provided to all departments.	Clear mandate of the procurement function established, staff informed, forms available, number and type of procurement processes handled, files of procurement processes organized, 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	Developed with the assistance of the professional service provider.	Number of transactions as compared to number of erroneous transactions.

Exceptions

In 2013, the Agency faced three main categories of deviation that led to exceptions reported in the Register of Exceptions:

- A posteriori commitments
- Procedural errors
- Missions guideline interpretation

The main reasons associated with the a posteriori commitments were limitations in planning.

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.

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[10].

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 institution .

Heraklion, 17/06/2014

[signed]

Udo Helmbrecht
Executive Director

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

ANNEXES

ANNEX 1: HUMAN AND FINANCIAL RESOURCES

Code ABB Activity	ABB Activity	Full Time Equivalents (FTE)
Work Stream 1	Evolving Risk Environment & Opportunities	3.1
Work Stream 2	Improving Pan-European CIIP & Resilience	11.9
Work Stream 3	Enabling Communities to improve NIS	10.0
SR	Stakeholder Relations	2.5
PS	Project Support Activities	0.6
PAU	Public Affairs Activities	3.9
None	Management & support activities	8.0
	Total	**40.0***

* Staff directly involved in the implementation of the Annual Work Programme

Financial resources

In 2013, the Agency allocated its appropriations at a rate of 99.99% (considering the non-automatic carry overs as committed on 31/12/2013), repeating the performances of 2012, 2011 and 2010. The efficient planning of Work Programme projects and relevant procurement procedures, allowed the Agency to carry out its operational activities as specified in the Work Programme 2013 within the year 2013, and to make the investments needed to ensure an appropriate operating environment, compliance with the regulatory framework and the continued provision of services by the Agency.

Payments reached the level of 91.6% of the total committed appropriation and 86% of the total appropriations for 2013. In addition, the payment rate of the appropriations carried forward from 2012 reached the level of 92%. These figures demonstrate the strong effort made to finalise administrative and operational activities and deliverables within the financial year. Both commitment and payment rates confirm the sustained capacity of the Agency to efficiently utilise its annual budget, given that the appropriations of the Agency are non-differentiated. An overview of the year's performance follows below:

Total EU Subsidy – C1

Budget Title	Description	Budget ('000 EUR)	Committed ('000 EUR)	%	Paid ('000 EUR)	%
Title 1	Staff expenditure	5,743	5,743	100%	5,545	97%
Title 2	Administrative expenditure	1,389	884	64%	568	41%
Title 3	Operational expenditure	1,898	1,898	100%	1,695	89%
Total		**9,030**	**8,525**	**94%**	**7,807**	**86%**

External Assigned revenue (rent subsidy from Hellenic Republic) – R0

Budget Title	Description	Budget ('000 EUR)	Committed ('000 EUR)	%	Paid ('000 EUR)	%
Title 2	Administrative expenditure	640	640	100%	340	53%
Total Budget		**640**	**640**	**100%**	**340**	**53%**

Carry forward (N+1) – C8 or C3

Type	Budget	%
Automatic Carry Forwards to year N+1 (C8)	718	7.95%
Non-automatic Carry Overs to year N+1 – on MB decision[1] (C3)	505	5.59%
Adjusted Commitments' rate[2]		**100%**
Adjusted Payments' rate[3]		**100%**

1 This amount corresponds to two calls for tenders launched in 2013 for works necessary for Athens office refurbishment (tentative cost 480,000 EUR) and for the lease of optical fibre line for Athens office (tentative cost 24,934 EUR); both contracts will be awarded in 2014. The amount was carried over to 2014 with the approval of the Management Board, and committed in March 2014.

2 The adjusted commitments' rate corresponds to rate of the sum of actual commitments made plus the non-automatic carry overs over total C1 appropriations (EU subsidy received in 2013). The rent subsidy received by the Hellenic Republic is excluded as it is a separate source of revenue.

3 The adjusted payments' rate corresponds to rate of the actual payments made over the actual commitments made on C1 appropriations (EU subsidy received in 2013). It excludes the amount of the non-automatic carry over (504,934 EUR) as it was not available for payment. The rent subsidy received by the Hellenic Republic is excluded as it is a separate source of revenue.

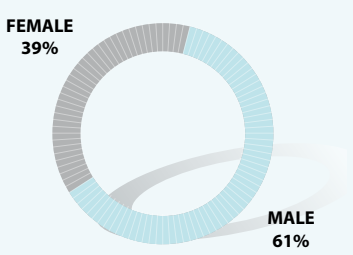
The initial Budget of ENISA was amended twice in 2013 in order to include:

- The amount of 480,632 EUR requested to the Budgetary Authority for the estimated refurbishment works and other investments needed for the new Athens office.
- The amount of 640,000 EUR granted as a rent subsidy by the Hellenic Republic by a Greek Law and a subsequent ministerial decision of the Minister of Infrastructure, Transport and Networks signed in September 2013.

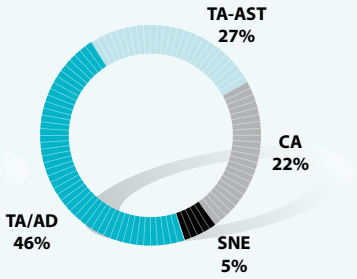
Statistics on ENISA staff

As of 31/12/2013, ENISA counts 59 Staff members: 43 TA's (27 AD's and 16 AST's), 13 CA's and 3 SNE's.

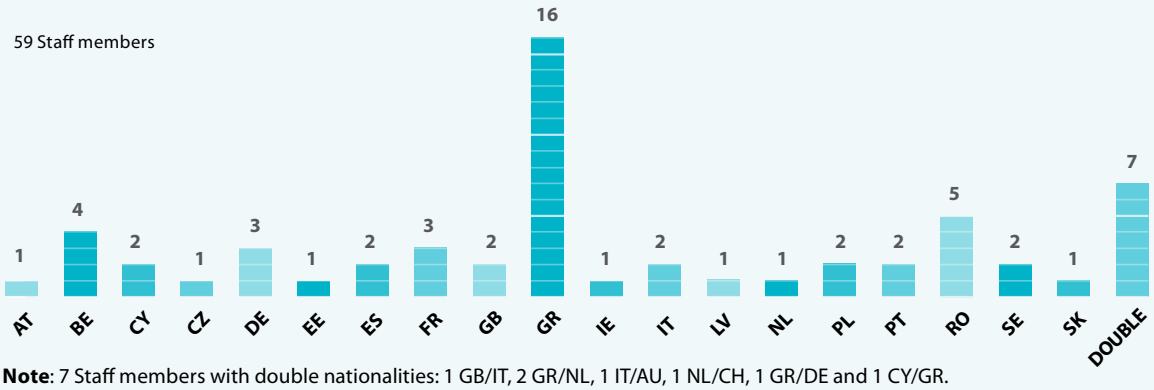
STAFF MEMBERS BY GENDER



STAFF MEMBERS BY FUNCTION GROUP

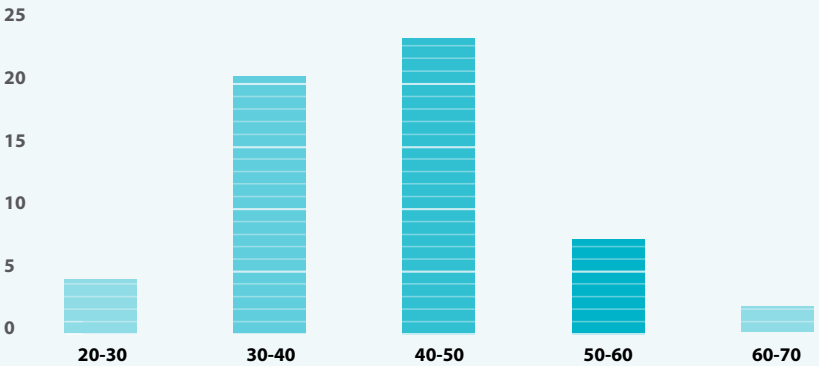


STAFF MEMBERS BY NATIONALITY



Note: 7 Staff members with double nationalities: 1 GB/IT, 2 GR/NL, 1 IT/AU, 1 NL/CH, 1 GR/DE and 1 CY/GR.

AGE ANALYSIS



ANNEX 2: DRAFT ANNUAL ACCOUNTS AND FINANCIAL REPORTS

Table 1: Outturn on C1 and R0 commitment appropriations in 2013 (in Mn. EUR)

Chapter		Commitment appropriations	Commitments made	%
		1	2	3=2/1
Title A-1	**STAFF**			
A-11	Staff in Active Employment	4.79	4.79	100.00%
A-12	Recruitment Expenditure	0.42	0.42	100.00%
A-13	Socio-medical Services and Training	0.08	0.08	100.00%
A-14	Temporary Assistance	0.45	0.45	100.00%
Total Title A-1		**5.74**	**5.74**	**100.00%**
Title A-2	**FUNCTIONING OF THE AGENCY**			
A-20	Buildings and Associated Costs	1.46	0.98	67.04%
A-21	Movable Property and Associated Costs	0.10	0.10	100.00%
A-22	Current Administrative Expenditure	0.05	0.05	100.00%
A-23	Information and Communication Technologies	0.43	0.41	94.22%
Total Title A-2		**2.03**	**1.52**	**75.11%**
Title B0-3	**OPERATING EXPENDITURE**			
B3-0	Group Activities	0.65	0.65	100.00%
B3-2	Horizontal Operational Activities	0.18	0.18	100.00%
B3-6	Core Operational Activities	1.06	1.06	100.00%
Total Title B0-3		**1.90**	**1.90**	**100.00%**
TOTAL %		**9.67**	**9.17**	**94.78 %**

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

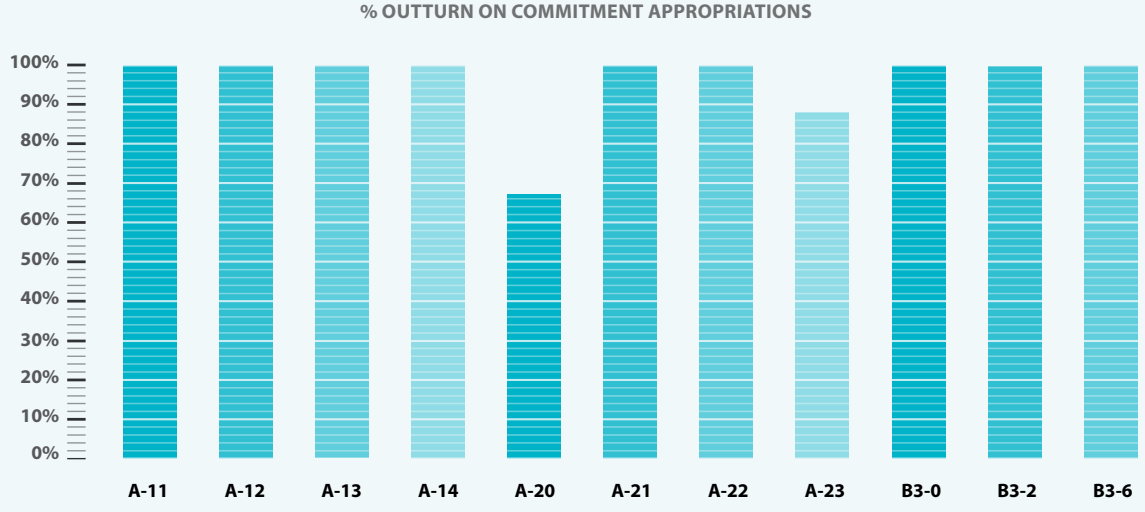


Table 2: Outturn on payment appropriations in 2013 (in Mn. EUR)

Chapter		Payment appropriations	Payments made	%
		1	2	3=2/1
Title A-1	**STAFF**			
A-11	Staff in Active Employment	4.79	4.79	100.00%
A-12	Recruitment Expenditure	0.46	0.41	87.31%
A-13	Socio-medical Services and Training	0.10	0.08	77.50%
A-14	Temporary Assistance	0.54	0.41	75.91%
Total	**A-1**	**5.90**	**5.69**	**96.39%**
Title A-2	**FUNCTIONING OF THE AGENCY**			
A-20	Buildings and Associated Costs	1.51	0.68	44.69%
A-21	Movable Property and Associated Costs	0.11	0.03	24.04%
A-22	Current Administrative Expenditure	0.07	0.06	94.71%
A-23	Information and Communication Technologies	0.58	0.38	65.69%
Total	**A-2**	**2.27**	**1.15**	**50.53%**
Title B0-3	**OPERATING EXPENDITURE**			
B3-0	Group Activities	0.76	0.63	82.60%
B3-2	Horizontal Operational Activities	0.35	0.30	84.77%
B3-6	Core Operational Activities	1.09	1.03	94.82%
Total	**B0-3**	**2.19**	**1.95**	**89.01%**
TOTAL %		**10.37**	**8.79**	**84.78%**

* Payment appropriations authorised include, in addition to the budget voted by the legislative 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).

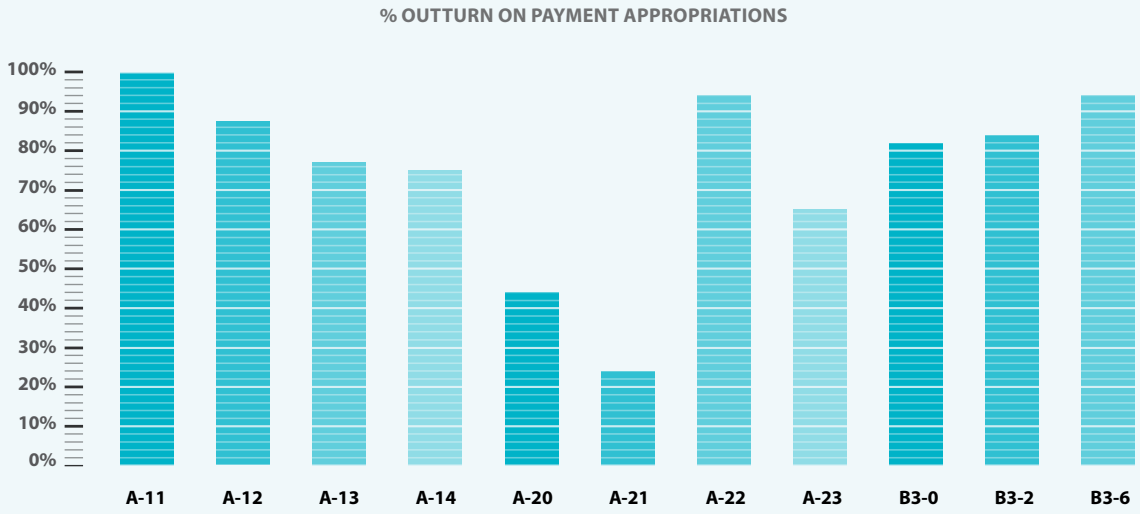


Table 3: Breakdown of commitments to be settled at 31/12/2013 (in Mn EUR)

2013 Commitments to be settled

Chapter		Commitments 2013	Payments 2013	RAL 2013	% to be settled
		1	2	3=1-2	4=1-2//1
Title A-1	**STAFF**				
A-11	Staff in Active Employment	4.79	-4.79	0.00	0.00%
A-12	Recruitment Expenditure	0.42	-0.36	0.06	13.98%
A-13	Socio-medical Services and Training	0.08	-0.06	0.02	23.54%
A-14	Temporary Assistance	0.45	-0.33	0.12	26.72%
Total	**A-1**	**5.74**	**-5.54**	**0.20**	**3.46%**
Title A-2	**FUNCTIONING OF THE AGENCY**				
A-20	Buildings and Associated Costs	0.98	-0.62	0.36	36.60%
A-21	Movable Property and Associated Costs	0.10	-0.01	0.08	85.73%
A-22	Current Administrative Expenditure	0.05	-0.04	0.00	5.99%
A-23	Information and Communication Technologies	0.41	-0.23	0.17	42.74%
Total	**A-2**	**1.52**	**-0.91**	**0.62**	**40.42%**
Title B0-3	**OPERATING EXPENDITURE**				
B3-0	GROUP ACTIVITIES	0.65	-0.55	0.10	16.04%
B3-2	Horizontal Operational Activities	0.18	-0.14	0.04	23.75%
B3-6	Core Operational Activities	1.06	-1.01	0.06	5.25%
Total	**B0-3**	**1.90**	**-1.69**	**0.20**	**10.72%**
TOTAL %		**9.17**	**-8.15**	**1.02**	**11.11%**

Table 4: Balance sheet 2013 (in EUR)

BALANCE SHEET		
BALANCE SHEET	**2013**	**2012**
NON CURRENT ASSETS	**242,332**	**194,399**
Intangible Assets	1,682	6,832
Property, plant and equipment	240,650	187,567
CURRENT ASSETS	**2,158,996**	**1,150,315**
Short-term Receivables	599,939	69,103
Cash and Cash Equivalents	1,559,057	1,081,212
ASSETS	**2,401,328**	**1,344,714**
NON-CURRENT LIABILITIES	**-**	**-**
Provisions (long term)	-	-
CURRENT LIABILITIES	**1,196,562**	**885,818**
Short-term provisions	723,731	93,000
Accounts Payable	385,331	792,818
LIABILITIES	**1,196,562**	**885,818**
NET ASSETS (ASSETS less LIABILITIES)	**1,204,767**	**458,895**

Table 5: Economic Outturn Account 2013 (in EUR)

ECONOMIC OUTTURN ACCOUNT		
ECONOMIC OUTTURN ACCOUNT	**2013**	**2012**
OPERATING REVENUES	**9,684,054**	**8,076,637**
Revenue from the European Union Subsidy	8,975,136	8,076,498
Other revenue	6,053	139
Revenue from Administrative operations	702,866	-
OPERATING EXPENSES	**-8,935,750**	**-8,327,117**
Administrative Expenses	-7,434,458	-6,011,578
Operational Expenses	-1,501,291	-2,315,539
OTHER EXPENSES	**-2,432**	**-3,550**
Financial Expenses	-1,609	-2,423
Exchange rate loss	-823	-1,127
ECONOMIC OUTTURN FOR THE YEAR	**745,872**	**-254,030**

Remark: The figures included in Tables 4 & 5 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 01 July 2014).

Table 6: Average payment times for 2013

Average Payment Time for 2013	22.86
Total number of payments	1,366
Within Time Limit	1,041
Percentage	76.21%
Average Payment Time	13.87
Late Payment	325
Percentage	23.79%
Average Payment Time	51.65

Table 7: Situation on revenue and income on 2013 (in EUR)

Title	Description	Year of Origin	Revenue and Income recognized	Revenue and Income cashed	Outstanding Balance
90-0	Subsidy From The Eu General Budget	2013	9,030,185.00	9,030,185.00	0.00
92-0	OTHER CONTRIBUTIONS	2013	640,000.00	340,065.40	299,934.60
TOTAL			**9,670,185.00**	**9,370,250.40**	**299,934.60**

ANNEX 3: INTERNAL CONTROL TEMPLATE(S) FOR BUDGET IMPLEMENTATION (ICTS)

Stage 1: Procurement

A - 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) so 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 procurement/work programme	100% of the forecast procurements (open procedures published in the Official Journal of the European Union and on ENISA's 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:** number of purchases rejected as unjustified. Estimation of litigation avoided and eventual discontinuation of the service provided.	**Effectiveness:** number of projected tenders cancelled; number of contracts discontinued or under-utilised due to poor planning. Efficiency: for consultancy based tenders for operations; average person day cost per tender.
	Validation by Authorising Officer Sub Delegated (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 team meeting.		

B - 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 accepted if they are incorrectly submitted due to poorly defined 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:** N° of 'open' or procedures where only one or no offers were received. N° 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.>60.000 €) are reviewed. **Depth** risk based, depends on the sensitivity.		

C – 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:** Numbers 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 conflicts of interest.	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:** Number of procurements successfully challenged during standstill period.	

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 planned products/services/ works are not, totally or partially, provided in accordance with the technical description and requirements foreseen in the contract and/or the amounts paid exceed those 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.		

Stage 3 – Supervisory measures

Main control objectives: Ensuring that any weakness in the procedures (tender and financial transactions) is detected and corrected

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
An error or non-compliance with regulatory and contractual provisions, including technical specifications, or a fraud is not prevented, detected or corrected by ex-ante control, prior to payment.	Supervisory desk review of procurement and financial transactions.	Representative sample. Depth: review of the procedures implemented (procurement and financial transactions).	**Costs:** estimation of cost of staff involved. **Benefits:** Amounts detected associated with fraud & error. Deterrents & systematic weaknesses corrected.	**Effectiveness:** Amounts associated with errors detected (related to fraud, irregularities and error). In % over total checked. N° system improvements made. **Efficiency:** Costs of the ex post controls and supervisory measures with respect to the 'benefits'. Average cost of an ex-post control.
	Ex-post publication (possible reaction from tenderer / potential tenderer such as whistle blowing).	Potentially 100%		
	Review of ex post results.	100% at least once a year. Depth: look for any systemic problem in the procurement procedure and in the financial transaction procedure and any weakness in the selection process of the ex post controls.		
	Review of exceptions reported.	100% at least once a year. Depth: look for any weakness in the procedures (procurement and financial transactions).		
	Review of the process after each procedure.	100%. Depth: review any significant problem that occurred.		

ANNEX 4: PERFORMANCE INFORMATION INCLUDED IN EVALUATIONS

As this is a new requirement for ENISA's Annual Activity Report, the Agency will change its approach. Until 2014, ENISA approached the topic of "impact assessment" in a more global way, by commissioning an impact assessment of the Agency as a whole. ENISA is now looking into making the assessment of the direct impact of its products, deliverables and services an inherent part of its project management. This approach has already been applied in selected projects in 2014. For example, by issuing evaluation sheets to participants of training programmes or workshops, by issuing surveys in order to assess the quality of products or by assessing an entire thematic area (impact assessment in the area of CERT support).

ANNEX 5: LIST OF ENISA MANAGEMENT BOARD REPRESENTATIVES AND ALTERNATES (16/12/2013)

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	**Giuseppe ABBAMONTE** *Head of the Unit in charge of Trust and Security* *DG Communications Networks, Content and Technology* giuseppe.abbamonte@ec.europa.eu
Stephen QUEST *Director General* *DG Informatics* Stephen.quest@ec.europa.eu	**Marcel JORTAY** *Director in charge of infrastructure services provision* *DG Informatics* Marcel.Jortay@ec.europa.eu

MEMBER STATES REPRESENTATIVES

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	**Georgi TODOROV** *Deputy Minister of Transport, Information Technologies and Communications* gtodorov@mtitc.government.bg	**Vasil GRANCHAROV** *Director of Computer Security Incidents Response Team directorate, Executive Agency 'Electronic Communications Networks and Information Systems'* vgrancharov@esmis.government.bg
Croatia	**Zeljko TABAOVIC** *Deputy Director, Croatian Post and Electronic Communications Agency* zeljko.tabakovic@hakom.hr	**Ivana BIKIC** *Deputy Director, Croatian Post and Electronic Communications Agency* ivana.bikic@hakom.hr
Cyprus	**Antonis ANTONIADES** *Senior Officer of Electronic Communications and Postal Regulation* antonis.antoniades@ocecpr.org.cy	**Costas EFTYHYMIOU** *Officer of Technical Affairs at Office of the Commissioner of Electronic Communications and Postal Regulation* costas.efthymiou@ocecpr.org.cy
Czech Republic	**Mariana CAPKOVA** *National Cyber Security Centre* *National Security Authority* m.capkova@nbu.cz	**Jaroslav SMID** *Deputy Director* *National Security Authority of the Czech Republic* j.smid@nbu.cz
Denmark	**Thor SOMMERSTRAND** *Head of Section* *Ministry of Defence* *Centre for Cyber Security* thosom@govcert.dk	**Flemming FABER** *Senior Adviser* *Ministry of Defence* *Centre for Cyber Security* ff@govcert
Estonia	**Jaan PRIISALU** *Director General* *Estonian Information Systems Authority* jaan.priisalu@ria.ee	**Mait HEIDELBERG** *IT-Counsellor of the Ministry of Economic Affairs and Communications* mait.heidelberg@mkm.ee
Finland	**Timo KIEVARI** *Ministerial adviser* *Ministry of Transport and Communications* timo.kievari@lvm.fi	**Pauli PULLINEN** *Senior Officer* *Ministry of Transport and Communications* *Communications Policy Department* pauli.pullinen@lvm.fi
France	**Patrick PAILLOUX** *Director General of ANSSI* *(French Network and Information Security Agency)* secretariat.anssi@ssi.gouv.fr	**Jean-Baptiste DEMAISON** *ANSSI, International Relations* rit.sr.eu@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	**Nikos MOURKOGIANNIS** nikos@nikos.com	**Theodoros KAROUBALIS** *Hellenic Ministry of Transport and Communications* t.karoubalis@yme.gov.gr

Member State	Representative	Alternate
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	**Zoltan Attila NAGY** *National Information Security Authority* *Ministry of National Development* attila.zoltan.nagy@nfm.gov.hu
Ireland	**Aidan RYAN** *Telecommunications Adviser* *Department of Communications* Aidan.Ryan@dcmnr.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@sviluppoeconomico.gov.it	**Alessandro RIZZI** *Ministry of Economic Development* *Department of Communications* alessandro.rizzi@mise.gov.it
Latvia	**Ieva KUPCE** *Adviser of State* *Secretary Ministry of Defence* ieva.kupce@mod.gov.lv	
Lithuania	**Saulius STAROLIS** *Head of Electronic Commun ications Unit* *The Ministry of Transport and Communications of the Republic of Lithuania* saulius.starolis@sumin.lt	**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	**Anna CATANIA** *Chief Information Officer* *Information Management Unit,* *Ministry of Foreign Affairs* anna.catania@gov.mt	**Massimo VELLA** *Chief Information Officer* *Information Management Unit,* *Office of the Prime Minister* massimo.vella@gov.mt
Netherlands	**Edgar DE LANGE** *Senior policy adviser* *Ministry of Economic Affairs* *Dir.-Gen. for Energy, Telecommunications and Competition* e.r.delange@minez.nl	**Peter HONDEBRINK** *Ministry of Economic Affairs* *Dir.-Gen. for Energy, Telecommunications and Competition* j.p.hondebrink@minez.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* pdurbajlo@abw.gov.pl
Portugal	**José TORRES SOBRAL** *DiretorGeral do Gabinete Nacional de Segurança e Autoridade Nacional de Segurança* jtsobral@netcabo.pt	**Manuel PEDROSA DE BARROS** *Diretor da Direção de Segurança das Comunicações da ANACOM, 2730-216 Barcarena* manuel.barros@anacom.pt
Romania	**Liviu NICOLESCU** *Director General* *CERT Romania* liviu.nicolescu@cert-ro.eu	**Dan TOFAN** *Technical Director* *CERT Romania* dan.tofan@cert-ro.eu

Member State	Representative	Alternate
Slovakia	**Peter BIRO** *Information Society Division* *Ministry of Finance of the Slovak Republic* peter.biro@mfsr.sk	**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	**Manuel ESCALANTE GARCIA** *Director General* *Instituto Nacional de Tecnologias de la Communication (INTECO)* manuel.escalante@inteco.es	**Ignacio GONZALEZ UBIERNA** *Deputy director for Corporate Development* *Instituto Nacional de Tecnologias de la Communication (INTECO)* Ignacio.gonzalez@inteco.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	**Amy JORDAN** *BIS Cyber Security and Resilience team; Head, International, Resilience and Programme management* amy.jordan@bis.gsi.gov.uk	**Colin WHORLOW** *Head of International Relations* *CESG* colin.whorlow@cesg.gsi.gov.uk

EEA-COUNTRY REPRESENTATIVES (OBSERVERS)

Group	Representative	Alternate
Iceland	**Björn GEIRSSON** *Director of Legal Divison* *Post and Telecom Administration in Iceland* bjorn@pfs.is	
Liechtenstein	**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	**Christine HAFSKJOLD** *Senior Adviser* *Norwegian ministry of government administration, reform and church affairs* *Department of ICT policy and public sector reform* christine.hafskjold@fad.dep.no

ANNEX 6: THE PERMANENT STAKEHOLDER'S GROUP 2012-2015

Name		Job Title	Organisation	Nationality	Sector
Constance	**Bommelaer**	Director	Internet Society (ISOC)	French	Users
Martin	**Boyle**	Senior Policy Advisor	Nominet	British	Industry
Ilias	**Chantzos**	Director of Government Relations	Symantec	Greek	Industry
Raoul	**Chiesa**	Principal	Cyberdefcon Ltd	Italian	Industry
Nick	**Coleman**	Global Cloud Security Leader	IBM	British	Industry
Andrew	**Cormack**	Chief Security Adviser	JANET(UK)	British	Users
Gianluca	**D'Antonio**	CISO	FCC Group	Italian	Users
Harald	**Deppeler**	Information Security Manager	Google Switzerland GmbH	Swiss	Industry
Christos	**Dimitriadis**	Head of Information Security	INTRALOT Group	Greek	Users
Serge	**Droz**	Head of SWITCH Security	SWITCH	Swiss	Industry
Stefan	**Fenz**	Senior Researcher	Vienna University of Technology	Austrian	Academia
Patrick	**Froyen**	Senior IT Expert	European Central Bank	Belgian	Users
Denis	**Gardin**	Senior Vice president, Head of New Technology Ventures	EADS	French	Industry
Corrado	**Giustozzi**	lecturer	Università Campus Biomedico	Italian	Academia
Marcos	**Gómez-Hidalgo**	Security/e-Trust Deputy Manager	INTECO	Spanish	Users
Janusz	**Gorski**	Professor of Software Engineering	Gdansk University of Technology	Polish	Academia
François	**Gratiolet**	CSO	Qualys, Inc.	French	Industry
Dimitris	**Gritzalis**	Professor of ICT Security	Athens University of Economics and Business	Greek	Academia
Bruno	**Halopeau**	Information Assurance & Cyber Defence First Officer	Europol	French	Users
Stamatis	**Karnouskos**	Senior Researcher/ Research Expert	SAP	Greek, German	Industry
Cornelia	**Kutterer**	Director	Microsoft	German	Industry
Mika	**Lauhde**	Vice President, Government Relations and Business Development	SSH Communication Security	Finnish	Industry
Jean-Pierre	**Mennella**	Cyber Security Manager	Alstom Grid Power Electronic and Automation	French	Industry
Katerina	**Mitrokotsa**	Senior Researcher	Ecole Polytechnique Federale de Lausanne	Greek	Academia
Rain	**Ottis**	Scientist / Senior Analyst	NATO Cooperative Cyber Defence Centre of Excellence	Estonian	Industry
Bart	**Preneel**	Professor	Katholieke Universiteit Leuven	Belgian	Academia
Alfredo	**Reino**	Security Solutions Architect	Verizon	Spanish	Industry
Volker	**Schneider**	Senior Business Development Manager	secunet Security Networks	German	Industry
Marc	**Vael**	Chief Audit Executive	SMALS vzw	Belgian	Industry
Claire	**Vishik**	Security Policy/ Technology Manager	Intel	USA	Industry

ANNEX 7: A LIST OF ENISA'S WORK PROGRAMME PUBLICATIONS

WS1 - Evolving Risk Environment & Opportunities		
WPK 1.1 - Identification & mitigation of threats affecting Critical Information Infrastructure		
D1	D1: A description of the most important risks identified by the assessment of the processed data, especially when they affect critical information infrastructures	Amending WP 2013 (Reduced scope) ENISA Threat Landscape 2013 https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
D2	A Good Practice Guide on dealing with these risks, where appropriate together with proposals on how to coordinate these activities with other communities	Amending WP 2013 (Reduced scope) Smart Grid Threat Landscape https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/smart-grid-threat-landscape-and-good-practice-guide/
D3	Regular reports on identified risks and opportunities in the form of "Flash Notes" and other suitable formats	Flash Note: Can Recent Attacks Really Threaten Internet Availability? https://www.enisa.europa.eu/publications/flash-notes/flash-note-can-recent-attacks-really-threaten-internet-availability Flash note: Cyber-attacks – a new edge for old weapons https://www.enisa.europa.eu/publications/flash-notes/cyber-attacks-2013-a-new-edge-for-old-weapons
WPK 1.2 - Identification & mitigation of threats affecting Trust Infrastructure		
D1	A description of the most important risks identified by the assessment of the processed data, especially when the affect trust infrastructure (technology and services)	Trusted e-ID Infrastructures and services in EU -TSP services, standards and risk analysis report https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/trusted-eid/ Trusted e-ID Infrastructures and services in EU -TSP services, standards and risk analysis report https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/trusted-eid/ Trusted e-ID Infrastructures and services in EU - Recommendations for Trusted Provision of e-Government services https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/trusted-egov/
D2	A Good Practice Guide on dealing with these risks, where appropriate together with proposals on how to coordinate these activities with other communities	eIDAS in e-finance and e-payment services https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/eIDAS-in-e-finance-and-e-payment-services/
D3	Regular reports on identified risks and opportunities in the form of "Flash Notes" and other suitable formats	Flash notes merged with WPK 1.1. D3 Amending WP 2013

WS2 - Improving Pan-European CIIP & Resilience		
WPK 2.1 - Cyber crisis cooperation		
D1	Good Practice Guide on National Risk Assessment and Threat Modelling	http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/nlra-analysis-report
D2	International Workshop on Good Practices for Cyber	http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conferences/2nd-enisa-conference/report

D3	Planning and Organising Cyber Exercises: Methodology, Templates and Toolkit	Amending WP2013 (cancelled)

WS2 - Improving Pan-European CIIP & Resilience continued from page 6		
WPK 2.2 Facilitating Public-Private cooperation		
D1	Management of EP3R Constituency and Task Forces (workshops/calls)	EP3R 2013 Activity Report
D2	Three Position Papers (one for each Task Force)	EP3R – PP.TF.TermDef.CatAssets www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/tf-tdca EP3R – PP.TF.IncidentMgmt.MutualAidStrategies https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/tf-masim/ EP3R – PP.TF.TrustedInfSharing https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/tf-tis/ MARIE Phase 2 Report https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/mutual-aid-assistance/m-a-r-i-e-phase-ii-recommendations-report/
D3	Roadmap for 'European Cyber-Security Month' activities	Amending WP 2013 (Reduced scope) https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2013/ecsm-roadmap
WPK 2.3 Improving transparency of security incidents		
D1	Analysis of Annual 2012 Incident Reports and Recommendations for Mitigating Threats	Amending WP 2013 (Reduced scope) Annual Incident Report 2012 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012 National Roaming for resilience https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/national-roaming-for-resilience Power Supply Dependencies in the Ecomms Sector https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies
D2	Analysis of Incident Reporting Schemes for Cloud Computing	https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/incident-reporting-for-cloud-computing/
D3	Technical Implementation Guidelines for Data Breach Notification – Update	https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/proposal-for-one-security-framework-for-articles-4-and-13a
WPK 2.4 Enhancing the security of Governmental Clouds, Smart Grids and Interconnected Networks		
D1	Good Practice Guide for secure deployment of Governmental Clouds	http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds
D2	Guidelines on testing the security of and patching ICS-SCADA systems	Good practices for an EU ICS testing coordination capability https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/ics-cerc/good-practice-guide-for-certs-in-the-area-of-industrial-control-systems White paper– Window of Exposure a real problem for SCADA systems https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/window-of-exposure-a-real-problem-for-scada-systems
D3	Guidelines for enhancing the Resilience of Data Communication Networks	Amending WP 2013 (Reduced scope) https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/guidelines-for-enhancing-the-resilience-of-ecommunication-networks

WS3 - Enabling Communities to Improve NIS		
WPK 3.1 - Application of good practice for CERTs		
D1	Secure communication's platform for European n/g CERTs (Requirements & stocktaking)	Detect, SHARE, Protect – Solutions for Improving Threat Data Exchange among CERTs https://www.enisa.europa.eu/activities/cert/support/data-sharing/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs
D2	EISAS – deployment in Europe (a feasibility study)	https://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas-deployment-feasibility-study
D3	Good practice guide on Alerts, Warnings and Announcements (including an inventory of Incident Response Methodologies)	"Best practice guide on Alerts, Warnings & Announcements". https://www.enisa.europa.eu/activities/cert/support/awa
D4	CERT Inventory; an extended overview (inventory and interactive map)	https://www.enisa.europa.eu/activities/cert/background/inv
WPK 3.2 - Enabling collaborative communities		
D1	Good practice guide on the practical implementation of the "directive on attacks against information systems"	"A Good Practice Collection for CERTs on the Directive on attacks against information systems" https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/the-directive-on-attacks-against-information-systems
D2	8th Annual CERT workshop report (public version)	"8th ENISA Workshop 'CERTs in Europe' report" https://www.enisa.europa.eu/activities/cert/support/files/8th-enisa-workshop-certs-in-europe-report
D3	CERT exercise material – extended – cybercrime scenarios (handbook and toolset)	"ENISA CERT exercise material extended with cybercrime scenarios" http://www.enisa.europa.eu/activities/cert/support/exercise
D4	New version of Baseline capabilities framework – international harmonisation (Status report on capabilities harmonisation with worldwide stakeholders) and appropriate ICS-CERT capabilities	Good practice guide for CERTs in the area of Industrial Control Systems https://www.enisa.europa.eu/media/press-releases/mitigating-attacks-on-industrial-control-systems-the-new-guide-from-enisa CERT communities – Recognition mechanisms and schemes https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/cert-community-recognition-mechanisms-and-schemes/
D5	CERT training support (TRANSITS and ENISA training portfolio activities)	No deliverable
D6	Good practice guide on harmonisation and implementation of legal frameworks for information sharing and international incident handling process	Amending WP 2013 (cancelled)
WPK 3.3 - Enabling the information society		
D1	Supporting EC activities in the implementation of trustmarks. Identifying best practice from security certification that could be deployed for privacy certification and trustmark	Paper on certification: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/security-certification-practice-in-the-eu-information-security-management-systems-a-case-study Paper on trustmarks: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/on-the-security-privacy-and-usability-of-online-seals/
D2	Recommendations for best practice on data security of personal data/the use of cryptographic techniques for eGov services in Europe	Paper on security of personal data: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/recommended-cryptographic-measures-securing-personal-data Cryptographic techniques for eGov services: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report
D3	Good practices for security of electronic identification systems	Amending WP 2013 Guidelines for Trust Service Providers: http://www.enisa.europa.eu/activities/identity-and trust/trust-services/guidelines-tsp
D4	eID workshop	Amending WP 2013 - Workshop conducted on 24th September in Brussels: http://www.enisa.europa.eu/activities/identity-and-trust/trust-services/eid-workshop
D5	Dissemination activity (e.g. panel session) focusing on the work in the area of privacy and trust	Amending WP 2013 Panel at CPDP conference - Privacy and Network Information Security in Education: http://www.cpdpconferences.org/Resources/CPDP2014_Programme.pdf

Additional papers (extra miles)	
Brokerage model of NIS in Education	https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/brokerage-model-for-network-and-information-security-in-education/
Securing personal data in the context of data retention. Analysis and recommendations	https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/securing-personal-data-in-the-context-of-data-retention/
Proposal of methodology of severity assessment of data breaches	https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn-severity

European Commission

ENISA Annual Report 2013

Luxembourg: Publications Office of the European Union
2014 - II, 68 pp. – 21 x 29.7 cm
ISBN 978-92-9204-087-1
ISSN 1830-981X
doi:10.2824/32013

HOW TO OBTAIN EU PUBLICATIONS

Free publications:
- via EU Bookshop (http://bookshop.europa.eu);
- at the European Union's representations or delegations. You can obtain their contact details on the Internet (http://ec.europa.eu) or by sending a fax to +352 2929-42758.

Priced publications:
- via EU Bookshop (http://bookshop.europa.eu).

Priced subscriptions (e.g. annual series of the Official Journal of the European Union and reports of cases before the Court of Justice of the European Union):
- via one of the sales agents of the Publications Office of the European Union (http://publications.europa.eu/others/agents/index_en.htm).

TP-AB-14-001-EN-N

European Union **Agency for Network and Information Security**
PO Box 1309, 710 01, Heraklion, Greece
Tel: +30 2810391280, Fax: +30 2810391410
http://www.enisa.europa.eu

Publications Office

9 789292 040871 >