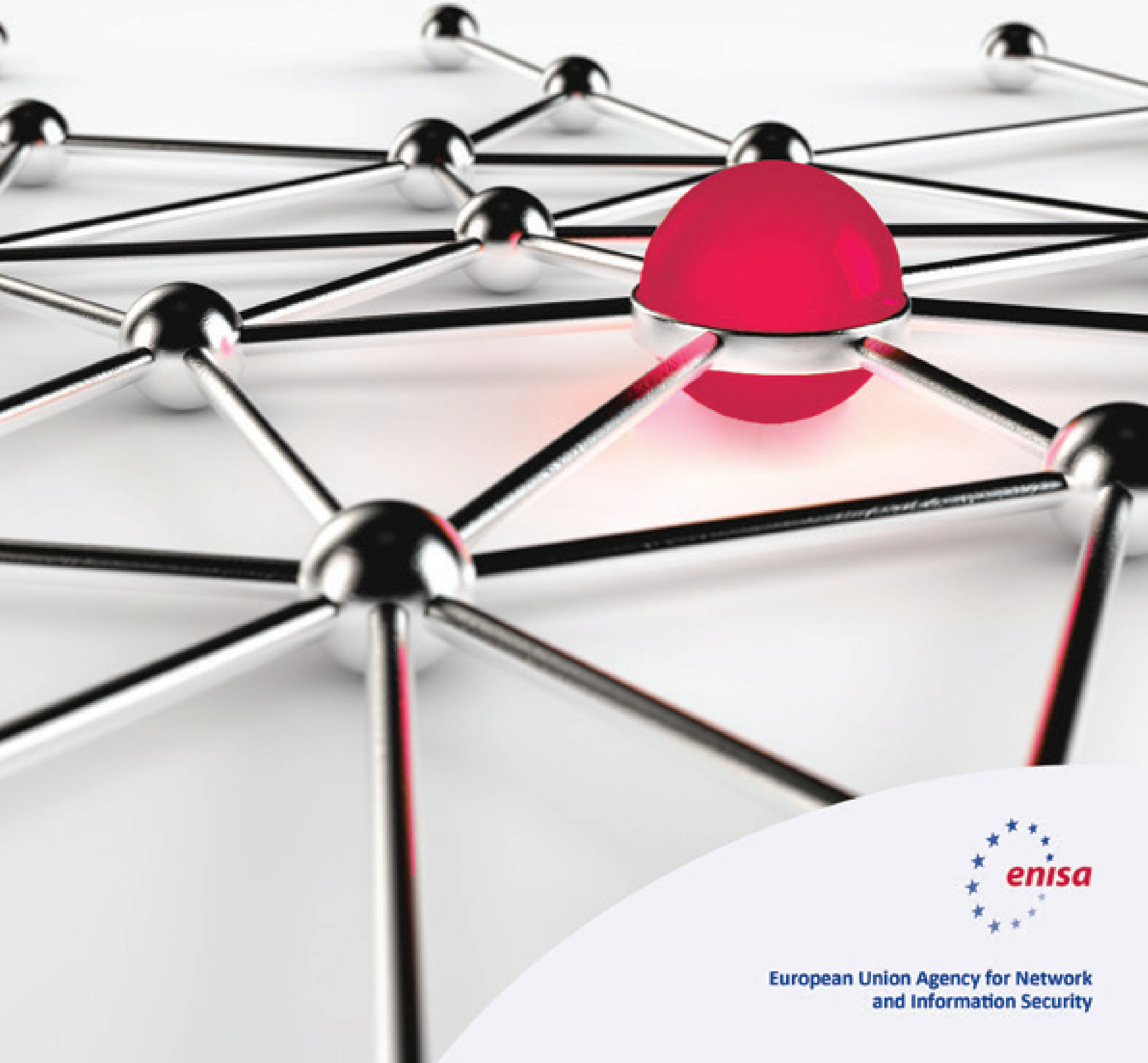
ENISA
Annual Activity Report 2014



enisa

European Union Agency for Network and Information Security

Cover image, head of chapters image © Theaphotography | Dreamstime.com - European Union Series Photo
Other images © ENISA or Shutterstock

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

Luxembourg: Publications Office of the European Union, 2014

Print:	ISBN 978-92-9204-123-6	ISSN 1830-981X	doi:10.2824/43877	TP-AB-15-001-EN-C
PDF:	ISBN 978-92-9204-124-3	ISSN 2314-9434	doi:10.2824/521040	TP-AB-15-001-EN-N

Printed in Italy

Printed on elemental chlorine-free bleached paper (ECF)

ENISA
Annual Activity Report 2014

European Union
Agency for
Network and
Information Security

10 YEARS OF CYBER SECURITY FOR EUROPE
2004 - 2014

A message from the Executive Director

Overview

I am happy to state that 2014 was another successful year for the Agency, with ENISA maintaining its track record of delivering according to plan and within allocated budget. At the same time, we improved the positioning of services for our major stakeholders while ensuring compliance with the regulatory framework. On a more personal note, the Management Board approved the extension of my mandate for one more term of 5 years, which I take as a sign that the Agency is responding well to the needs of its stakeholder communities.

External Impact

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

- Recommendations to its stakeholders
- Support for policy development and implementation
- 'Hands on' work with operational communities.

Udo Helmbrecht

Throughout 2014, ENISA strengthened its contribution in each of these areas, supporting Member States and private sector actors in responding to a rapidly developing threat environment and helping to lay solid foundations for the information systems of the future.

Where recommendations are concerned, the Agency produced a total of 37 reports on a wide variety of subjects, ranging from national issues such as the protection of critical infrastructure to issues affecting individual citizens such as privacy and data protection. The *ENISA Threat Landscape* is an example of such a report. This document offers a consolidated picture of threat information collected from public sources throughout the globe and presents the top threats and the way in which they are evolving in distinct business areas. One of the strengths of the ENISA Threat Landscape approach is that it provides useful information to a diverse set of stakeholder communities.

The work carried out in the area of Article 13a of the Telecommunications Framework Directive of 2009 continues to be the best known example of where ENISA is working to support policy initiatives; in addition to this we are active in a number of policy initiatives, including support for the eIDAS legislation [11] and preparing for implementation of the proposed NIS Directive [3] and Data Protection legislation [10].

The pan-European Exercise continues to provide valuable insight into the way in which operational communities collaborate across the EU in order to respond to serious NIS incidents that affect several Member States. Previous exercises allowed the Member States to develop a set of standard operating procedures (SOPs) for handling such incidents. The 2014 exercise, which is based on the participation of operational teams spread throughout the EU was used to test and further develop these procedures. Building on this past experience, the 2014 exercise introduced a new level of sophistication by explicitly testing the tactical, operational and strategic phases of response to an incident in separate steps. The third phase of this exercise, which concerns the strategic response, will be carried out in 2015.

Article 14 requests, which are essentially a mechanism that allows Member States and EU institutions to request specific items of work of the Agency outside the work programme execution process, continue to be popular. ENISA received 12 new requests in 2014 and continued to work on 19 ongoing requests (including 2013) from following countries: Austria, Croatia, Cyprus, Czech Republic, Estonia, Germany, Greece, Italy, Latvia, Luxemburg, Malta, Poland, Portugal, Spain and from the European Commission.

Internal improvements

In order to support the new mandate and further improve the operational model based on two locations, I introduced a new organisational structure in October 2014. This new structure is dictated by the new challenges identified in the rapidly changing operating environment with the limited number of human resources at the Agency's disposal.

In addition, a large refurbishment project was conducted to improve the working conditions of the staff located in Athens. This refurbishment did not impact the delivery of ENISA work programme and the Agency delivered on time and within budget. The newly refurbished building not only represents a significant improvement in the daily lives of our operational staff, but is also better equipped from an IT and telecommunications perspective, which should also result in further performance gains.

Conclusions

2014 has been another very successful year for the Agency. It has been a year in which we have strengthened our relations with our stakeholders and assisted them in making significant improvements to the state of cyber security throughout the EU. In parallel, we continue to make internal improvements that keep staff morale high and make the agency a challenging and pleasant place to work.

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

Udo Helmbrecht
Executive Director, ENISA

List of abbreviations

APF: Annual Privacy Forum
CE2014: Cyber Europe 2014
CEP: Cyber Exercises Platform
CERT: Computer Emergency Response Team
CEN: European Committee for Standardization
CENELEC: European Committee for Electrotechnical Standardization
CII: Critical Information Infrastructures
CIIP: Critical Information Infrastructure Protection
CISO: Chief Information Security Officer
CSCG: ETSI CEN-CENELEC Cyber Security Coordination Group
CSIRT: Computer Security Incidents Response Teams
COD: Core Operational Department
CSS: Cyber Security Strategy
D: Deliverable
DG: EC Directorate-General
DG CONNECT: EC Directorate-General CONNECT
DPA: Data Protection Authorities
EC: European Commission
EC3: Europol’s European Cybercrime Centre
ECSM: European Cyber Security Month
ED: Executive Director
eID: electronic Identity
ENISA: European Union Agency for Network and Information Security
ETSI: European Telecommunications Standards Institute
EU: European Union
EURO SCSIE: European SCADA Security Information Exchange
FAP: Finance, Accounting and Procurement Section
FIRST: Forum of Incident Response and Security Teams
FM: Facilities Management
FTE: Full Time Equivalents
H2020: Horizon 2020
HR: Human Resources Section
IAS: Internal Audit Service
ICC & IAC: Internal Control Coordination and Internal Audit Capability
ICS: Industrial Control Systems
ICT: Information and Communication Technologies
IS: Information Systems
ISO: International Organization for Standardization
ISO: Information Security Officer
ISP: Internet Service Providers
ITFMU: Information Technology & Facilities Management Unit
IXP: Internet exchange point
KII: Key Impact Indicator
KPI: Key Performance Indicator
LEA: Law Enforcement Agency
MB: Management Board
MS: Member State
n/g CERT: National / Governmental CERT
NCO: National Contact Officer
NCSS: National Cyber Security Strategies
NIS: Network and Information Security
NLO: National Liaison Officer
NRA: National Regulatory Authority
PPP: Public Private Partnership
PSG: Permanent Stakeholders Group
Q: Quarter
QMS: Quality Management System
R & D: Research and Development
SCADA: Supervisory Control & Data Acquisition
SME: Small and Medium Enterprise
SOGIS: Senior Officials Group Information Systems Security
SOP: Standard Operating Procedures
TF-CSIRT: Task Force of Computer Security Incidents Response Teams
TSP: Trust Service Provider
US: United States of America
WP: Work Programme
WPK: Work Package
WS: Work Stream

Table of contents

A message from the Executive Director ii

List of abbreviations iv

Table of contents v

1 Introduction 1

1.1 ENISA in brief 2

1.2 The year in brief 2

1.3 Summary 3

1.3.1 Key performance indicators 3

1.3.1.1 Supporting EU policy building. Identifying evolving threats, risks and challenges 3

1.3.1.2 Supporting EU policy building. Contributing to EU policy initiatives 3

1.3.1.3 Support capacity building. Support Private Sector Capacity Building 3

1.3.1.4 Support cooperation. Implementation of EU legislation 3

1.3.1.5 Support cooperation. Crisis cooperation — exercises 4

1.3.2 Policy highlights of the year 4

1.3.3 Key conclusions on the effectiveness of the internal control systems and financial management 4

1.3.4 Information for the stakeholders 5

2 Policy achievements 6

2.1 Achievement of general and specific policy objectives 7

2.1.1 Policy achievements in WS1- Support EU policy building 7

2.1.1.1 General achievements. Achievement of Impact Indicators 10

2.1.1.2 Specific achievements. Mapping of deliverables into papers/publications/activities 11

2.1.2 Policy achievements in WS2- Support capacity building 12

2.1.2.1 General achievements. Achievement of impact indicators 15

2.1.2.2 Specific achievements. Mapping of deliverables into papers/publications/activities 16

2.1.3 Policy achievements in WS3- Support cooperation 18

2.1.3.1 General achievements. Achievement of Impact Indicators 20

2.1.3.2 Specific achievements. Mapping of deliverables into papers/publications/activities 22

2.1.4 Horizontal operational activities 23

2.1.4.1 Article 14 requests 23

2.1.4.2 National liaison officer network 24

2.1.4.3 Corporate communication, dissemination activities and outreach 24

2.1.4.3.1 Celebrating a decade of contribution to the EU's cyber security — High level Event 2014 25

2.1.4.3.2 ENISA branding of its 10-year celebration 25

2.1.4.3.3 Publications 25

2.1.4.3.4 Multilingual approach ... 25
2.1.4.3.5 Media outreach ... 25
2.1.4.3.6 Cross media impact ... 26
2.1.4.3.7 Social media ... 26
2.1.4.3.8 Digital media ... 26
2.1.4.3.9 Additional outreach activities ... 26
2.1.4.4 Quality management system ... 27
3 Management of resources ... 28
3.1 Management Board ... 29
3.2 Major events ... 29
3.3 Management of financial resources ... 29
3.3.1 Budget execution of EU subsidy (C1 funds) ... 29
3.3.2 Budget execution of additional funds received in 2013 for Athens office refurbishment works (C3 appropriations) ... 29
3.3.3 Amending budgets/budgetary Transfers ... 30
3.3.4 Carry forward of commitment appropriations ... 31
3.3.5 Types of procurement procedures ... 31
3.3.6 Interest charged by suppliers ... 31
3.4 Management of human resources ... 31
3.4.1 Human resources ... 31
3.4.2 Results of screening ... 32
3.5 Assessment by management ... 32
3.5.1 Effectiveness of controls for legality and regularity ... 32
3.6 Budget implementation tasks entrusted to other services and entities ... 32
3.7 Assessment of audit results and follow up of audit recommendations ... 32
3.7.1 Internal Audit Services (IAS) ... 32
3.7.2 European Court of Auditors (ECA) ... 32
3.7.3 Follow up of audits plans, audits and recommendations. ... 33
3.7.4 Follow up of observations from the discharge authority. ... 33
3.7.4.1 Follow-up of the 2011 discharge ... 33
3.7.4.2 Budget and financial management ... 33
3.7.4.3 Commitments and carry overs ... 33
3.7.4.4 Transfers ... 33
3.7.4.5 Procurement and recruitment procedures ... 33
3.7.4.6 Prevention and management of conflicts of interests and transparency ... 33
3.7.4.7 Comments on internal controls ... 34
3.7.4.8 Internal audit ... 34
3.7.4.9 Performance ... 34

4 Assessment of the effectiveness of the internal control systems 35
4.1 Risk management 36
4.2 Compliance and effectiveness of internal control standards 36
4.2.1 Mission (ICS 1) 36
4.2.2 Ethical and organisational values (ICS 2) 36
4.2.3 Staff allocation and mobility (ICS 3) 36
4.2.4 Staff evaluation and development (ICS 4) 36
4.2.5 Objectives and performance indicators (ICS 5) 36
4.2.6 Risk management process (ICS 6) 37
4.2.7 Operational structure (ICS 7) 37
4.2.8 Processes and procedures (ICS 8) 37
4.2.9 Management supervision (ICS 9) 37
4.2.10 Business continuity (ICS 10) 38
4.2.11 Document management (ICS 11) 38
4.2.12 Information and communication (ICS 12) 38
4.2.13 Accounting and financial reporting (ICS 13) 38
4.2.14 Evaluation of activities (ICS 14) 38
4.2.15 Assessment of internal control systems (ICS 15) 39
4.2.16 Internal audit capability (ICS 16) 39
5 Management assurance 40
5.1 Review of the elements supporting assurance 41
5.2 Exceptions 42
6 Declaration of assurance 43
Annexes 45
A. Human resources 46
A.1. Organisational chart 46
A.2. Establishment plan 2014 46
A3. Information on entry level for each post type 47
A.4. Information on the benchmarking exercise 48
A.5. Human resources statistics 49
A.6 Human resources by activity 50
B. Financial resources 50
B.1. Provisional annual accounts 2014 50
Balance sheet 2014 (in EUR) 50
Statement of financial performance 2014 (in EUR) 51
B2. Financial Reports 2014 51

C. Materiality criteria ... 53

D. Internal control templates for budget implementation (ICT) ... 53

Stage 1: Procurement ... 53

A — Planning ... 53

B — Needs assessment and definition of needs ... 54

C — Selection of the offer and evaluation ... 54

Stage 2 — Financial transactions ... 55

E. The permanent stakeholders' group, term of office 2012-2015 ... 55

Nominated members ... 55

Experts appointed '*ad personam*' ... 55

F. List of ENISA Management Board representatives and alternates ... 56

Commission representatives ... 56

Member States representatives ... 57

EEA-country representatives (observers) ... 59

G. List of policy documents ... 59

1

Introduction

1.1 ENISA in brief

The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe. ENISA supports the EU and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents. ENISA's vision is *to secure and enable Europe's information society* and to use its unique competencies to help to drive the cyber landscape in Europe.

The Agency works closely together with members of both the public and private sector, to deliver advice and solutions that are based on solid operational experience. ENISA also supports the development of the European Union (EU) policy and law on matters relating to network and information security (NIS), thereby contributing to economic growth in Europe's internal market.

ENISA was established in 2004 by Regulation (EC) No 460/2004 of the European Parliament and the Council. The Agency therefore celebrated in 2014 ten years of successful activity in the European Cyber Security Landscape. At the same time, 2014 is the first year of the new mandate of the Agency. Regulation (EU) No 526/2013 ([1]) of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security extends ENISA's mandate until 19 June 2020.

ENISA's strategic objectives include: (i) developing and maintaining a high level of expertise of EU actors taking into account evolutions in network and information security (NIS); (ii) assisting the Member States and the Commission in enhancing capacity building throughout the EU; (iii) assisting the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security; and (iv) enhancing cooperation both between the Member States of the EU and between related NIS communities.

According to article 4 of Regulation 526/2013, the Agency is comprised of the Management Board (MB); the Executive Director and staff; and the Permanent Stakeholders Group (PSG). In order to contribute to enhancing the effectiveness and efficiency of the operation of the Agency, the MB has established an Executive Board.

The MB holds its ordinary meeting to adopt decisions on budgetary and administrative matters as well as rules implementing provisions of ENISA Regulation No 526/2013 and Staff Regulations. The Board also adopts planning documents such as annual work programme, multi-annual staff policy plan, statement of estimates and others.

The PSG is an advisory body in respect of the agency's performance of its activities. It also advises the Executive Director on drawing up a proposal for the Agency's work programme. Two PSG meetings were held as planned during the 2014.

1.2 The year in brief

2014 was another successful year for the Agency. As can be seen in Section 2, ENISA delivered according to plan and within the allocated budget, improving its roles and the positioning of its services to its stakeholders while ensuring compliance with the regulatory framework.

Building on its renewed regulatory framework, ENISA was particularly active in:

- Supporting EU policy building by developing and maintaining high level of expertise related to NIS, facilitating voluntary information, establishing mutual interactions, contributing to EU policy initiatives and supporting EU in education research and standardisation.
- Supporting capacity building of EU Member States, public and private sectors as well as contributing to raising the level of awareness of EU citizens.
- Supporting the implementation of EU legislation related to NIS and supporting cooperation between all stakeholders relevant and active in the area of NIS.

The activities and the achievements of 2014 are presented in Section 2, with the more significant achievements being also highlighted in Section 1.3. The activities are presented by matching the achieved results against the impact indicators and the proposed deliverables from WP2014. The horizontal activities, such as Article 14 requests ([2]), collaboration with NLO, communication and dissemination activities are also presented in Section 2.

[1] For the links and names of all relevant policy documents mentioned in this report please see Annex G.

[2] Article 14 of ENISA Regulation (EU) No 526/2013 (a) the European Parliament; (b) the Council; (c) the Commission; and (d) any competent body appointed by a Member State, such as a national regulatory authority could address requests for advice and assistance falling within the Agency's objectives and tasks. An overview of the requests to the Agency that were addressed during 2014 is included in section 2.1.4.1.

To support the new mandate and activities based in two locations, in line with the operational and horizontal objectives of the Agency, ENISA's structure (see Section 3.4 and Annex A) was reorganised by the Executive Director in October 2014. The Agency's organisational structure is dictated by the new challenges identified in the rapidly changing operating environment with the limited number of human resources at the Agency's disposal. During 2014, a large refurbishment project was conducted to improve the working conditions of the staff located in Athens. This refurbishment did not impact the delivery of ENISA work programme and the Agency delivered in time and within budget. The management of resources is described in Section 3 while more information is provided on assessment and management assurance in Sections 4 and 5.

The document includes also a set of annexes proving more details for this report.

In September 2014, the Management Board endorsed the extension of the mandate of the Executive Director of ENISA, Udo Helmbrecht for one more term of 5 years.

1.3 Summary

1.3.1 Key performance indicators

Whilst the agency delivered against its annual work programme, it is worth highlighting that all deliverables met or exceeded the key performance indicators set (see Section 2.1 for more details). Some of these achievements are outlined here and examples are provided on how the agency achieved its goals.

1.3.1.1 Supporting EU policy building. Identifying evolving threats, risks and challenges

- **Impact Indicator (I.I.1.1-1):** The ENISA Threat Landscape becomes an important point of reference for security experts worldwide and is referenced in at least 10 security related information sources worldwide.

- **Achieved results:** Achieved: More than 20 different organisations are using the conclusions of ENISA's Threat Landscape report 2014. Several hundred references to ENISA Threat Landscape 2013 have been made via the main cyber security web pages and blogs.

- **NB:** The number of organisations quoting the ENISA Threat Landscape deliverables is significantly above expectations.

1.3.1.2 Supporting EU policy building. Contributing to EU policy initiatives

- **Impact Indicator (I.I.1.2-3):** Five Member States eID competent bodies/authorities, five independent auditing bodies and five trust service providers take part in the development of a common audit framework for trust service providers.

- **Achieved results:** Achieved: In total, more than 35 stakeholders requested to review the draft document, including FESA members (Member States), TSPs and auditing bodies. The paper underwent reviews in various stages of the development process.

- **NB:** ENISA set of recommendations for TSPs developed in 2014-2015 is becoming a real point of reference for European TSPs in their daily work.

1.3.1.3 Support capacity building. Support Private Sector Capacity Building

- **Impact Indicator (I.I.2.2-3):** 15 Cloud Computing Providers and five Member States competent authorities contribute to ENISA's study on minimum security measures for cloud computing.

- **Achieved results:** Achieved: 20 Cloud providers and 12 Member States participating in the study for Cloud Certification Metaframework.

- **NB:** ENISA collected the ICT security requirements for the public sector from 12 Member States. This study was greatly complemented by the input from the community, which was a great undertaking for ENISA to centralise all the information.

1.3.1.4 Support cooperation. Implementation of EU legislation

- **Impact Indicator (I.I.3.2-1):** 23 Member States contribute to ENISA's work on the implementation of Article 13a and 12 Member states directly use the outcomes of this work by explicit references or by adopting the same approach nationally.

- **Achieved results:** Achieved. All 28 Member States plus two EFTA Countries sent to ENISA and the Commission annual summary reports about incidents that occurred in 2013. All Member States use the ENISA Technical Guideline on Article 13a Incident Reporting in their annual reporting. More than 12 Member States and some of the larger European Electronic Communications Providers use directly or refer to the ENISA Technical Guideline on Security Measures. During 2014, ENISA performed three workshops with the Article 13a Expert Group attended by NRAs from around 20 Member States.

- **NB:** ENISA reports in this area rely now on input from all EU Member States and two EFTA countries and are used by more than 12 Member States and service providers.

1.3.1.5 Support cooperation. Crisis cooperation — exercises

- **Impact Indicator (I.I.3.1-1):** At least 24 EU Member States and EFTA countries confirm their support for Cyber Europe 2014 (CE2014).

- **Achieved results:** Achieved: CE 2014 involved 1400 experts and over 450 teams, with an equal representation from the public and private sector (n/g CERTs, cyber security agencies, public sector teams, Telecom Operators, Energy Sector Companies). Over all the different phases of Cyber Europe 2014 there were 29 different participating countries (26 EU MS, 3 EFTA) and the EU Institutions. In the first phase of CE2014 (TLEx) over 600 experts were involved, coming from 214 teams representing both private and public sector institutions (n/g CERTs, cyber security agencies, public sector entities, telecom operators, energy sector companies etc.). In the second phase of CE2014 (OLEx) over 800 experts were involved. An impressive number of over 1400 experts were involved in the exercises in some way during CE2014. Member States have declared their satisfaction with the exercise through evaluation surveys and through communications via the ENISA Management Board members and NLOs.

- **NB:** This activity had a record number of participants and it is worth mentioning also the number of Member States involved and the participation of private sector.

1.3.2 Policy highlights of the year

The policy highlights of 2014 were as follows:

- Successful execution of the pan-European cyber security exercise

- ENISA support of EU policy and legislation

- Publication of recommendations in a number of areas central to NIS policy

The successful completion of the tactical and operational phases of the 2014 pan-European cyber security exercise marks a significant step in improving the level of preparedness of the EU for a major cyberattack targeting several Member States. Previous exercises allowed the Member States to develop a set of Standard Operating Procedures (SOP) for handling such incidents. The 2014 exercise, which is based on the participation of operational teams spread throughout the EU is now being used to test and further develop these procedures. The third phase of this exercise, which concerns the strategic response, will be carried out in 2015.

ENISA carried out a number of activities that directly or indirectly support EU policy initiatives. The Agency supported the Commission and the Member States in the development of a common audit framework for trust service providers in the context of the eIDAS regulation. In parallel, the Agency continues to support Member States in the implementation of Article 13a of the Telecommunications Framework Directive. The reports that are published by the Agency and which reflect data collected through this process provide a valuable insight into the risks affecting telecommunications infrastructure.

The Agency continues to support developments in the area of data protection by producing targeted studies illustrating how the concepts underlying the proposed new legislation can be implemented in real operational environments. Indeed, ENISA is uniquely positioned to assist the private sector in implementing more effective tools and procedures in this area.

Finally, ENISA published a number of studies that provide concrete advice and recommendations to its stakeholders in a variety of areas central to current NIS policy. The ENISA Threat Landscape is a good example of a study that is interesting to all ENISA stakeholders, providing a description of the top threats and how they apply to different business models. Other ENISA studies provide advice and guidance in areas that are key to economic growth, such as Cloud Computing, SCADA systems, SMART cities and the protection of Critical Information Infrastructure.

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

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

Compliance with these standards is compulsory for financial management.

The Agency has also put in place an organisational structure and a set of internal control systems that are 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 that its internal control systems need to comply with. Previously developed internal procedures were grouped together, prioritised and implemented in the daily workflows of the Agency, as deemed appropriate.

In 2014, the Agency focused on compliance with the standards that were identified as areas of concern during the risk assessment exercise, as well as on the recommendations raised by the auditing bodies (ECA and IAS). During 2014, the Agency achieved compliance with the internal control standards. For more details please refer to Sections 3 to 6 and to the Annexes of this report.

1.3.4 Information for the stakeholders

Whilst ENISA has aligned its activities with the EU policy agenda and is delivering high quality results, the growing demand to secure our infrastructures and economy call for ENISA's proactivity in in the area of NIS.

Recently ENISA assessed both the current cyber-threat landscape and upcoming trends. While significant changes in top threats, increased complexity of attacks, successful internationally coordinated operations of law enforcement and security vendors have been noted, successful attacks on vital security functions of the Internet can also be observed. Positive developments can be attributed to successful law enforcement operations and to the mobilisation of the cyber-security community.

But there is an alarming side to the threat landscape:

- Core security protocols of the Internet have been under massive stress.
- Massive data breaches demonstrated how effectively cyber-threat agents abuse security weaknesses of businesses and governments.
- Privacy and personal data breaches have weakened the trust of users in the Internet.
- Increased sophistication and advances in targeted campaigns have demonstrated new qualities of attacks.

It is evident that these cyber-threat dynamics dictate the need for a better orchestration of all relevant stakeholders. Some of the conclusions arising out of this assessment are:

- *It is imperative to increase cyber-threat knowledge through cooperation:* The 'publicity' of threat information in related media is quite high. In the future it will be necessary to establish cooperation (consolidate efforts) among various players in the field to quickly obtain quality information on cyber threats and on defence measures. As Cyber-Europe has demonstrated, cooperation and coordination is key to effective response to cyber-security incidents.
- *Capability building in cyber-threat assessment and defence is of strategic importance*: Sophistication of cyber threats are increasing. We see currently defence practices from the past losing efficiency (i.e. classical signature-based anti-virus). Methods used by high capability threat actors today are adopted by cyber criminals tomorrow. This increases challenges in capability building.
- *It is vital to collect accurate information on successful cyber-security incidents*: The unknown number of breaches and security incidents is of major concern to security experts and in particular to law enforcement. Breach notification needs to be put on a wider basis via corresponding regulations in various areas/sectors, eventually covering end-user impact. This will help assessing the currently large grey numbers assumed.
- *Increased agility in security response is essential*: The high speed of changes in cyber-threat landscape makes agile response indispensable. Information on cyber threats should be the key parameter in actively adapting security protection practices towards a more agile management of security at all (technical, organisational and policy) levels.

ENISA seeks to support the NIS community, the Member States and the EU institutions in the coordination of better mechanisms and improved means to support the policy agenda of the EU. ENISA will continue to contribute its expertise to support NIS in Europe in the context of the current threat landscape and the current challenges in the area of NIS.

2

Policy achievements

2.1 Achievement of general and specific policy objectives

The core activities of ENISA for 2014 have been grouped into three work streams (WS). This section follows the same structure for reporting as the structure of the ENISA work programme 2014. The three streams of activity during 2014 were:

- WS1: 'Support EU policy building' designed to support the policy-making process by making available to policy-makers consolidated information on the emerging threat landscape and by formulating key messages to the Member States on how to ensure that their policies and capabilities are aligned with EU objectives, taking into account lessons learned within the different Member States. This involves the unification of available information sources under a common context and will also require the involvement of important stakeholders in the areas of threat assessment, risk mitigation and policy definition.

- WS2: 'Support capacity building' addressed a number of activities designed to assist both the public sector and private sector in the Member States in protecting critical information infrastructures (CIIP). By facilitating cooperation and coordination between public and private sectors within the Member States, ENISA continues to support the development of policies, measures, and recovery strategies to meet the challenges of a continuously evolving threat environment.

- WS3: 'Support cooperation' was about strengthening NIS in the European single market. Cooperation strengthens the capacities of Member States, EU institutions and third countries and helps them to deal with crises. The approach builds upon existing collaboration in existing communities, further enhancing community building in Europe and beyond. This work also looked at the development of tools to facilitate and improve the international communication and interchange of security relevant information within communities sharing the same interest in different Member States.

In the following sections, we will focus on each of these streams of activities. After a general presentation of the policy achievements, more detailed information is provided matching planned activities and the achieved results. Detailed tables are provided showing the proposed Impact Indicators and how they were achieved as well as the proposed deliverables and the achieved publications or activities.

2.1.1 Policy achievements in WS1-Support EU policy building

The following work packages constitute Work Stream 1. For each work package, the main objectives and policy achievements are identified.

- WPK1.1. ***Identifying evolving threats, risks and challenges***

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

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

  - Policy achievements and evolution in the ***area of threats and risks, supporting ENISA objectives and mandate as well as Council Resolution on a collaborative European approach to network and information security***:

    - ENISA developed a perspective of the European landscape of the NIS gaps and needs. The deliverables on threat landscape provide a European perspective based collected threats (e.g. incorporating information on European companies such as size, type of business, etc.).

        - The ENISA Threat Landscape 2014 was developed as continuation of the work started in 2012. Compared to previous years, there is noticeable improvement in the quality of threat information collected within related organisations. The improvements in information collection were based on liaison with sources of threat information to establish effective dissemination of generated information.

        - Analysis and assessment of previous year forecasts was carried out.

- WPK1.2. ***Contributing to EU policy initiatives***.

    - The main objective of this work package was to provide input to new policy initiatives before they are launched and to assist the European Commission and the Member States in implementing such policies initiatives with an NIS perspective.

    - Policy achievements and evolution in the ***area of cloud, supporting EU's cloud computing strategy and partnership***:

        - ENISA continues to play an active role in the implementation of the EU's cloud computing strategy. The Agency provides technical advice, recommendations and good practices to Commission's Selected Industry Groups in Cloud Computing (C-SIGs). ENISA is the leader of the C-SIG on certification publishing two tools (Cloud Certification Schemes List and Cloud Certification Schemes Metaframework available here: https://resilience.enisa.europa.eu/cloud-computing-certification) fulfilling in this way the first objective of the strategy. The Agency also participated in the C-SIG on SLAs and Code of Conduct.

Cloud Cert Schemes List

Cloud Cert Schemes Meta

        - ENISA organised the 3rd Secure Cloud conference offering an interesting agenda for 2 days (SecureCloud2014). The conference was opened by Commission's Vice-President Kroes and involved many high-level presentations from both public and private sector experts.

    - Policy achievements and evolution in the ***area of smart grid, supporting EU's Smart Grids strategy***:

        - Since 2013, ENISA assists the Commission, Member States and the private sector in the implementation of the EU's smart grids strategy. The Agency provides technical advice, recommendations and good practices in the area of minimum security measures for smart grids, certification of smart grid components, privacy profile of smart meters, and incident reporting mechanisms. In 2014, the smart grid security measures were adopted by the Smart Grid Task Force of the European Commission.

        - To enhance this work the European Commission organised a dissemination workshop for the smart grid security measures with representatives from the private and public sector reaching out to the greater community. The outcome of this workshop is a decision of the European Commission to fund a study on costs and incentives of implementation of these security measures.

        - ENISA initiated collaboration with SOGIS (Senior Officials Group for Information Systems Security) on ICT security certification. Together with the EU, the Agency jointly organised a workshop on IT security certification as a competitive advantage of European industry.

- Policy achievements and evolution in the ***area of personal data protection and secure services, supporting the reform of data protection framework***:
  - In 2013, ENISA initiated a new activity in the area of cryptography with an emphasis on providing technical specifications for cryptographic algorithms to protect personal data in e-government (eGov) services. Technical protection measures to prevent data breaches, specified in legal documents such as European Commission regulation 611/2013, need to be matched with technical specifications in order to secure personal data. During 2014, ENISA updated the recommendations published during 2013 and extended them to cover more application scenarios such as cloud computing.
  - In 2014, ENISA published its first best practice guide for prevention of data leakage and appropriate controls for the access of data using security and privacy by design and by default to support with a technical perspective the policy requirements for data protection.
  - Furthermore ENISA organised an event, the Annual Privacy Forum (APF'2014), to establish a forum fostering the exchange of information and experiences between the research and academic communities, and the EU policy and industry representatives in the area of privacy and data protection. The event, organised together with European Commission DG CONNECT followed the success of the first edition of APF'2012. The focus of the event was to bring a strong technical perspective to the debate, to focus on mechanisms to protect personal data, and to allow different communities to exchange best practices.
- Policy achievements and evolution in the ***area of EU electronic identification and trust services framework, supporting the new regulation on trust service providers:***
  - ENISA continued and expanded its support focusing the recently adopted Regulation on electronic identification and trusted services for electronic transactions in the internal market. ENISA has already contributed to this area by providing recommendations in the areas of mechanisms for reporting security breaches by the trust service providers to the competent bodies and minimum security measures and security best practices for trust services providers.
  - During 2014, ENISA focused its support related to the implementation of the provisions of the proposal, with a focus on the areas of common audit schemes for trust services providers in Member States as well as technical guidelines for conformity assessment bodies performing audits and trust service providers.

- WPK1.3. ***Supporting the EU in education, research and standardisation***.
  - During 2014, ENISA continued its efforts to support EU funded R & D initiatives such as FP7 and H2020 and standardisation activities including EU initiatives such as the ETSI CEN CENELEC Cyber Security Coordination Group (CSCG). Furthermore, activities have been carried out in the area of education following the objectives of the NIS cyber security strategy such as NIS driving license and European Cyber Security Month 2014 (ECSM'2014).
  - Policy achievements and evolution in the ***area of standardisation, supporting NIS cyber security strategy and the Action Plan for an innovative and competitive Security Industry as well as Council Resolution on a collaborative European approach to Network and Information Security:***
    - Since 2012, ENISA contributes actively to the creation and work of the ETSI CEN-CENELEC cyber security coordination group (CSCG). This collaboration with CSCG continued during 2014 seeking out synergies with the Agency's work programme and involved standardisation bodies in the different work packages, as appropriate.
    - Responding to a request from ETSI, ENISA participated in the review of the ETSI technical specification TS 119 312 — Electronic signatures and infrastructures (ESI) cryptographic suites.

- In 2014, ENISA developed an inventory of relevant standardisation activities in the areas of NIS and privacy.

- Policy achievements and evolution in the ***area of education, supporting NIS cyber security strategy:***

  - Contribution to the 'EU NIS driving licence'. Together with relevant stakeholder community, ENISA coordinated the development of a road map for the implementation of a 'Network and information security driving licence'. This road map covers the needs of different levels of education, e.g. primary, secondary and tertiary education. It exploits existing material and synergies among relevant training bodies.

  - ENISA contributed/participated in the evaluation of the calls of proposals for EU funded R & D published by the European Commission and provides advice via advisory boards for EU funded projects.

  - ENISA also analysed the status of cyber security competitions in Europe. Such competitions could be used to trigger an interest for the area of NIS.

  - During 2014 ENISA supported the European Commission in preparing the European Cyber Security Month 2014 (ECSM'2014). This is a continuation of the activity of 2013; during 2014 many more Member States participated in ECSM.

2.1.1.1 General achievements. Achievement of Impact Indicators

WS 1	**WS1- Support EU policy building**	
Nr.	Impact indicator (I.I.)	Achieved results
WPK1.1.	**WPK 1.1: Identifying evolving threats, risks and challenges**	
I.I.1.1-1	The ENISA Threat Landscape becomes an important point of reference for security experts worldwide and is referenced in at least 10 security related information sources worldwide.	Achieved: More than 20 different organisations are using the conclusions of ENISA's Threat Landscape report 2014. Several hundred references to ENISA Threat Landscape 2013 have been made via the main cyber security web pages and blogs.
I.I.1.1-2	It is referenced by five stakeholders from the two sectors covered.	Achieved: Both ENISA thematic threat landscapes have been referenced by couple of tens of stakeholders from Internet infrastructure, smart home and converged media sectors.
I.I.1.1-3	Identified emerging threats and trends have been taken into consideration in at least five R & D projects in EU.	Achieved: Most of the threats identified in ENISA thematic landscapes have been addressed in various H2020 projects. This has been assessed by reviewing activities of ENISA in H2020 projects. A detailed assessment of which projects manage which threat/risk has yet to be performed by the time of publication.
WPK1.2.	**WPK 1.2: Contributing to EU policy initiatives**	
I.I.1.2-1	10 cloud computing providers and five Member States support ENISA's recommendations for improving NIS aspects of cloud computing	Achieved: More than 20 providers and 15 Member States support ENISA's recommendations on cloud security.
I.I.1.2-2	15 smart grids providers and five Member States competent authorities support ENISA's guidelines for implementing the smart grids strategy	Achieved: More than 30 experts from private sector DSOs (distribution system operators), manufacturers, vendors and public energy regulatory authorities and TSOs (transmission system operators) supported the guidelines.
I.I.1.2-3	Five Member States eID competent bodies/authorities, five independent auditing bodies and five trust service providers take part in the development of a common audit framework for trust service providers.	Achieved: In total, more than 35 stakeholders requested to review the draft document, including FESA members (Member States), TSPs and auditing bodies. The paper underwent reviews in different stages of the development process.

I.I.1.2-4	ENISA recommendations on algorithms and parameters for secure services for the protection of personal data in the context of eGov services supported by competent authorities in at least five Member States;	Achieved: The reports providing guidelines for securing personal data (cryptographic measures, privacy technologies) were produced in collaboration with well-known experts from different States and competent authorities. Furthermore, feedback was provided by competent authorities. The reports are supported by competent authorities from more than five different Member States and standardisation bodies.
WPK1.3.	**WPK 1.3: Supporting EU in education, research and standardisation**	
I.I.1.3-1	At least five members of the R & D community integrate NIS components in their activities and projects.	Achieved: Representatives from 11 countries participated in the work undertaken by ENISA — workshops and reports. In 2014 various scenarios were developed, which will be further implemented during 2015.
I.I.1.3-2	Two seminars or workshops organised to validate the usefulness of NIS driving license material, addressed to different target audiences, with a minimum of 10 participants from several Member States.	Achieved: 2 seminars organised in April and September to prepare and to validate the deliverable published: 'Roadmap for NIS education programmes in Europe'. The road map is structured in three parts. The first part maps the courses and materials available. The second part presents the gaps between existing training/certification schemes and market needs, including proposals of scenarios to narrow the existing gaps. Finally, a list of recommendations is presented for further steps and an open call from ENISA is available in order to identify leading organisations best positioned to further work on the implementation. Approximately 40 participants from more than 10 Member States participated in the workshops.

2.1.1.2 Specific achievements. Mapping of deliverables into papers/publications/activities

WS 1	**Support EU Policy Building**	
Nr.	WP 2014 Planned deliverable	Deliverables /publications and links
WPK 1.1	**Identifying technological evolution, risks and challenges**	
D1	Annual EU Cyber Security Threats Landscape	'ENISA Threat Landscape 2014', https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2014
D2	Identification of trends, security challenges, associated risks and required countermeasures, for emerging technologies (with special attention to selected areas/sectors)	1) 'Threat Landscape and good practice guide for smart home and converged media' https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/threat-landscape-for-smart-home-and-media-convergence/ 2) 'Threat Landscape and good practice guide for Internet infrastructures' https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/iitl
WPK 1.2	**Contributing to EU policy initiatives**	
D1	Engaging Cloud Computing Stakeholders in the EU's Cloud Computing Strategy and Partnership (workshops, contributions to Commission's SIG and ECP work, Q2-Q4 2014)	ENISA, together with Cloud Security Alliance (CSA) and Fraunhofer-FOKUS, organised SecureCloud, a European conference with a specific focus on cloud computing security, on 1-2.04.2014. https://cloudsecurityalliance.org/events/securecloud2014/ Contributions EU Cloud Strategy (WG Certification, WG SLAs).
D2	Engaging with stakeholders for the secure implementation of EU's Smart Grids policies (workshops, contributions to COM' EG 2 and MS actions, Q2-Q4 2014)	Dissemination workshop for the EG2 deliverable on 'Security measures for smart grids' organised on 02.04.2014. Participated in Smart Grid Task Force — Expert Group 2 (managed by EC DG ENER) and provided contributions to the group.
D3	Algorithms and parameters for secure services (study, Q4)	'Algorithms, key size and parameters report 2014', https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014 'Study on cryptographic protocols', https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/study-on-cryptographic-protocols
D4	Best practice guide for Privacy and Security by Design and Default for the prevention of data leakage and appropriate controls for the access of data (report, Q4)	'Best practice guide for Privacy and Security by Design and Default', https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design/

D5	Auditing framework for trust services: Technical guidelines for independent auditing bodies and supervisory authorities on the implementation of audit schemes for trust service providers in MS. (Report, Q3 2014)	'Auditing framework for trust services' https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp-auditing-framework/
D6	Annual Privacy forum 2014 (APF'2014) (Workshop, report, Q2-Q4 2014)	Forum took place in Athens on 20-21.05.2014. Report: 'Privacy Technologies and Policy' http://privacyforum.eu/news/proceedings-apf14-privacy-technologies-and-policy http://2014.privacyforum.eu/programme
WPK1.3	**Supporting the EU in education, research and standardisation**	
D1	Inventory of standardisation activities in NIS and Privacy (Workshops, report, Q1-Q4, 2014)	'Standardisation in the field of Electronic Identities and Trust Service Providers', https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/standards-eidas
D2	Road map for the implementation of the 'NIS Driving license"	1) 'Cyber security competitions — the status in Europe', https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/cybersecurity-competitions-2014-the-status-in-europe 2) 'Roadmap for NIS education programmes in Europe', https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/roadmap-for-nis-education-programmes-in-europe 3) Extra mile: 'Public Private Partnerships in Network and Information Security Education', https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/public-private-partnerships-in-network-and-information-security-education

2.1.2 Policy achievements in WS2-Support capacity building

EU Member States and private sector companies have different maturity levels in their capabilities to address cyber-attacks and disruptions. ENISA, with this work stream, aims to raise the level of security across Member States and the private sector by supporting the development of relevant capabilities.

The following work packages constitute Work Stream 2. For each work package, the main objectives and policy achievements are identified.

- WPK 2.1. ***Support Member States' capacity building***
  - The objective of this work package is to support the development of prevention, detection, analysis and response capabilities within Member States institutions and EU institutions.
  - Policy achievements and evolution in the ***area of cyber security strategies, supporting the Digital Agenda and the EU cyber security strategies***:
    - ENISA continues to support Member States in developing their capabilities in the area of National Cyber Security Strategies (NCSS). The Agency, building on previous work in the area of NCSS, acted during 2014 as facilitator among Member States and fostered the sharing of good practices. In 2013, ENISA created a map of cyber security strategies; in 2014, this became a central point of information on existing strategies from the EU and across the world. The map is updated regularly (and is available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world).
    - ENISA took stock of existing evaluation/assessment mechanisms of NCSS, identifying good practices, validating them with public and private sector and finally issuing a white paper with practical recommendations on the evaluation and update of existing NCSS. ENISA created in 2013 the NCSS working group with experts from the governmental agencies dealing with NCSS. In 2014, five new Member States representatives joined the group. The first workshop on NCSS took place in 2014 and gathered more than 50 participants from the public and private sector and the European Commission.

- Policy achievements and evolution in the ***area of developing CERT capabilities, supporting the Digital Agenda:***

    - In 2014, ENISA built upon its work in this area, and took stock of its work in the area of CERTs in the last 8 years. The goal was to concisely draw 'lessons learned' through a dialogue with relevant stakeholders, and to draw a road map of CERT activities for the coming years.

    - To support above-mentioned action, on request, tailored support capability building for CERTs trainings were organised focusing on suitable exercises to technical staff from EU Member States, EU institutions and other appropriate audiences.

- Policy achievements and evolution in the ***area of regional, sector-specific and national cyber exercises, supporting EU Cyber cyber security strategy:***

    - In the past, the Agency has supported national, regional and sectorial cyber exercises efforts upon request (Art14 of the ENISA regulation). This effort continued in 2014 in line with the ENISA regulation, the EU cyber security strategy and the EU Member States' needs.

    - Where appropriate the Agency collaborated with and supported regional or sectorial cyber exercises in a cost efficient manner, for example by re-using exercise planning and management knowledge and tools from other exercises and efforts.

- Policy achievements and evolution in the **area of National and European PPPs, supporting EU Cyber Security Strategy:**

    - ENISA continued to support Member States in the development of their capabilities in the area of national public-private partnerships (PPPs). A limited number of PPPs openly discussed with ENISA on the structure, topics and procedures followed. This year ENISA was able to engage with more than 12 Member States on the topic of NCSS, where national PPPs are present. During the NISP and NCSS meetings there were more than 15 private companies consulted on the topic.

- WPK 2.2. ***Support private sector capacity building***

    - The objectives of this work package were to focus on enhancing the capabilities of the private sector through cooperation with the public sector in several areas such as smart grids, ICS-SCADA, cloud computing, finance and electronic communication networks. The work carried out in this context attempted to improve the capacity of the Member States for dealing with large-scale cyber incidents, by improving the state of preparedness of the private sector community. ENISA assisted Member States in achieving this by providing assistance and advice but did not engage in operational work.

    - Policy achievements and evolution of the activity **leverage the NIS Platform as a tool to enhance public private cooperation, as covered by EU Cyber Security Strategy:**

        - In 2014, ENISA supported the NIS platform, the successor of EP3R, with the goal of engaging more targeted public and private stakeholders, especially experts from small industry players. ENISA supported the working groups and their chairpersons (e.g. via the resilience portal, conference calls), contributing to the outcomes of the working groups, and ensuring its quality. The Agency kept the working groups informed about the latest developments in their respective areas including deliverables published by the Agency (e.g. art. 13 a working group).

        - The NIS platform community has grown exponentially: Over 500 participants from all Member States, involvement of public, private sector and academia. The NISP working groups called for future research and evolution of security practices for large and SMEs.

    - Policy achievements and evolution of the activity on **Provide advice and assistance to targeted stakeholder communities, as covered by EU cyber security strategy and CIIP action plan:**

        - In 2014, the Agency also took stock of existing initiatives on the certification of cyber security skills of ICS-SCADA experts and issued practical recommendations to stakeholders for the wide deployment of such schemes. A workshop under the topic was organised, bringing together 60 experts from this community (public and private sector).

        - ENISA runs an expert group with 15 experts from utilities manufactures vendors and public authorities. In addition, ENISA is supporting and contributing to the EURO SCSIE group, a recognised WG on ICS SCADA security.

        - As an additional study, ENISA issued a report on 'Smart grid certification in Europe: challenges and recommendations' and organised a validation workshop.

        - In the area of Cloud Computing and in order to support cloud certification activities for the EC Cloud Strategy, ENISA collected the ICT security requirements for the public sector from 12 Member States. This study has been complemented by the community, which has been enhanced by the effort of ENISA to centralise the information collected. This undertaking has been greatly appreciated by the European Commission and the community.

        - ENISA, under the 'Governmental clouds' study, created a useful 'how-to' guide with a step-by-step procedure the public administrators would need to follow to deploy cloud services. This study has been validated by 4 user cases of cloud computing implementations in the Member States.

        - Since 2013, ENISA runs a working group with experts from 17 Member States on the area of governmental Clouds, which validates and supports ENISA's work.

        - ENISA provided advice in the area of finance, as covered by *Network and information security in the finance sector* study. ENISA study was completed by interviewing 12 NCBs (national central banks), and 15 industry representatives. The Agency identified possible areas of improvement and issued recommendations that will improve the security of transactions in the finance sector.

        - The Electronic Communications (eComms) reference group has grown and it now comprises of 23 providers that support ENISA's work on a harmonised framework for minimum security measures.

        - Under this experts' group, the Internet Infrastructure security and resilience reference group was created. This group brings together 20 technical experts in network operations, cyber security and contingency, with representatives from Internet organisations, Internet service providers, academia and governments from 10 different Member States. In 2014 the contributions of this group to the ENISA deliverable 'threat landscape of the Internet infrastructure' and 'Methodologies for the identification of CIIs assets and services' were fundamental and helped to focus the studies.

- WPK 2.3. ***Raising the level of preparedness of EU citizens***

    - The objectives of this work package were to (a) support awareness-raising and training activities in Member States to develop the security dimension in the use of ICTs and (b) support the organization of the cyber security month by providing expertise related to the activities of ENISA.

October is European Cyber Security Month

    - Achievements and evolution in the activities linked to ***raising the level of preparedness of EU citizens, supporting ENISA objectives and the cyber security strategy:***

- Through its NIS expertise, ENISA participated together with different stakeholders in actively promoting cyber security awareness. The 2014 activities were built on the activities from previous years; at the same time the 2014 results provided the priorities and the context for growth and development for the future years.

- The agency supported the European Commission in preparing and running the European Cyber Security Month (ECSM), in October 2014. A report was also published assessing the impact and the development of ECSM 2014.

- ENISA maintained a webpage and supported ECSM by providing a new self-assessment tool, using the ENISA knowledge database and the agencies deliverables as raw material. ENISA established partnerships with academic institutions and provided information and expertise in its core areas in order to feed the academic curricula and the recommendations from ENISA reports.

- Furthermore ENISA cooperated with educational bodies to do all the preparatory activities to successfully organize a cyber-security championship from 2015 where university students will compete in proposing NIS solutions.

2.1.2.1 General achievements. Achievement of impact indicators

WS2	**WS2- Support capacity building**	
Nr.	Impact indicator (I.I.)	Achieved results
WPK2.1.	**WPK 2.1: Support member states' capacity building**	
I.I.2.1-1	10 Member States and five private companies support ENISA's conclusions on national cyber security strategies	Achieved: The ENISA NCSS working group is comprised of 14 Member States and 1 EU country and is actively contributing to the ENISA NCSS studies. More than 15 private companies (mostly from energy sector) support ENISA recommendations.
I.I.2.1-2	Improved operational practices of CERTs (ongoing support with best practices development) training provided to a minimum of 20 participants of different organisations	Achieved: In total more than 135 people were trained in the year 2014 (675 % achievement); and the new CERT training material achieved around 20 000 unique page views (published Q4/2014), whilst for the existing material succeeded in attracting over 134 000 unique page views in 2014.
I.I.2.1-3	6 Member States and 10 private companies support ENISA recommendations on national PPPs	Limited achievement. NPPPs received feedback from only four Member States, whilst the only industry player that agreed to reply was from Portugal. The final work was not substantial enough to be published.
WPK2.2.	**WPK 2.2: Support private sector capacity building**	
I.I.2.2-1	10 Member States and 20 Private Companies contribute to NIS Platform Working Groups	Achieved: 20 Member States and more than 300 organisations are subscribed in the NIS Platform working groups
I.I.2.2-2	10 ICS-SCADA providers/manufacturers support ENISA's conclusions on the Certification of Cyber Security Skills of ICS-SCADA experts	Achieved: ENISA runs a working group with 15 experts from utilities manufactures vendors and public authorities. In addition ENISA supports and contributes to the EURO SCSIE group, a highly recognised WG on ICS SCADA security.
I.I.2.2-3	15 Cloud Computing Providers and five Member States competent authorities contribute to ENISA's study on minimum security measures for cloud computing.	Achieved: 20 Cloud providers and 12 Member States participated in the study for 'Cloud certification metaframework'.
I.I.2.2-4	12 Cloud Computing Providers and five Member States competent support ENISA's conclusions on Procurement Guidelines for Cloud Computing Providers	Achieved: 20 cloud providers and 7 Member States participated in the study 'Security framework for governmental clouds'.
I.I.2.2-5	10 Finance Sector IT Security/IT Auditors agree on ENISA's recommendations on secure inter-banking communications and transactions.	Achieved: 25 experts participated in EG FI which supported the ENISA study on 'Network and Information Security in the Finance Sector'. Eight Member States are represented in this EG.
I.I.2.2-6	10 e-comms providers support the Harmonised Minimum Security Measures for ISPs	Achieved: The participants in the ENISA Electronic Communications Reference Group which consist of 23 providers; support ENISAs work on a joint technical guideline on Article 13a (Telecom Framework Directive) security measures and Article 4 (ePrivacy Directive) security measures.

WPK2.3.	WPK 2.3: Raising the level of preparedness of EU citizens	
I.I.2.3-1	At least 20 of the EU Member States involved in the European Cyber Security Month;	Achieved: 27 Member States and 3 other partners involved in ECSM.
I.I.2.3-2	Ensure that a minimum of five Member States support the cyber security championship;	Achieved: Five Member States were involved in the workshop in preparing the ground for the 2015 Championship
I.I.2.3-3	Improved consultation process in order to feed the activities of next years;	Achieved: Several consultation meetings and surveys were organised in order to receive the input from all parties involved in view of deployment in 2015 and beyond.

2.1.2.2 Specific achievements. Mapping of deliverables into papers/publications/activities

WS2	Support Capacity Building	
Nr.	WP 2014 Planned deliverable	Deliverables /publications and links
WPK2.1	**Support Member States' capacity building**	
D1	Assisting MS in building capabilities on NCSS (workshops, Q1-Q4)	Workshop on Cyber Security Strategies organised on 27.11.2014, https://resilience.enisa.europa.eu/enisas-ncss-project/enisa-cyber-security-strategies-workshop
D2	White paper — How to evaluate a national cyber security strategy (report, Q3 2014)	'An evaluation framework for Cyber Security Strategies', https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1/an-evaluation-framework-for-cyber-security-strategies
D3	Good practice guide on training methodologies, etc. for operational teams and communities like CERTs ('Train the trainers handbook') derived from experiences from delivering suitable CERT training (Q4 2014)	'Good Practice Guide on Training Methodologies', https://www.enisa.europa.eu/activities/cert/support/exercise/good-practice-guide-on-training-methodologies
D4	Regular update of 'Baseline capabilities' definition and status and conclusions for new training material (Q4, 2014)	'"Baseline Capabilities" definition and status', https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/national-governmental-certs-enisas-recommendations-on-baseline-capabilities/
D5	New set of CERT exercise material with at least five new scenarios from the four areas of the 'Baseline capabilities', including the topic of processing of actionable operational information (Q4 2014)	1) Developing countermeasures; 2) Common framework for artefact analyses activities; 3) Advanced artefact handling; 4) Processing and storing artefacts; 5) Building an artefact handling and analyses environment. All available here: http://www.enisa.europa.eu/activities/cert/training/training-resources
D6	Stocktaking of achievements in the area of CERTs and a draft road map to plan future work in this area (Q4 2014)	'Impact Assessment and Roadmap', https://www.enisa.europa.eu/activities/cert/other-work/supporting-the-cert-community-impact-analysis-and-roadmap
D7	Assisting MS in building capabilities on national PPPs (workshops, Q1–Q4)	Panel on PPPs during the National Cyber Security Strategies workshop, 27.11.2014, https://resilience.enisa.europa.eu/enisas-ncss-project/enisa-cyber-security-strategies-workshop
WPK2.2	**Support private sector capacity building**	
D1	Support the working groups of the NIS platform (workshops, contributions, technical support, Q1–Q4, 2014)	1) NIS Platform: - Support DG CNECT — H4 for project Management and coordination of WGs and rapporteurs - Support to DG CNECT — H4 in the organization of the plenary meetings of the 30 April 2014 and the 25th November 2014 - User management, mailing lists, online collaboration and content management on the Resilience portal 2) Report 'EP3R 2009-2013 future of NIS Private public cooperation' https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/ep3r-2009-2013

D2	White paper on the certification of smart grids (report, Q3, 2014)	'Smart grid security certification in Europe', https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/smart-grid-security-certification Validation workshop for 'Smart Grid Components Certification' reports organised on 30.09.2014, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2014/certification-of-cyber-security-skills-of-ics-scada-experts-and-smart-grid-components
D3	White Paper on the Certification of Cyber Security Skills of ICS SCADA experts (report, Q3 2014)	'Recommendations for developing harmonised certification schemes at European level for Cyber Security Skills of ICS SCADA experts' https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/certification-of-cyber-security-skills-of-ics-scada-professionals Validation workshop for the 'CERTIFICATION OF CYBER SECURITY SKILLS OF ICS SCADA EXPERTS' report organised on 30.09.2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2014/certification-of-cyber-security-skills-of-ics-scada-experts-and-smart-grid-components
D4	Harmonised Minimum Security Measures for ISPs (report, Q4 2014)	'Technical guidelines on security measures for Art.4 and Art.13a', https://resilience.enisa.europa.eu/article-13/guideline-on-security-measures-for-article-4-and-article-13a/
D5	Minimum Security Measures for Cloud Computing (report, Q4, 2014)	'Cloud Certification Schemes Meta Framework', published on the resilience portal, https://resilience.enisa.europa.eu/cloud-computing-certification/cloud-certification-schemes-metaframework
D6	White Paper — Procurement Guidelines for Secure Cloud Computing Deployment (report, Q4, 2014)	'Security Framework for Governmental Clouds', https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/govenmental-cloud-security/security-framework-for-govenmental-clouds/security-framework-for-governmental-clouds
D7	Guidelines for the identification of critical services, assets and links in Electronic Communication Networks (report, Q4, 2014)	'Methodologies for the identification of critical information infrastructure assets and services', https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/Methodologies-for-identification-of-ciis
D8	Guidelines for Secure Inter-Banking Communications and Transactions (report, Q4, 2014)	'Network and Information Security in the Finance Sector — Regulatory landscape and Industry priorities', https://www.enisa.europa.eu/activities/Resilience-and-CIIP/nis-in-finance/network-and-information-security-in-the-finance-sector/
WPK2.3	**Raising the level of preparedness of EU citizens**	
D1	Provide technical guidance and support for European Cyber-Security Month (dissemination material, Q4 2014);	1) The launch of the event organised on 01.10.2014, alongside ENISA's high-level event '10 years of securing Europe's cyber security… and beyond!' 2) Dissemination materials available at: https://cybersecuritymonth.eu/ 3) European Cyber Security recommendations for all, http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2014 4) ESCM 2014 Deployment report, https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2014

2.1.3 Policy achievements in WS3-Support cooperation

Cooperation is a necessary prerequisite for strengthening the capacities of Member States, EU institutions and the private sector. During 2014, ENISA continued to build upon existing collaboration in existing communities, and to further enhance community building in Europe. ENISA continues to provide a supporting role for these communities, developing tools to facilitate and improve the international communication and interchange of security relevant information within communities sharing the same interest in different Member States.

The following work packages constitute Work Stream 3. For each work package the main objectives and policy achievements are identified.

- WPK 3.1. ***Crisis cooperation — exercises***.
    - The objective of this work package was to prepare and carry out the Cyber Europe Exercise 2014, in close collaboration with all relevant stakeholders.
    - Policy achievements and evolution in the **area of Pan-European Cyber Exercises, supporting EU Cyber Security Strategy, CIIP Action Plan 2009 and 2011, EU Internal Security Strategy:**
        - In 2014, ENISA organised the third pan-European cyber exercise, Cyber Europe 2014 (CE2014). This exercise built on the experience gained in previous exercises and took account of previous recommendations. The exercise was more ambitious than previous efforts, e.g., technical depth, scenarios, stakeholders involved, objectives, procedures to be tested, complexity etc.
        - The exact setup and exercise plan was agreed upon by the EU Member States and EFTA countries, in line with the EU cyber security strategy.
        - Enhancing the capacity to support and organise cyber exercises. ENISA further enhanced its methodology, seminars, trainings and technical capabilities on the organisation and management of large-scale cyber crisis exercises. The Agency continued enhancing its capabilities for managing complex, distributed exercises, by building on previous efforts in tools and methods and by facilitating strategic partnerships, such as the one with DG JRC. For example, more structural links have been established with the European Cybercrime Centre and the European Defence Agency.
        - Cyber Crisis Cooperation and Exercises activities overview. ENISA continued to support Member States in the maintenance and training of operational procedures for cyber crisis cooperation. This and the activities described above including key findings in the area of Cyber Crisis Cooperation and Exercises (C3E) are summarised in a report published at the end of 2014. This report will help ENISA to reach out to other communities/sectors with lessons learnt from supporting exercises (achieving broader impact).
    - In the ENISA WP 2014, an activity was proposed, pending the agreement of MB, covering a possible EU-US Cybersecurity Exercise. This activity was not carried out, in agreement with the European Commission and the ENISA MB.

Biggest EU cyber security exercise to date Cyber Europe 2014

- WPK 3.2. ***Implementation of EU legislation***.
    - The objectives of this work package were twofold, (a) the continuation of work in the area of Incident Reporting (Article 13a) by analysing the received data, and (b) the preparation for the reporting for Article 4 of the ePrivacy Directive and Article 15 [3] of the European Com-

[3] The Article 15 referring to '*Security requirements applicable to trust service providers*' in the *proposed* eIDAS regulation (Commission Communication (COM(2012)238 final of 4 June 2012) changed number to Article 19 in the *adopted* Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation), published in July 2014.

mission proposal for the Regulation on eID and trusted services.

- Policy achievements and evolution in the **area of analysis of incident reporting, supporting EU Cyber Security Strategy, Article 13a of the revised Framework Directive on electronic communications and Articles 4 of the ePrivacy Directive:**

    - ENISA continued collecting and analysing national reports of security breaches from NRAs in accordance with Article 13a of the Framework Directive on electronic communications. The annual incident report covering incident of 2013 was published during 2014. All the 28 Member States plus two EFTA countries sent to ENISA and the European Commission the annual reports for 2013.

    - All Member States use the ENISA Technical Guideline on Article 13a Incident Reporting in their annual reporting. More than 12 Member States and some of the larger European Electronic Communications Providers use directly or refer to the ENISA Technical Guideline on Security Measures.

    - The series of Article 13a expert's group meeting continue by having ENISA organising the 14th meeting of the group in October 2014 in Athens.

    - ENISA supported the creation of a joint WG of all the competent authorities of implementing the Article 4 (NRAs and DPAs) under the auspices of the European Commission.

    - Despite the fact that the deliverable foreseen in the work programme 2014 called 'Guidelines on Incident Reporting Scheme for Article15' was postponed for next year, according to WP2014 amendments, ENISA created a reference group of experts, called the Article19 EG ([4]), with representatives for 14 Member States.

- Some of the activities foreseen in ENISA WP2014 were amended during the year and two of the activities of WPK3.2 were cancelled due to the fact that the respective proposed legislation was not approved as considered in Work programme planning. The affected activities are: the Guidelines on Incident Reporting Scheme for Article 15 ([5]), in the context of regulation on electronic identification and trusted services, as well as the activity intended to Support the implementation of the upcoming NIS Directive.

- WPK 3.3. ***Regular cooperation among NIS communities***.

    - The objective of this work package was to further enhance the cooperation between operational communities, mainly CERTs and Law Enforcement Agencies.

    - Achievements and evolution in the activities linked to ***NIS cooperation*****, supporting EU Cyber Security Strategy, Digital agenda, the communication on EU Internal Security Strategy:**

        - During 2014, ENISA continued to actively support, and when appropriate, organise common trainings with communities such as CERTs and LEA; two workshops from the annual series of workshops 'CERTs in Europe' were organised in 2014, which was the 9th annual edition.

        - ENISA leveraged synergies with the European Cyber Crime Centre (EC3), through formal and informal cooperation channels, where appropriate respecting the respective mandates.

        - During 2014, the Agency continued to collect good practices for CERTs and LEAs, and further enhanced the ENISA exercise and training material. ENISA took stock of existing communities and cyber security challenges related to the work of CERTs and published best practices and guidelines.

[4] Refers to Article 19 '*Security requirements applicable to trust service providers*' of the *adopted* Regulation (EU) N°910/2014.

[5] Refers to Article 15 of the *proposed* eIDAS regulation. As explained in previous footnotes, in the adopted Regulation (EU) N°910/2014, this is now Article 19 '*Security requirements applicable to trust service providers*'.

2.1.3.1 General achievements. Achievement of Impact Indicators

WS3	**WS3 — Support cooperation**	
Nr.	Impact indicator (I.I.)	Achieved results
WPK3.1.	**WPK 3.1: Crisis cooperation — exercises**	
I.I.3.1-1	At least 24 EU Member States and EFTA countries confirm their support for Cyber Europe 2014 (CE2014)	Achieved: CE 2014 involved 1400 experts and over 450 teams, with an equal representation of public and private sector teams (n/g CERTs, Cybersecurity Agencies, Public Sector teams, Telecom Operators, Energy Sector Companies). In the different phases of Cyber Europe 2014 there were 29 different participating countries (26 EU Member States, 3 EFTA) and the EU Institutions. In the first phase of CE2014 (TLEx) over 600 experts were involved, coming from 214 teams representing both private and public sector institutions (n/g CERTs, Cybersecurity Agencies, Public sector entities, telecom operators, energy sector companies etc.). In the second phase of CE2014 (OLEx) we had over 800 experts. An impressive total of over 1400 experts were involved in the exercises in some way during CE2014. Member States have declared their satisfaction to the exercise through evaluation surveys and through communications via the ENISA Management Board members and NLOs.
I.I.3.1-2	At least 80 % of Member States that are in the process of establishing National Contingency Plans by 2016 are supported by ENISA.	Achieved: One of the objectives of CE2014 was to give the opportunity to Member States to test their national capabilities and procedures. Out of the 29 countries (EU and EFTA) that collectively participated in the first two phases of CE2014 (TLEx and OLEx) all have confirmed that they have tested their national contingency plans and capabilities. Overall 29 countries (26 EU Member States, 3 EFTA) were supported.
I.I.3.1-3	At least 24 Member States are familiar with the operational procedures during cyber crisis by 2016	Achieved. The second phase of CE2014 was mainly focused on testing the operational procedures for cyber security cooperation in Europe. All of the 26 countries that participated in this phase were trained to use these procedures. In addition, the countries that did not play in this phase had access to and received the updated version of the SOPs within the pilot SOP portal within the Cyber Exercise Platform.
WPK3.2.	**WPK 3.2: Implementation of EU legislation**	
I.I.3.2-1	23 Member States contribute to ENISA's work on the implementation of Article 13a and 12 Member states directly use the outcomes of this work by explicit references or by adopting the same approach nationally.	Achieved: All 28 Member States plus two EFTA Countries sent to ENISA and the Commission annual summary reports about incidents that occurred in 2013. All Member States use the ENISA Technical Guideline on Article 13a Incident Reporting in their annual reporting. More than 12 Member States and some of the larger European Electronic Communications Providers use directly or refer to the ENISA Technical Guideline on Security Measures. During 2014 ENISA has performed three workshops with the Article 13a Expert Group attended by NRAs from around 20 Member States.
I.I.3.2-2	10 Member States contribute to the work facilitated by ENISA on implementing and enforcing article 4 and 6 Member States make direct use of the outcomes of this work by explicit references or by adopting the same approach nationally.	Achieved: The participants in the ENISA Electronic Communications Reference Group consisting of 23 Providers support ENISAs work on a joint technical guidelines on Article 13a (Telecom Framework Directive) security measures and Article 4 (ePrivacy Directive) security measures.
I.I.3.2-3	10 Member States contribute to ENISA's work on implementing article 15	Work postponed. Based on the WP2014 amendment (October 2014) due to the late adoption of the regulation on trust service providers, the deliverable addressing Article 15, of mentioned regulation, has been postponed for 2015.

WPK3.3.	WPK 3.3: Regular cooperation among NIS communities	
I.I.3.3-1	At least 10 Member States and two national/international LEA support the conclusions of the 9th ENISA CERT workshop.	Achieved: In total we hosted 44 participants from several parties: 19 Member States + Switzerland + Norway; 10 international organisations + 11 LEA + 23 CERTs
I.I.3.3-2	At least 10 Member States support the Good Practice Guide and/or (where applicable) training and exercise material for the exchange and processing of actionable information by CERTs	Achieved. As part of expert group, reviewers, commenters ENISA hosted teams from Siemens (Germany), SWITCH (Switzerland), Portugal (CERT.PT), Poland (CERT.PL), Austria (CERT.AT) Czech Republic (CESNET), from the US (CERT.CC and US-CERT) international organisations like FIRST, NEC, NATO, NAIST, Invincea and the CSIRT Gadgets Foundation (13 teams altogether). In the BoF session at the FIRST conference 2014 many more teams provided input for the study. Participants in the TF-CSIRT meeting in Las Palmas: CERT.AT, CERT.EE, CERT.CZ, Inteco-CERT, Janet, CSIRT.MU, CERT.PL, CERT.PT, SWITCH, CIRCL, Siemens CERT, Pionier-CERT/PSNC, Panasonic, XING-cert, IRIS-CERT, UiO-CERT (14 teams)
I.I.3.3-3	10 operational CERTs agree to adopt the recommendations of stocktaking on channels and formats for exchange of operational information	Achieved. Most of the EU teams use the same or similar concepts and models like the study laid out. Several discussions throughout the year and addressing the CERT communities resulted in positive feedback from a minimum of 13 Member States (from several teams, among them from Portugal, Poland, Austria, Switzerland, Luxembourg, Romania, Denmark, Norway, Czech Republic, Germany, Latvia, Belgium, CERT-EU, etc.)
I.I.3.3-4	Two CERTs agree to pilot the good practice material for first responders (material developed in cooperation and accordance with the EC3) (Q4)	Achieved. Teams from Switzerland, Portugal and Czech Republic agreed to pilot the material, so that when ENISA does a follow-up project, experiences will already exist.

2.1.3.2 Specific achievements. Mapping of deliverables into papers/publications/activities

WS3	**Support cooperation**	
Nr.	WP 2014 Planned deliverable	Deliverables/publications and links
WPK3.1	**Crisis cooperation — exercises**	
D1	Cyber Europe 2014: Exercise Plan and Exercise (exercise, Q4 2014)	Exercise organised on 30.10.2014.
D2	Report on Cyber Crisis Cooperation and Exercise Activities and Findings (report, Q4 2014)	'Report on Cyber Crisis Cooperation and Management', https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/ccc-study
D3	EU-US Cyber security exercise plan	Was subject to further approval and it was not carried out.
WPK3.2	**Implementation of EU legislation**	
D1	Analysis of Annual 2013 incident reports and recommendations on addressing significant incidents (report, Q2/3 2014)	1) 'Annual Incidents report 2013', https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2013 2) 'Technical Guideline on Incident Reporting V2.1', https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/Technical %20Guidelines %20on %20Incident %20Reporting/technical-guideline-on-incident-reporting 3) 'Technical Guideline on Security Measures V2.0', https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/technical-guideline-on-minimum-security-measures/technical-guideline-on-minimum-security-measures 4) 'Secure ICT Procurement in Electronic Communications', https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/requirements-ecomms-vendors/secure-ict-procurement-in-electronic-communications 5) 'Security Guide for ICT Procurement', https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/requirements-ecomms-vendors/security-guide-for-ict-procurement 6) 'Protection of underground electronic communications infrastructure', https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/protection-of-underground-infrastructure
D2	Guidelines on Incident Reporting Scheme for Article 15 (report, Q4 2014)	Cancelled (See Amendment of WP 2014). First ENISA workshop with national authorities held in Brussels on the 17.11.2014. Minutes available upon request.
D3	Support the implementation of the NIS Directive (workshops, Q2-Q4)	Cancelled (See Amendment of WP 2014).
WPK3.3	**Regular cooperation among NIS communities**	
D1	9th ENISA CERT workshop to prepare a road map for future work of ENISA in the area of CERT training and CERT cooperation with LEA (in cooperation with EC3)(Q4)	ENISA 9th annual workshop 'CERTs in Europe'. Two parts. Part I organised on 27-28.05.2014 and Part II organised on 13-14.10.2014.
D2	Good practice guide and/or (where applicable) training and exercise material for the exchange and processing of actionable information by CERTs (Q4 2014)	'Best practice guide on exchange processing of actionable information — exercise material', https://www.enisa.europa.eu/activities/cert/support/ActionableInformationforSecurityIncidentResponse.pdf
D3	Draft report *Stocktaking on channels and formats for exchange of operational information*	'Stocktaking of standards formats used in exchange of processing actionable information', https://www.enisa.europa.eu/activities/cert/support/ActionableInformationforSecurityIncidentResponse.pdf
D4	Draft report *Scalable and accepted methods for trust building within and among communities*	'Scalable and Accepted Methods for Trust Building in Operational Communities', https://www.enisa.europa.eu/activities/cert/support/information-sharing/scalable-and-accepted-methods-for-trust-building
D5	Good practice material for first responders in cooperation with the EC3 (Q4)	'Good practice material for first responders', https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/electronic-evidence-a-basic-guide-for-first-responders/

2.1.4 Horizontal operational activities

2.1.4.1 Article 14 requests

This section provides an overview of the requests to the Agency according to article 14 of Regulation (EU) No 526/2013.

In summary, key figures are the following: 12 new requests in 2014 while 19 ongoing requests (including 2013) from following countries: Austria, Croatia, Cyprus, Czech Republic, Estonia, Germany, Greece, Italy, Latvia, Luxemburg, Malta, Poland, Portugal, Spain and from European Commission. The effort in man days was provided by staff from the Core Operations Department — there were no additional staff costs incurred. The budget was provided out of the Title 3 budget.

	Origin	Institution	Title
1	Austria	Bundeskanzleramt Österreich	Abuse helper project
2	Croatia	Croatian Regulatory Authority for Network Industries (HAKOM)	Assistance to enhance cyber security capabilities in Croatia
3	Cyprus	Office of the Commissioner for Electronic Communications and Postal Regulation (OCECPR)	Participating in the pilot step-by-step guide, best practices of national risk assessments for cyber security
4	Czech Republic	National Security Authority	Assistance to enhance the cyber security capabilities in the Czech Republic
5	European Commission	DG Connect — Directorate H; Unit 4 Trust and Security	Cryptographic protection measures supporting Regulation (EU) No 611/2013 of 24 June 2013
6	Estonia	Estonian Information Systems Authority	Request for training on Planning and Organising Exercises
7	Estonia	Estonian Academy of Security Services	Request for support for 'First responders and cyber forensics' course CEPOL
8	Germany	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BFDI)	Cooperation in area of privacy
9	Greece	Hellenic National Defence General Staff	Request for support by the MoD Greece — PANOPTIS
10	Greece	Hellenic Ministry of Infrastructure, Transport and Networks	Request by the Hellenic Ministry of Infrastructure, Transport and Networks
11	Italy	Istituto Superiore delle Comunicazioni e delle Tecnologie dell' Informazione Ministero dello Sviluppo Economico	Technical meeting of the Governmental/National CERTs
12	Latvia	Institute of Mathematics and Computer Science University of Latvia	Organizing training courses in Latvia
13	Luxembourg	Le Gouvernement du Grand-Duché De Luxembourg Ministère de l'Économie Direction du commerce électronique et de la sécurité de l'information	Organization of a CERT workshop in Luxembourg on the 24th of October
14	Malta	Malta Critical Infrastructure Protection Unit	Organizing training courses in Malta
15	Malta	Malta Critical Infrastructure Protection Unit	On-site training of ENISA CERT Training
16	Poland	NASK (Research and Academic Computer Network)	Honeynet Project Workshop
17	Portugal	CERT Portugal	Call for inputs on BEREC WP 2015
18	Portugal	Autoridade Nacional de Comunicações (ANACOM)	The project focuses on improving incident handling automation for CERTs
19	Spain	National Security Department — Spanish Prime Minister's Office	Request for seminar on NCPs and National Exercises

2.1.4.2 National liaison officer network

In 2014, ENISA regularly communicated with the members of the NLO network, the informal network of all Member States, including Iceland, Liechtenstein and Norway, as well as the Commission and Council. As the NLO members are key actors for the Agency's daily work and interaction, in terms of outreach, effective liaison in the Member States and dissemination, the communication covered time-critical announcements and information on upcoming ENISA project related tenders, requests vacancy notices, and events organised by ENISA or where the Agency contributes to (for example co-organiser, etc.).

An assessment of the NLO section page under the ENISA home page was carried out in an effort to revise this tool of communication between the Agency and the NLOs. New sections were added to this area of the ENISA website, such as the News from the Member States and information on NLO meetings (agenda, presentations, etc.)

A generic presentation about ENISA was distributed to the network in order to aid NLOs in their role of 'facilitators' of ENISA activities in their country.

NLOs actively supported eight (8) ENISA projects in 2014 compared to three (3) in 2013. Their contribution was instrumental in the implementation of the European Cyber-Security Month (ECSM), the Smart Grid security mandates stocktaking and the National Cyber-Security Strategies (NCSS) workshop and working group.

2.1.4.3 Corporate communication, dissemination activities and outreach

Following the Agency's re-organisation in 2013, the communications team now consists of the Spokesperson (or alternate: Corporate Communication Assistant) who collaborates and liaises closely with the Stakeholder Communication Assistant from the Core Operations Department.

Cooperation with media outlets placed emphasis on the EU and Brussels media scene. The result was increased TV coverage, editorials in the press and articles published in numerous media outlets for 2014. Also the communication was tailored towards public relations campaigns for specific events, projects, activities and deliverables. This incorporated digital communications, external communications, media and events across the EU, promoting in a dynamic way the digital revolution and the EU single market.

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

ENISA celebrates 10 years of supporting EU cyber security with a high-profile event on the Future of Cyber Security Challenges

2.1.4.3.1 Celebrating a decade of contribution to the EU's cyber security — High level Event 2014

ENISA celebrated on 1 October its **10-year Agency presence** with **a high-level event** '10 years of securing Europe's cyber security… and beyond!' in Brussels, recapping the achievements of the Agency during these ten years, and looking ahead at the future cyber challenges for Europe. The event also included the official launch of the European Cyber Security Month (ECSM). For the occasion the Agency produced relevant material:

- the 2014 High-level event — ENISA today and in the Future publication, providing an overview of ENISA's work at a policy, operational and EU level
- the ENISA cyber cooperation report looks at a decade of achievement, summarising the threat landscape, the recent developments in EU policy and the regulatory framework.
- EU Digital Security Policy (policy) paper, which looks into the barriers for an alternative model for the EU cyber security industry
- 7 Information Briefs with recommendations on cyber security topics in several EU languages

The event focused on the European Parliament and the new Commission of the next five years, looking ahead at the future cyber challenges for Europe. Topics discussed included:

- Can Cybersecurity be an Economic Enabler?
- Can we Secure Future Technologies?
- Cyber Security in the EU — achievements and future challenges
- Showcasing in a Live Hacking demonstration

2.1.4.3.2 ENISA branding of its 10-year celebration

This year ENISA's **promotional material** reflected its 10-year celebration. The material was distributed at the high-level event, to special events, workshops or conferences, as well as to ENISA visitors and for awareness raising.

Throughout the year an anniversary banner was visual on all Agency corporate material, featuring on the website, the social media outlets, stationary and all materials produced or used. This enhanced putting across the message on cyber security and the Agency's presence in the field. It also enhanced overall **visual identity** and contributed in the effort to trigger perceptions and discussion on cyber security.

2.1.4.3.3 Publications

ENISA is active in publishing the results of its work i.e. reports, studies, info notes and enhancing its communication and reach with various stakeholders. The Agency makes a point of making the Executive Director, the Head of Core Operations and staff members available to communicate and provide their expertise externally to the public. Within this context, a significant number of **interviews, editorials, and feature articles** are provided to key publications and media outlets promoting cyber security and awareness from an official EU and respected source.

In addition, the Agency has published numerous publications with 45 work programme deliverables as well as various ad hoc technical or policy reports, papers and studies or other publications.

2.1.4.3.4 Multilingual approach

A key challenge always remains reaching out to diverse publics. The communications team continues its efforts in providing tailor made, consistent messages, using the appropriate channels. In addition the Agency publishes its press releases in five languages — English, German, French, Spanish and Greek — for its stakeholders and media.

2.1.4.3.5 Media outreach

ENISA's impact, outreach and media programme gives the Agency the opportunity to extend its reach to more stakeholders than through direct means. Following the successful practice of the previous years, through an enhanced media distribution and monitoring process, the Agency enhanced the targeting and reach of its media work. During 2014, major accomplishments include the:

- Production and release of 23 media releases
- Publication of 103 individual news items on the ENISA website

- Simultaneous publication of media releases and news items in ENISA's social media channels (Facebook, Twitter, LinkedIn)

2.1.4.3.6 Cross media impact

ENISA generated 4 346 mentions in EU media compared to 2 500 last year, increasing significantly its reach and impact across the EU's 24 languages. Directly, media releases on the ENISA website received more than 213 000 unique page views in 2014, while individual news stories on the ENISA website received more than 84 000 direct hits. Figures continue to show a clear correlation between peaks in web visitors and the distribution of media releases in multiple channels, thus demonstrating the beneficial effect of the communication and media activity.

Total readership reached 5.4 million in total, with an Internet reach of 3.9 billion for the year.

2.1.4.3.7 Social media

ENISA continues its successful engagement with the online community through its social media outlets. All of ENISA's activities and deliverables are communicated via the social media channels, and generate increasing traffic towards them and the Agency website, activities and deliverables. In addition, they are incorporated in the Agency's communication (publications, presentations, emails, brand material etc.) Furthermore the Agency conducted an external analysis which showed that the channels are updated often, achieving a better impact and reach. In particular, social media monitoring reports have shown an increased reach of ENISA's channels. Main accomplishments include:

- More than 6000 followers in the ENISA Twitter channel
- More than 2800 Tweets from the Agency's account. In total there were 16 625 tweets placing twitter as the Agency's leading social media outlet.
- 3500 Followers in the ENISA LinkedIn page
- 58 videos posted to YouTube
- Hundreds of thousands of users reached by messages posted by ENISA

2.1.4.3.8 Digital media

ENISA's website continues to be the Agency's main communication channel. In 2014, the efforts for improvement were continued and several recommendations from the usability study performed in 2013 were implemented. ENISA's website received more than 3 million unique page views in 2014.

Technical improvements in 2014 included the development of new web tools for the Agency's website and portals (used by specialist expert communities) and the application of all the security patches to the infrastructure used by the ENISA site.

The dedicated portal for the European Cyber Security Month was redesigned and enhanced with new functionalities to better support the ECSM initiative and its constantly growing community.

Furthermore, the structure of the Agency's three mini sites in Greek, German and French was further enhanced in 2014 in a constant effort for improvement. The structure has become more user friendly and news in these three languages is presented and read with much less effort.

ENISA created around 46 videos and clips communicating its events and activities. Indicatively we mention the CE2014 official video clip, CE2014 official launch, the ENISA high-level event and ECSM launch, the Annual Privacy Forum 2014, and the Secure Cloud 2014. Videos are of increasing interest to various stakeholder groups and the Agency envisages the production of more and relevant material for a number of its activities, helping its messages to be communicated in a more interactive manner.

2.1.4.3.9 Additional outreach activities

ENISA continued actively its participation to **events** increasing visibility, involvement, recognition and awareness at a local, national or EU level.

Increased coverage was generated regarding ENISA's threat landscape report, CERT training, National Cyber Security strategies, Cyber Europe 2014 (CE2014), one of the Agency's flagship initiatives, and the Cloud Certification Schemes Metaframework, mapping security requirements, with its first client being the EU Commission. CE2014 was the biggest pan-European cyber exercise to date, bringing together over 50 senior representatives from 23 European Union and EFTA countries, with over 600 actors across Europe.

A particular interest was taken in bringing the Agency and the EU closer to the local community which was reflected through the participation in the **Model European Union (MEU) Creta 2014,** between 22-26 October 2014 in Heraklion Crete; a handover ceremony for the **donation of electronic equipment** in December 2014; and an event with the regional government celebrating ENISA's 10-year presence in Crete. In the beginning of the year, the former EU Vice President and Commissioner for the Digital Agenda Neelie Kroes, visited the ENISA premises in Athens. The European Cyber Security Month (ECSM) and Europe Day are two other EU activities ENISA is actively involved in, encouraging and promoting the local community participation.

The Communications team continues its close collaboration with the NIS experts supporting the production of the **Info Notes** activity where short expert reports provide a pragmatic analysis on trending security issues and themes. The activity has proven to be an important tool which stakeholders turn to for reliable information on security issues. Themes included the 'Heartbleed" ([6]) vulnerability and the BASH Shellshock Bug ([7]).

A new section '**News from the Member States'**, was added to our webpage, following a request of the community. This section covers the latest technical cyber security updates from the EU Member States and is aimed to increase interaction with the specific community.

2.1.4.4 Quality management system

In 2014, the Agency continued developing its quality management system (QMS) responding to a mix of regulatory, compliance and stakeholder requirements. The QMS comprises of a set of standard operating procedures (SOPs) and other guidance instruments that address critical business areas. A dedicated methodology supports the generic promulgation of operational procedures of the Agency based on the Deming cycle; this methodology allows for the setting of SMART goals and KPIs in line with standardisation requirements in quality management.

In 2014, a set of tools and applications were launched to improve operational performance most notably in the area of project management; consequently a project management methodology and a project office facility were made available to increase operational efficiency and productivity, while a project management tool was further developed to improve its fitness for purpose.

[6] ENISA Flash NB: Heartbleed — A wake-up call, April 2014, available at: http://www.enisa.europa.eu/publications/flash-notes/flash-note-heartbleed-a-wake-up-call/at_download/fullReport

[7] ENISA Flash NB: The BASH Shellshock Bug, September 2014, available at: http://www.enisa.europa.eu/publications/flash-notes/flash-note-the-bash-shellshock-bug/at_download/fullReport

3

Management of resources

3.1 Management Board

The agency is governed by the Management Board (MB), composed of one representative from each Member State and two representatives from the European Commission. EEA countries are presented as observers to the MB. In line with Regulation (EU) No 526/2013, the MB held its ordinary meeting in October 2014. At this meeting, the MB adopted a number of administrative, budgetary and management decisions. For example, the amendments to the work programme 2014 were adopted to reflect the recent adoption of the Regulation on electronic identification and trust services (Regulation (EU) No 910/2014) and still ongoing legislative procedure to adopt the NIS Directive (COM(2013)48 Final).

The adoption of the ENISA anti-fraud strategy was among the decisions taken. Minutes and decisions of the MB are available on the ENISA website: http://www.enisa.europa.eu/about-enisa/structure-organization/management-board.

In addition, the MB Chair called for an extraordinary meeting on the extension of the term of office of the Executive Director. The Board decided to extend the term of office for 5 years.

3.2 Major events

During 2014, there were no major events to significantly impact ENISA activities and delivery against its work programme.

3.3 Management of financial resources

3.3.1 Budget execution of EU subsidy (C1 funds)

In terms of budget execution, the expenditure appropriations corresponding to the Union contribution allocated to ENISA and the interest generated by cash at banks during 2014, i.e. the budget of ENISA of 9 091 917.98 EUR, were committed at a rate of 100.00 % on 31.12.2014 compared to 99.72 % on 31.12.2013.

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

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

The respective payment rate on EU subsidy expenditure appropriations as included in the MFF 2014-2020 was 85.61 % in 2014 compared to 91.32 % in 2013. The payment rate of 2014 is slightly lower than 2013. However, the ratio of payment is high and demonstrates that the capacity of the Agency to finalise its annual activities and to execute the relevant payments within the year of reference was maintained. The procurement planning which was moved forward to the end of the preceding year (2013) and enabled the launch of projects related to the work programme in early 2014, contributed significantly to the improvement of the payment rate of appropriations of the year (C1).

3.3.2 Budget execution of additional funds received in 2013 for Athens office refurbishment works (C3 appropriations)

In addition to the initial EU subsidy to its budget 2013, in November 2013 ENISA was granted the amount of 480 632.00 EUR, which resulted in the funds carried over to 2014 for commitment (non-automatic carry over). The total amount of 504 934.00 EUR – related to the refurbishment works and infrastructure investments in the new office in Marousi, Athens – was carried over to 2014 by Decision MB/2014/02 WP of the Management Board adopted on 7 February 2014.

Following a call for tenders for the refurbishment works, which concluded to the award of a contract, and the signature of another contract for upgrading Internet connectivity infrastructure (Dark Fibre), ENISA finally committed 503 834.00 EUR, and the total amount of budget 2013 which remained uncommitted (and was therefore cancelled) was 1 100.00 EUR, representing 0.01 % of the total budget 2013 [8].

The tables below demonstrate a detailed analysis of the commitments and payments made in 2014, including the appropriations carried over from 2013 by decision of the Management Board for the refurbishment works.

[8] Budget commitment validated and contract awarded for the refurbishment project for 478.900 EUR on 17/03/2014. Budget commitment validated and contract awarded for upgraded Internet connectivity (Dark Fibre) for 24.934 EUR on 07/03/2014. Total amount committed in 2014 on amounts carried over from 2013, based on MB decision: 503.834 EUR.

3.3.3 Amending budgets/budgetary Transfers

The following table summarises the budget transfers and the amending budget (AB) 1/2014 effect on the initial budget 2014:

Table — Summary of transfers and AB 1/2014 effect:

	Initial budget	Transfers 1-3 B2014 approved by ED	Amending budget 1/2014 transfers	New appropriations 2014 (AB 01/2014)
Title 1	5 947 226.00	0.00	– 896.00	5 946 330.00
Title 2	875 000.00	0.00	670 000.00	1 545 000.00
Title 3	2 264 128.00	0.00	0.00	2 264 128.00
Total	**9 086 354.00**	**0.00**	**669 104.00**	**9 755 458.00**

The table below summarises the budget transfers and the amending budget (AB) 2/2014 effect:

Table — Summary of transfers and AB 2/2014 effect:

	New appropriations 2014 (AB 01/2014)	Transfers 4-7 B2014 approved by ED	Correction of allocation of new revenue appropriations (AB 02/2014)	Amending budget 2/2014 Transfers	New appropriations 2014 (AB 02/2014)
Title 1	5 946 330.00	– 209 836.61	0.00	– 218 518.53	5 517 973.86
Title 2	1 545 000.00	110 700.00	– 47 161.34	204 856.63	1 813 395.29
Title 3	2 264 128.00	99 136.61	0.00	13 662.90	2 376 927.51
Total	**9 755 458.00**	**0.00**	**– 47 161.34**	**0.00**	**9 708 296.66**

The table below summarises the effect of the budget transfers following the adoption of the AB 02/2014 to the final budget execution:

Table — Summary of transfers' effect on final budget execution:

	New appropriations 2014 (AB 02/2014)	Transfers 8-12 B2014 approved by ED	Final budget e xecution 2014
Title 1	5 517 973.86	43 102.60	5 561 076.4600
Title 2	1 813 395.29	48 407.99	1 861 803.28
Title 3	2 376 927.51	– 91 510.59	2 285 416.92
Total	**9 708 296.66**	**0.00**	**9 708 296.66**

3.3.4 Carry forward of commitment appropriations

The commitment appropriations corresponding to the EU subsidy (C1 appropriations), which were not consumed by payments at the end of 2014, were carried forward (automatic carry forward) to 2015 (C8 appropriations).

All commitment appropriations corresponding to the subsidy from the Greek Government for the lease of ENISA premises in Greece (external assigned revenue — R0 appropriations) were paid by 31 December 2014, therefore no commitment appropriations were automatically carried over to 2015 (R0 appropriations).

The commitment appropriations corresponding to the carried over amount from 2013 by a decision of the Management Board (non-automatic carry-over to C3 appropriations 2014) which were not paid by 31 December 2014, i.e. the amount of 23 945.00 EUR payable to the contractor that was withheld as performance guarantee, is automatically carried forward to 2015 (C8 appropriations 2015).

The funds carried forward to 2015 (C8 appropriations) are detailed below:

Title	Carried forward (to C8 2015) EU subsidy	Carried forward (C3 2014 to C8 2015) EU subsidy	Total carried forward to 2015 EU subsidy
Title 1 — Staff	394 950.16	0.00	384 950.16
Title 2 — Administration	589 036.04	23 945.00	612 981.04
Title 3 — Operations	334 489.60	0.00	334 489.60
Total	**1 308 475.80**	**23 945.00**	**1 332 420.80**

The total cancelled appropriations carried forward from 2013 to 2014 (C8 appropriations of 2014) but finally not paid in 2014, was 49 460.01 EUR (representing 6.89 % of the total appropriations carried forward to 2014).

3.3.5 Types of procurement procedures

In 2014, a total of 29 procurement procedures were launched, 42 contracts (18 framework service contracts and 25 service contracts) and 236 purchase orders (95 of which were issued against pre-existing framework service contracts) were signed.

3.3.6 Interest charged by suppliers

During 2014, the Agency had to pay no interest to its suppliers as result of keeping the payment terms agreed with the suppliers.

3.4 Management of human resources

3.4.1 Human resources

At the end of 2014, 62 statutory staff were employed in the Agency. During 2014, three staff left the Agency, ten vacancy notices were published and seven staff were recruited.

ENISA still experiences challenges in attracting and holding suitably qualified staff to support the activities of the Agency. This is a challenge due to several factors, however one prime factor is the location, Heraklion, where international education is a challenging factor.

In relation to the schooling for ENISA staff members:

- a service-level agreement has been concluded with each of the private schools being used by the children of the staff in Athens as there are no European schools based there.

- A new mandate and service agreement has been concluded between the Commission and ENISA which provides the detail of the funding for European schools being used by the children of the staff of ENISA.

In 2014, 20 implementing rules prepared by the Commission were considered by ENISA and sent to the Management Board for approval. These approved implementing rules provide clarification and detail on the application of the staff regulations, which provide the legal basis for the obligations and rights of staff members.

In 2014, ENISA also engaged consultants to complete a staff survey to report on aspects of living and working at ENISA. The results were compared with a previous staff survey carried out in 2012; significant improvements verified as to past results have been noted. The results of the latest survey are being analysed with a view to learning and improving the quality of the lives of staff at ENISA.

A number of activities with staff were held throughout the year to improve team building and the working environment. These exercise proved to be well received by the staff and helps to bridge the barrier created from the operation of two offices in a small agency.

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

3.4.2 Results of screening

The Agency performed a job screening benchmarking exercise for the first time in 2014. The result of the exercise, which is a snap shot of the staffing situation on end December 2014, appears in Annex A.4. For 2014 there are no comparative data related to the previous year. The 'overhead', support functions, is only 22 % of the total population, which is below the maximum value accepted for the Agencies that is estimated at 25 %.

3.5 Assessment by management

3.5.1 Effectiveness of controls for 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 and the nature of the payments concerned. In order to achieve the best control possible, the Agency has focused intensively on the verification of results before transactions are initiated ('*ex-ante* verification').

In line with Internal Control Standard 8 (ICS 8 Processes and Procedures), the Agency has done the *ex-post* control report of the 2013 financial year. The recommendations issued in the report were addressed during the year.

The *ex-post* controls of the financial year 2013 were quite extensive. A total of 224 financial transactions were sampled and controlled representing 16,27 % of all financial transactions of the Agency and representing 70.29 % of the 2013 Agency's budget.

The *ex-post* controls of the financial year 2014 followed procedures set in previous years. A total of 174 financial transactions were sampled and controlled representing 9.22 % of all financial transactions of the Agency or 70.99 % of the 2014 Agency's budget. As a result, one recommendation was issued in regard to the *a posteriori* commitments of the Agency – the late opening of the financial tool ABAC at the beginning of the year.

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

3.6 Budget implementation tasks entrusted to other services and entities

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

3.7 Assessment of audit results and follow up of audit recommendations

3.7.1 Internal Audit Services (IAS)

At the beginning of 2014, the Agency had 25 open recommendations. During the year, the Agency closed 24 of them. In November 2014, the IAS visited the Agency in order to proceed with a control 'on the spot' to close the remaining open recommendations. After their visit, the Agency remains with only one open recommendation. This open recommendation will be closed as soon as the Agency implements a tool for e-workflows (implementation in January 2015). The Agency has an internal control coordinator's team.

3.7.2 European Court of Auditors (ECA)

The annual report of ECA for 2012 ENISA contained two important recommendations. The Court noted a weakness in the documentation of the fixed assets and a delay in performance of a physical inventory count.

The first recommendation concerning the weakness in the documentation of the fixed assets was closed by the ECA. A lot of effort was put into the management of fixed assets. A full physical inventory was done across both premises (Heraklion and Athens), the retirement exercise was done and the reconciliation of fixed assets with the accounts was finalised.

The second recommendation concerning the physical inventory is a process that is still ongoing. Indeed, the declassification exercise was done in 2014 as well as the donation exercise. The process regarding the disposal of the remaining declassified items, by way of destruction and auction, will be completed by the end of the first semester of 2015.

The ECA's report on 2014 accounts is expected in the third quarter of 2015. The Agency expects that the Court's opinion on the true and fair presentation of the accounts as well as on the legality and regularity of the transactions underlying the accounts will be unqualified as it has been for the past eight years.

3.7.3 Follow up of audits plans, audits and recommendations.

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

This recommendation will be closed in the beginning of 2015, as soon as the Agency will implement an e-workflow tool (implementation in January 2015).

3.7.4 Follow up of observations from the discharge authority.

Regarding the European Parliament decision of 3 April 2014, the Executive Director of the Agency was granted the discharge in respect of the implementation of the Agency's budget for the financial year 2012.

Regarding the European Parliament decision of 3 April 2014, the closure of the accounts of the Agency for the financial year 2012 was approved.

3.7.4.1 Follow-up of the 2011 discharge

The discharge authority acknowledged that the reduction in the level of appropriations carried forward to the next year was achieved by shifting procurement planning from the first quarter of the financial year to the last quarter of the preceding year.

The discharge authority acknowledged that the first Agency's inventory count was launched in April 2013 using ABAC assets application and technology, whereby the Agency verified the existence, valuation, eligibility and correctness of fixed asset records.

The discharge authority acknowledged that the necessary measures were taken to address the lack of transparency of recruitment procedures and that the Court of Auditors marked the issue as completed in its report.

3.7.4.2 Budget and financial management

The discharge authority noted with satisfaction that the effective implemented budget control system during the financial year 2012 resulted in a budget implementation rate of 100 % and that the payment appropriations execution rate was 91.45 %.

3.7.4.3 Commitments and carry overs

The discharge authority acknowledged that the Court of Auditors' annual audit had found no notable issues as regards the level of carry overs in 2012 and commended the Agency for adhering to the principle of annularity and for timely execution of its budget.

3.7.4.4 Transfers

The discharge authority noted with satisfaction that according to the annual activity report, as well as the Court of Auditors' audit findings, the level and nature of transfers in 2012 had remained within the limits of the financial rules and commended the Agency on its good budgetary planning.

3.7.4.5 Procurement and recruitment procedures

The discharge authority noted that for the year 2012, neither sampled transactions nor other audit findings had led to any comments on the Agency's procurement procedures in the Court of Auditors' annual audit report and noted that the Court of Auditors had made no comments in its annual audit report for 2012 with regard to the Agency's recruitment procedures.

3.7.4.6 Prevention and management of conflicts of interests and transparency

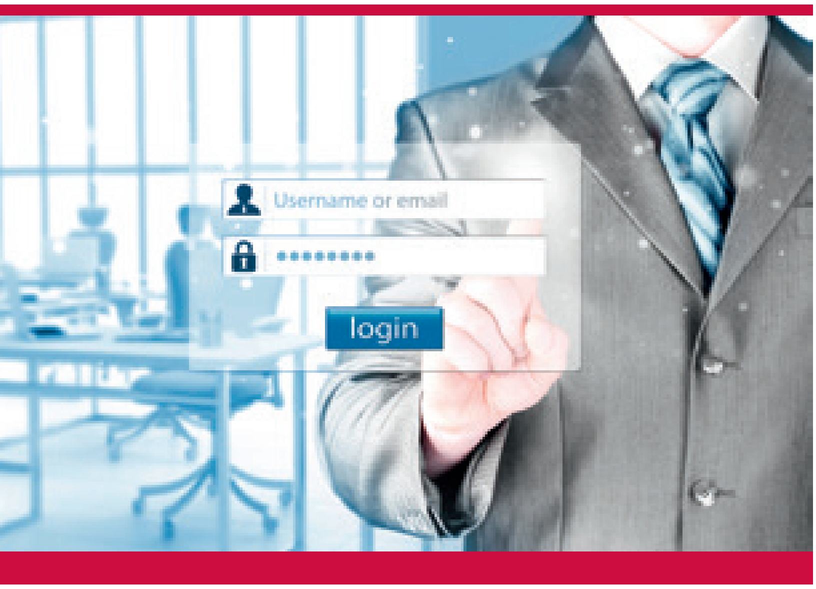
The discharge authority acknowledged that the Management Board approved and signed the decision on practical arrangements for implementing transparency and confidentiality rules in October 2013 and acknowledged from the Agency that CVs, declarations of interest of the Executive Director, the directors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

3.7.4.7 Comments on internal controls

The discharge authority noted with concern that according to the Court of Auditors' annual audit report, although the financial regulation and the corresponding implementing rules provide for a physical inventory of fixed assets at least every three years, this was not respected and the Agency did not carry out a comprehensive physical inventory in 2012, following the physical inventory of 2009; acknowledged that it would have been either very difficult or even counterproductive to carry out an inventory in 2012 because the inventory management module of the integrated budget and accounting platform, supported by the Commission (DG BUDG), has only been in place since that same year; it acknowledged that this issue had been addressed with the new system in 2013.

3.7.4.8 Internal audit

In 2012, the Commission's Internal Audit Service (IAS) carried out an in-depth risk assessment exercise in order to determine the audit priorities for the coming three years; observes that the IAS submitted its final strategic audit plan for 2013-2015 on 3 December 2012, defining the prospective topics for the IAS audits of the Agency for this period; notes that the IAS also carried out a desk review on information provided by the Agency, which showed that no critical recommendations were open as of 31 December 2012; notes with concern, however, that the implementation of four very important recommendations was delayed, with respect to the deadlines defined by the Agency in the original action plans; notes that two of those recommendations are actually closed.



3.7.4.9 Performance

The discharge authority requested the Agency to communicate the results and impact of its work on European citizens in an accessible way, mainly through its website.

The Agency is continually striving to improve the way in which it interacts with its stakeholder communities. Most of the Agency's work is aimed at professional audiences in both the private and public sector, which is where we place the emphasis on our stakeholder engagement strategy. However, we realise the need to keep the EU citizen informed about our work and we have therefore recently broadened our communications approach to include social media (notably Facebook and Twitter) whilst also improving our presence in the national and international press. The initial results are encouraging. As mentioned in Section 2.1.4.3 where more details on communication are given, ENISA generated 4 346 mentions during 2014 in EU media, which is higher than the outreach of 2013.. At the same time the number of website visits increased (please refer to Section 2.1.4.3 for detailed data). The presence of the Agency on social media is increasing, with the number of participants on Facebook and Twitter doubling in the last year.

The Agency also makes good use of classical communication tools. The annual report provides an extensive reference to the achievements and the concrete impact of Agency activities for any given year. The report shows that the activities of ENISA aim at enhancing the security infrastructure, regulations and culture of the Member States and the NIS community and indirectly affect the citizen's life. ENISA has launched an internal consultation process to identify the optimal form of report on the impact of its work to the EU citizen level.

4

Assessment of the effectiveness of the internal control systems

4.1 Risk management

The Agency is actually using the risk assessment done by the Internal Audit Service in 2012.

A revision of the risk management will be done during 2015.

In terms of fraud prevention and detection, the Management Board adopted the Agency's anti-fraud strategy and action plan in 2014.

4.2 Compliance and effectiveness of internal control standards

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

Compliance with these standards is compulsory for financial management.

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

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

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

4.2.1 Mission (ICS 1)

The Agency's mission and scope is described in the ENISA Regulation. Mission statements for departments and units were established based on the evolution of the organisation in 2014. The roles and tasks of each department and unit are clearly defined.

4.2.2 Ethical and organisational values (ICS 2)

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

4.2.3 Staff allocation and mobility (ICS 3)

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

4.2.4 Staff evaluation and development (ICS 4)

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

4.2.5 Objectives and performance indicators (ICS 5)

The work programme and budget preparation procedures were developed in 2009 and revised in 2014. The annual work programme (WP) of the Agency is developed by the Agency services, with continuous input and guidance from its two governing bodies, the Management Board and the permanent stakeholders group. The WP clearly sets out how the planned activities at each management level contribute to the achievement of objectives, taking into account the resources allocated and the risks identified. The WP objectives are established on SMART (specific, measureable, achievable, relevant, time-bound) criteria and are updated during the year in order to address significant changes in priorities and activities.

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

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

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

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

Finally, the Agency managed again to optimise the budget execution for 5 consecutive years. The commitment rate of budget appropriations available for the year 2014 (C1) reached 100 %, another consecutive year in which the total Agency budget was consumed.

4.2.6 Risk management process (ICS 6)

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

4.2.7 Operational structure (ICS 7)

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

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

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.

4.2.8 Processes and procedures (ICS 8)

Several policies were developed to strengthen the Processes and Procedures Internal Control Standard. The Agency created a policy on financial circuits. The roles and responsibilities of financial actors are described in this policy as well as existing workflows.

A code of professional conduct for *ex-ante* financial verification was developed. This document emphasises the role and responsibilities of the Financial Verifying Agent.

The Agency proceeded in 2014 with the full 2013 *ex-post* control exercise and will deliver the 2014 *ex-post* control report in the first quarter of 2015.

Importantly in 2014, a quality management system was implemented strengthening the performance management of the Agency.

4.2.9 Management supervision (ICS 9)

Management at all levels supervises the activities for which they are responsible and tracks the main issues identified. The Management Team, which comprises the Executive Director and the heads of departments and units, meets weekly and sets priorities for the actions to be taken in order to achieve the short- and 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.

4.2.10 Business continuity (ICS 10)

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

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

4.2.11 Document management (ICS 11)

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

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

4.2.12 Information and communication (ICS 12)

Internal communication measures and practices are in place for sharing information and monitoring activities. These include regular management team meetings during which issues relevant to performance, audit results and financial information are discussed, and actions are decided upon and assigned. Regular financial reporting is available to all staff on ENISA's intranet. All engagements in new projects are discussed during the implementation of the annual work programme and decisions are documented and communicated.

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

The weekly Staff Meeting is used as platform of communication between all departments. Every week, staff members can share their work with the rest of the Agency.

4.2.13 Accounting and financial reporting (ICS 13)

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

4.2.14 Evaluation of activities (ICS 14)

Key performance indicators are used in order to measure the performance and assess the impact of the Agency's projects as provided for in its Annual work programmes.

The General Report and the Annual Activity Report are the tools used by the Agency to report on performance and impact. The feedback of relevant stakeholders is taken into account.

4.2.15 Assessment of internal control systems (ICS 15)

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

4.2.16 Internal audit capability (ICS 16)

The head of the Administration and Support Department assumes the internal control coordination (ICC) function. He is responsible for implementing internal control systems in the Agency and liaising with the IAS of the European Commission. As the Agency lacks human resources, the role of Internal

Audit Capability (IAC) cannot be performed. Since 2005, the Agency has relied on the IAS to carry out internal audits. The IAS plays a key role in auditing bodies of the European Union.

Internal control tasks performed in ENISA include 100 % of *ex-ante* verifications, annual *ex-post* controls, hierarchical controls and outsourced engagements, coordinated by the ICC.

In line with the Strategic Audit Plan 2013-2015, the Internal Audit Service (IAS) carried out in 2014 a control 'on the spot'. Out of 25 open recommendations in 2014, there is only one left open, which will be closed early 2015. The role of ICC was reinforced in order to comply with all the recommendations issued by the IAS and ECA.

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

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

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, subcategories and business risks applicable at the organisational level, for ENISA as a whole. It includes:

- Risk categories and subcategories
- Risks specific to each category (business risks)
- Risk definition

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 pan.	Number of staff hired to cover new posts or make up for resignations.
7	Internal ICT networks and systems	Secure ICT networks and systems in place.	Results of external security assessment/ audit.
8	Public procurement	Regular, consistent observation of public procurement practices and appropriate assistance provided to all departments.	Clear mandate of the procurement function established, staff informed, forms available, number and type of procurement processes handled, files of procurement processes organised, and files for audit available. List of number of purchase orders per supplier, number of complaints processed.
9	Contract management	General support on contract management.	Number of contracts prepared and signed by the Agency, number of requests for support received from departments, number of claims processed.
10	*Ex-ante* controls	Well developed at procedural, operational and financial levels.	Number of transactions as compared to number of erroneous transactions.
11	*Ex-post* controls	Well developed and done on an annual basis	Number of transactions as compared to number of erroneous transactions.

5.2 Exceptions

In 2014, the Agency recorded 18 exceptions. Only four are with high materiality. For three of these cases, the root of the problem was the late opening of the financial tool ABAC and one case is with regard to the payment of the rent to the Greek authorities of the Athens building (delay in receiving the funds from the Greek authorities to pay the rent led to an *'a posteriori'* commitment).

The information reported in Parts 2 and 3 stems from the results of auditing by management and auditors. The results are contained in the reports listed. These reports result from a systematic analysis of the evidence available. This approach provides sufficient guarantees on the completeness and reliability of the information reported, and results in complete coverage of the budget delegated to the Executive Director of ENISA.

6

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 ([9]).

State that I have reasonable assurance that the resources assigned to the activities described in this report have been used for their intended purpose and in accordance with the principles of sound financial management, and that the control procedures put in place give the necessary guarantees concerning the legality and regularity of the underlying transactions.

This reasonable assurance is based on my own judgement and on the information at my disposal, such as the results of the self-assessment, ex-post controls, the work of the internal audit capability, the observations of the Internal Audit Service and the lessons learnt from the reports of the Court of Auditors for years prior to the year of this declaration.

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

Heraklion, 08.06.2015

[signed]

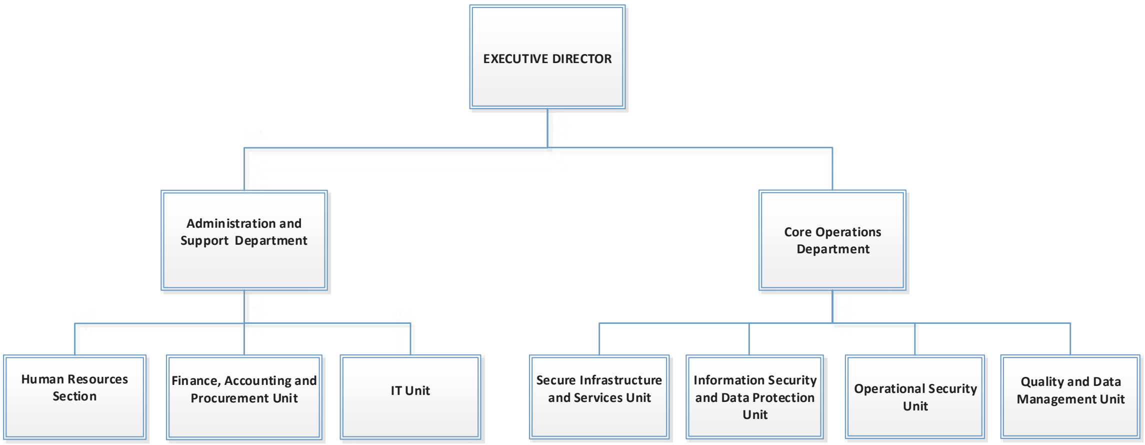
Udo Helmbrecht
Executive Director

([9]) True and fair in this context means a reliable, complete and correct view on the state of affairs in the service.

Annexes

A. Human resources

A.1. Organisational chart


EXECUTIVE DIRECTOR
Administration and Support Department
Core Operations Department
Human Resources Section
Finance, Accounting and Procurement Unit
IT Unit
Secure Infrastructure and Services Unit
Information Security and Data Protection Unit
Operational Security Unit
Quality and Data Management Unit

A.2. Establishment plan 2014

Function group and grade (TA/AST)	Posts	
	2014	
	Authorised under the Union budget	
	Permanent	Temporary
AD 16		
AD 15		1
AD 14		
AD 13		
AD 12		3
AD 11		
AD 10		5
AD 9		9
AD 8		7
AD 7		6
AD 6		
AD 5		3
AD Total:		34
AST 11		
AST 10		
AST 9		
AST 8		
AST 7		
AST 6		2
AST 5		6
AST 4		1
AST 3		2
AST 2		3
AST 1		
AST Total:		14
Grand Total:		48
Total Staff:		48

A3. Information on entry level for each post type

Job title	Type of contract (Official, TA or CA)	Indication whether the function is dedicated to administrative support or operation
Executive Director	TA	Operation
Head of Administration and Support Department	TA	Administrative
Head of Core Operations Department	TA	Operation
Head of Finance, Accounting and Procurement Unit	TA	Neutral
Head of Information and Technology Unit	TA	Administrative
Head of Information Security and Data Protection Unit	TA	Operation
Head of Operational Security Unit	TA	Operation
Head of Secure Infrastructure and Services	TA	Operation
Head of Quality and Data Management	TA	Operation
Expert in Network and Information Security	TA	Operation
Expert in Network and Information Security	TA	Operation
Expert in Network and Information Security	TA	Operation
Expert in Network and Information Security	TA	Operation
Expert in Network and Information Security	TA	Operation
Expert in Network and Information Security	TA	Operation
Expert in Network and Information Security	TA	Operation
Expert in Network and Information Security	TA	Operation
Expert in Network and Information Security	TA	Operation
Expert in Network and Information Security	TA	Operation
Expert in Network and Information Security	TA	Operation
Expert in Network and Information Security	CA	Operation
Expert in Network and Information Security	CA	Operation
Expert in Network and Information Security	CA	Operation
Expert in Network and Information Security	CA	Operation
Expert in Network and Information Security	CA	Operation
Expert in Network and Information Security	CA	Operation
Expert in Network and Information Security	CA	Operation
Expert in Network and Information Security	CA	Operation
Expert in Network and Information Security	TA	Operation
Expert in Network and Information Security	TA	Operation
Expert in Network and Information Security	TA	Operation
Network and Information Security — Research and Analysis Expert	TA	Operation
Network and Information Security — Research and Analysis Expert	TA	Operation
Network and Information Security — Research and Analysis Expert	TA	Operation
ICT Solutions Architect Expert	TA	Operation
Expert in Security Tools and Architecture	TA	Operation
Expert in Security Tools and Architecture	TA	Operation
Senior ICT Systems Officer	TA	Administrative
Senior Procurement Officer	TA	Neutral
Senior Safety and Security Officer	TA	Operation
Security and Resilience of Communication Networks Officer	CA	Operation
Security and Resilience of Communication Networks Officer	CA	Operation
ICT Systems Officer	CA	Administrative
Software Developer Officer	CA	Administrative
Legal Officer	TA	Coordination
Corporate Communications Officer and Spokesperson	TA	Coordination
Administrative Officer to the Management Board	TA	Operation
Senior Financial Assistant	TA	Neutral
Financial Assistant	TA	Neutral
Financial Assistant	CA	Neutral

Job title	Type of contract (Official, TA or CA)	Indication whether the function is dedicated to administrative support or operation
Financial Control Assistant	TA	Administrative
Finance and Procurement Assistant	CA	Neutral
Project Assistant	CA	Operation
NIS Assistant	TA	Operation
HR Assistant	TA	Administrative
HR Assistant	TA	Administrative
HR Assistant	CA	Administrative
Administrative Assistant	TA	Operation
Administrative Assistant	TA	Neutral
Administrative Assistant	TA	Operation
Administrative Assistant to the Core Operations Department	TA	Operation
Administration and Internal Communications Assistant	CA	Coordination
Assistant to the Head of Administration and Support Department	TA	Administrative
Personal Assistant to the Executive Director	TA	Operation
Facilities Management Assistant	CA	Administrative
Corporate Communications Assistant	CA	Operation
IT and Facilities Support Assistant	TA	Administrative

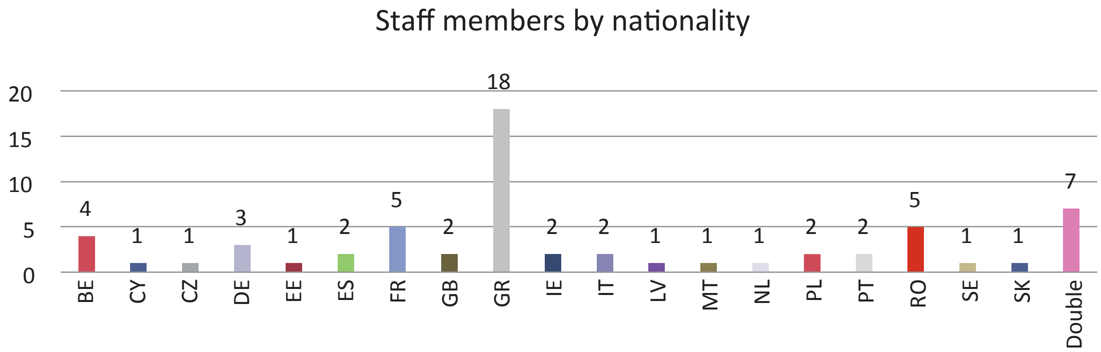
A.4. Information on the benchmarking exercise

Job type	2014
Administrative support and coordination	**22 %**
Administrative support	18 %
Coordination	4 %
Operational	**68 %**
Top operational coordination	5 %
General operational	63 %
Neutral	**10 %**
Finance and control	10 %

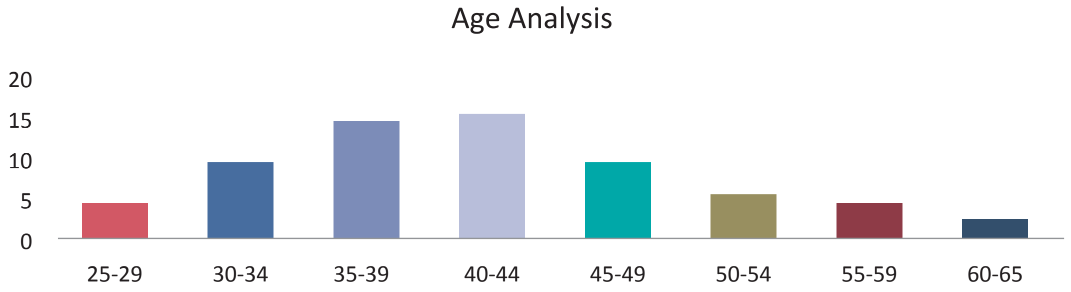
The benchmarking exercise followed the EU Commission methodology. All the values are within the acceptable values for an Agency of ENISA size (i.e. Overhead [administrative support and coordination] is below 25 %)

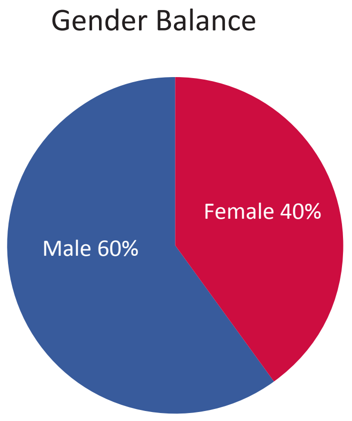
A.5. Human resources statistics

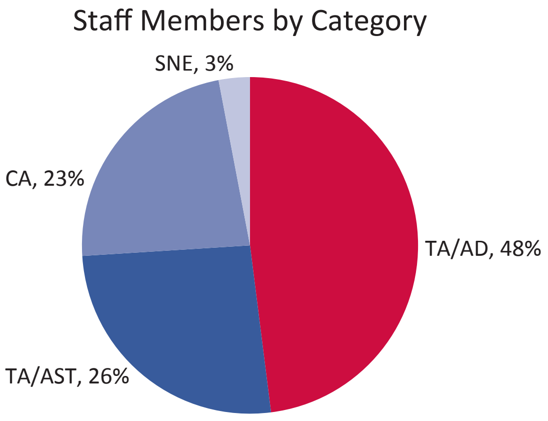
As of 31/12/2014, ENISA counts 62 staff members: 46 TAs (30 ADs and 16 ASTs), 14 CAs and 2 SNEs.



NB: 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.







A.6 Human resources by activity

OPERATIONAL ACTIVITIES 2014	Full-time equivalents (FTEs) staff in operations
WS1 — Support EU policy building	9.3
WS2 — Support capacity building	12.6
WS3 — Support cooperation	14.0
SR — Stakeholder relations	2.0
CC — Corporate communication	2.0
PS — Project support activities	2.0
Total	41.9

Remark: The figures in the table above provide an estimation of the human resources attributed in each of the operational activities of the Agency, according to the work programme 2014.

B. Financial resources

B.1. Provisional annual accounts 2014

Balance sheet 2014 (in EUR)

	2014	2013
NON CURRENT ASSETS	**813 993**	**242 332**
Intangible assets	1 954	1 682
Property, plant and equipment	812 039	240 650
CURRENT ASSETS	**1 652 400**	**2 158 996**
Short-term receivables	270 320	599 939
Cash and cash equivalents	1 382 080	1 559 057
ASSETS	**2 466 393**	**2 401 328**
NON-CURRENT LIABILITIES	**-**	**-**
Provisions (long term)	-	-
CURRENT LIABILITIES	**1 026 144**	**1 196 562**
EC Pre-financing received	105 318	136 715
EC Interest payable	17 323	47 589
Accounts payable	234 179	539 427
Accrued liabilities	469 324	385 331
Short-term provisions	200 000	87 500
LIABILITIES	**1 026 144**	**1 196 562**
NET ASSETS (ASSETS less LIABILITIES)	**1 440 249**	**1 204 767**

Statement of financial performance 2014 (in EUR)

	2014	2013
OPERATING REVENUES	**9 664 900**	**9 684 054**
Revenue from the European Union Subsidy	9 035 189	8 975 136
Other revenue	10 131	6 053
Revenue from administrative operations	619 580	702 866
OPERATING EXPENSES	**– 9 427 471**	**– 8 935 750**
Administrative expenses	– 7 735 138	– 7 434 458
Operational expenses	– 1 579 133	– 1 501 291
Adjustments to provisions	– 112 500	-
OTHER EXPENSES	**– 1 948**	**– 2 432**
Financial expenses	– 1 171	– 1 609
Exchange rate loss	– 777	– 823
ECONOMIC RESULT FOR THE YEAR	**235 481**	**745 872**

Remark: The figures included in the balance sheet and statement of financial performance are provisional since they are, as of the date of the preparation of the annual activity report, still subject to audit by the European Court of Auditors. It is thus possible that amounts included in these tables may have to be adjusted before the final accounts are adopted (deadline 01 July 2015).

B2. Financial Reports 2014

OUTTURN ON COMMITMENT APPROPRIATIONS IN 2014				
Chapter		Commitment appropriations authorised *	Commitments made	%
		1	2	3=2/1
Title A-1 STAFF				
A-11	Staff in active employment	4 152 943.85	4 152 943.85	100.00 %
A-12	Recruitment expenditure	198 135.48	198 135.48	100.00 %
A-13	Socio-medical services and training	193 994.10	193 994.10	100.00 %
A-14	Temporary assistance	982 403.03	982 403.03	100.00 %
Total Title A-1		**5 561 076.46**	**5 561 076.46**	**100.00 %**
Title A-2 FUNCTIONING OF THE AGENCY				
A-20	Buildings and associated costs	1 714 499.64	1 713 399.64	99.94 %
A-21	Movable property and associated costs	31 462.62	31 462.62	100.00 %
A-22	Current administrative expenditure	53 205.89	53 205.89	100.00 %
A-23	Information and communication technologies	878 862.51	878 062.72	99.91 %
Total Title A-2		**2 677 994.66**	**2 676 094.87**	**99.93 %**
Title B-3 OPERATING EXPENDITURE				
B-30	Group activities	798 639.98	798 639.98	100.00 %
B-32	Horizontal operational activities	307 658.14	307 658.14	100.00 %
B-36	Core operational activities	1 179 118.80	1 179 118.80	100.00 %
Total Title B-3		**2 285 416.92**	**2 285 416.92**	**100.00 %**
TOTAL ENSA		**10 524 488.04**	**10 522 588.25**	**99.98 %**

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

OUTTURN ON PAYMENT APPROPRIATIONS IN 2014				
Chapter		Payment appropriations authorised *	Payments made	%
		1	2	3=2/1
Title A-1 STAFF				
A-11	Staff in active employment	4 152 943.85	4 152 943.85	100.00 %
A-12	Recruitment expenditure	256 601.56	226 320.06	88.20 %
A-13	Socio-medical services and training	213 103.80	105 672.15	49.59 %
A-14	Temporary assistance	1 136 928.68	874 395.47	76.91 %
Total Title A-1		**5 759 577.89**	**5 359 331.53**	**93.05 %**
Title A-2 FUNCTIONING OF THE AGENCY				
A-20	Buildings and associated costs	1 771 910.03	1 674 754.56	94.52 %
A-21	Movable property and associated costs	113 646.04	85 648.26	75.36 %
A-22	Current administrative expenditure	55 921.87	53 170.76	95.08 %
A-23	Information and communication technologies	1 052 520.24	552 620.16	52.50 %
Total Title A-2		**2 993 998.18**	**2 366 193.74**	**79.03 %**
Title B-3 OPERATING EXPENDITURE				
B-30	Group activities	903 622.98	718 165.93	79.48 %
B-32	Horizontal operational activities	350 226.19	260 189.87	74.29 %
B-36	Core operational activities	1 234 990.01	1 154 753.58	93.50 %
Total Title B-3		**2 488 839.18**	**2 133 109.38**	**85.70 %**
TOTAL ENSA		**11 242 415.25**	**9 858 634.65**	**87.69 %**

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

BREAKDOWN OF COMMITMENTS TO BE SETTLED AT 31/12/2014					
Chapter			2014 Commitments to be settled		
		Commitments 2014	Payments 2014	RAL 2014	% to be settled
		1	2	3=1-2	4=1-2//1
Title A-1 STAFF					
A-11	Staff in active employment	4 152 943.85	-4 152 943.85	0.00	0.00 %
A-12	Recruitment expenditure	198 135.48	-171 855.94	26 279.54	13.26 %
A-13	Socio-medical services and training	193 994.10	-88 899.10	105 095.00	54.17 %
A-14	Temporary assistance	1 016 003.03	-762 427.41	253 575.62	24.96 %
Total Title A-1		**5 561 076.46**	**-5 176 126.30**	**384 950.16**	**6.92 %**
Title A-2 FUNCTIONING OF THE AGENCY					
A-20	Buildings and associated costs	1 713 399.64	-1 620 360.11	93 039.53	5.43 %
A-21	Movable property and associated costs	31 426.62	-11 037.30	20 389.32	64.88 %
A-22	Current administrative expenditure	53 205.89	-50 454.78	2 751.11	5.17 %
A-23	Information and communication technologies	878 062.72	-381 261.64	496 801.08	56.58 %
Total Title A-2		**2 676 094.87**	**-2 063 113.83**	**612 981.04**	**22.91 %**
Title B-3 OPERATING EXPENDITURE					
B-30	Group activities	798 639.98	-634 359.38	164 280.60	20.57 %
B-32	Horizontal operational activities	307 658.14	-217 685.57	89 972.57	29.24 %
B-36	Core operational activities	1 179 118.80	-1 098 882.37	80 236.43	6.80 %
Total Title B-3		**2 285 416.92**	**-1 950 927.32**	**334 489.60**	**14.64 %**
TOTAL ENSA		**10 522 588.25**	**-9 190 167.45**	**1 332 420.80**	**12.66 %**

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

SITUATION ON REVENUE AND INCOME IN 2014					
Title	Description	Year of origin	Revenue and income recognised	Revenue and income cashed in 2014	Outstanding balance
9000	SUBSIDY FROM THE EU GENERAL BUDGET	2014	9 085 458.00	9 085 458.00	0.00
9200	OTHER CONTRIBUTIONS	2013	299 934.60	299 934.60	0.00
9200	OTHER CONTRIBUTIONS	2014	616 378.68	616 378.68	0.00
9300	REVENUE FROM ADMINISTRATIVE OPERATIONS	2014	6 459.98	6 459.98	0.00
TOTAL ENSA			**10 008 231.26**	**10 008 231.26**	**0.00**

Average payment time for 2014							
Average payment time for 2014	Total number of payments	Within time limit	Percentage	Average payment time	Late payment	Percentage	Average payment time
21,34	1808	1440	79.65 %	13.00	368	20.35 %	53.94

C. Materiality criteria

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

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

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

D. Internal control templates for budget implementation (ICT)

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) and that the decision to procure was inappropriate to meet the operational objectives. Interruption or delay of the services provided due to a late contracting (poor planning and organisation of the procurement process).	Publication of intended procurements/Work programme Validation by AO(S)D of justification (economic, operation) for launching a procurement process Decisions discussed/taken at management team meeting	100 % of the forecast procurements (open procedures published in OJEU and website) are justified in a note addressed to the AO(D) 100 % of the forecast procurements All key procurement procedures (> amounts and/or having significant impact on the objectives of the Agency) are discussed at management meeting	**Costs**: estimation of cost of staff involved and the related contract values (if external expertise is used). **Benefits**: Amount of rejections of unjustified purchases. Estimation of litigation avoided and eventual discontinuation of the service provided.	**Effectiveness**: Number of projected tenders cancelled, Number of contracts discontinued or underutilised due to poor planning. **Efficiency**: For consultancy-based tenders for operations; average person day cost per tender.

B — Needs assessment and definition of needs

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

Main risks *It may happen (again) that…*	Mitigating controls	How to determine coverage frequency and depth	How to estimate the costs and benefits of controls	Possible control indicators
The best offer/s are not DG if it goes wrong submitted due to the poor definition of the tender specifications	AOSD supervision and approval of specifications	100 % of the specifications are scrutinised. **Depth** may be determined by the amount and/or the impact on the objectives of the Agency	**Costs**: estimation of cost of staff involved and the related contract values (if external expertise is used). **Benefits**: limit the risk of litigation, limit the risk of cancellation of a tender. Amount of contracts for which the approval and supervisory control detected material error.	**Effectiveness:** 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 and 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 conflict of interests	100 % of the members of the opening committee and the evaluation committee	**Costs**: estimation of cost of staff involved. **Benefits**: Amount of contracts for which the control prevented the risk of litigation or fraud.	
	Exclusion criteria documented	100 % checked. **Depth**: required documents provided are consistent	**Costs**: estimation of cost of staff involved. **Benefits**: Avoid contracting with excluded economic operators	
	Standstill period, opportunity for unsuccessful tenderers to put forward their concerns on the decision.	100 % when conditions are fulfilled	**Costs**: estimation of cost of staff involved. **Benefits**: Amount of procurements successfully challenged during standstill period.	

Stage 2 — Financial transactions

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

Main risks *It may happen (again) that…*	Mitigating controls	How to determine coverage frequency and depth	How to estimate the costs and benefits of controls	Possible control indicators
The products/services/works foreseen are not, totally or partially, provided in accordance with the technical description and requirements foreseen in the contract and/or the amounts paid exceed that due in accordance with the applicable contractual and regulatory provisions. Business discontinues because contractor fails to deliver	Operational and financial checks in accordance with the financial circuits. Operation authorisation by the AO For riskier operations, *ex-ante* in-depth verification. For high-risk operations, reinforced monitoring on deliverables timing. Management of sensitive functions	100 % of the contracts are controlled, including only value-adding checks. Riskier operations subject to in-depth controls. The depth depends on risk criteria. High-risk operations identified by risk criteria. Amount and potential impact on the Agency operations of late or no delivery	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).

E. The permanent stakeholders' group, term of office 2012-2015

Nominated members

Authority	Nominated representative	Alternate
Art. 29 Working Party	**Mr Alexander Dix,** Berlin DPA	
Body of European Regulators for Electronic Communications (BEREC)	**The Chairperson of the BEREC**	To be nominated on the ad hoc basis
Europol	**Mr Olivier Burgersdijk,** Head of Strategy of the European Cybercrime Centre (EC3) at Europol	**Mr Benoit Godart,** EC3

Experts appointed '*ad personam*'

Name		Job Title	Sector
Markus	Bautsch	Deputy Head of Department	Consumers
Constance	Bommelaer	Director	Users
Martin	Boyle	Senior Policy Advisor	Industry
Ilias	Chantzos	Director of Government Relations	Industry
Raoul	Chiesa	Principal	Industry
Nick	Coleman	Global Cloud Security Leader	Industry
Andrew	Cormack	Chief Security Adviser	Users
Gianluca	D'Antonio	CISO	Users
Harald	Deppeler	Information Security Manager	Industry
Christos	Dimitriadis	Head of Information Security	Users
Serge	Droz	Head of SWITCH Security	Industry
Stefan	Fenz	Senior Researcher	Academia
Patrick	Froyen	Senior IT Expert	Users
Denis	Gardin	Senior Vice president	Industry

Name		Job Title	Sector
Corrado	Giustozzi	lecturer	Academia
Marcos	Gómez-Hidalgo	Security/e-Trust Deputy Manager	Users
Janusz	Gorski	Professor of Software Engineering	Academia
François	Gratiolet	CSO	Industry
Dimitris	Gritzalis	Professor of ICT Security	Academia
Bruno	Halopeau	Information Assurance and Cyber Defence First Officer	Users
Stamatis	Karnouskos	Senior Researcher/ Research Expert	Industry
Cornelia	Kutterer	Director	Industry
Mika	Lauhde	Director	Industry
Jean-Pierre	Mennella	Cyber Security Manager	Industry
Katerina	Mitrokotsa	Senior Researcher	Academia
Rain	Ottis	Associate Professor	Academia
Bart	Preneel	Professor	Academia
Kai	Rannenberg	Chair of CEPIS Legal and security issues network	Academia
Alfredo	Reino	Security Solutions Architect	Industry
Volker	Schneider	Senior Business Development Manager	Industry
Marc	Vael	Chief Audit Executive	Industry
Claire	Vishik	Security Policy/Technology Manager	Industry

F. List of ENISA Management Board representatives and alternates

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

Commission representatives

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

Member States representatives

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 Technology and Communications gtodorov@mtitc.government.bg	Vasil **GRANCHAROV** Director of Computer Security Incidents Response Team directorate, Executive Agency 'Electronic Communication Networks and Information Systems' vgrancharov@esmis.government.bg
Croatia	Zeljko **TABAKOVIC**	Ivana **BIKIC**
Cyprus	Antonis **ANTONIADES** Senior Officer of Electronic Communications and Postal Regulation antonis.antoniades@ocecpr.org.cy	Costas **EFTHYMIOU** Officer of Technical Affairs at Office of the Commissioner of Electronic Communications and Postal Regulation costas.efthymiou@ocecpr.org.cy
Czech Republic	Jaroslav **SMID** Deputy Director National Centre for Cyber Security National Security Authority of the Czech Republic j.smid@nbu.cz	Roman **PACKA** Assistant Director of NSA r.packa@nbu.cz
Denmark	Anne Louise **CAPION** Senior adviser Danish Ministry of Defence Centre for Cyber Security loucap@cfcs.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 of 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	Jean-Baptiste **DEMAISON** Agence nationale de la sécurité des systèmes d'information (ANSSI) international.enisa-mb@ssi.gouv.fr	Yann **SALAMON** Agence nationale de la sécurité des systèmes d'information (ANSSI) international.enisa-mb@ssi.gouv.fr
Germany	Michael **HANGE** President of the Federal Office for Information Security (BSI) michael.hange@bsi.bund.de	Roland **HARTMANN** Head of International Relations Federal Office for Information Security (BSI) SIB@bsi.bund.de
Greece	Nikos **MOURKOGIANNIS** nikos@nikos.com	Theodoros **KAROUBALIS** Hellenic Ministry of Transport and Communications t.karoubalis@yme.gov.gr
Hungary	Ferenc **SUBA** **VICE-CHAIR OF ENISA MANAGEMENT BOARD** Senior Advisor National Cybersecurity Coordination Council Prime Minister's Office ferenc.suba@cyber security.me.gov.hu	Csaba **HORVATH** President National Information Security Authority Ministry of National Development Csaba.horvath@nfm.gov.hu
Ireland	Kevin **FOLEY** National Cyber Security Unit Department of Communications, Energy and Natural Resources Kevin.foley@dcenr.gov.ie	Paul **CONWAY** Head of Compliance and Operations Commission for Communications Regulation paul.conway@comreg.ie

Member State	Representative	Alternate
Italy	Rita **FORSI** Director General of Instituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI), Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, Department of Communications, Ministry of Economic Development rita.forsi@mise.gov.it	Alessandro **RIZZI** Ministry of Economic Development Department of Communications alessandro.rizzi@mise.gov.it
Latvia	Ieva **KUPCE** Adviser of State Secretary Ministry of Defence ieva.kupce@mod.gov.lv	Viktors **LIPENITS** Head of transport and communications division Ministry of Transport and Communications viktors.lipenits@sam.gov.lv
Lithuania		Dr Rytis **RAINYS** Head of Network and Information Security Department of the Communication Regulatory Authority of Lithuania rytis.rainys@rrt.lt
Luxembourg	François **THILL** Accréditation, notification et surveillance des PSC francois.thill@eco.etat.lu	Pascal **STEICHEN** Ministry of the Economy and Foreign Trade Department for electronic commerce and information security pascal.steichen@eco.etat.lu
Malta	John **AGIUS** Director (Critical Infrastructure Protection) Malta Critical Infrastructure Protection (CIP) Unit, Cabinet Office, Office of the Prime Minister john.f.agius@gov.mt maltacip@gov.mt	Charles **MIFSUD** CSIRT Malta Team Leader Malta Critical Infrastructure Protection (CIP) Unit Cabinet Office Office of the Prime Minister maltacip@gov.mt charles.h.mifsud@gov.mt
Netherlands	Elisabeth Christina (Elly) **van den HEUVEL**	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 p.durbajlo@abw.gov.pl
Portugal	José Carlos **BARREIRA MARTINS** Coordinator of the National Centre for Cybersecurity	Manuel **PEDROSA DE BARROS** Diretor da Direção de Segurança das Comunicações da ANACOM 2730-216 Barcarena manuel.barros@anacom.pt
Romania	Augustin **JIANU** Director CERT-RO augustin.jianu@cert-ro.eu	Dan **TOFAN** Technical Director CERT Romania dan.tofan@cert-ro.eu
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	National Security Department, Spanish Prime Minister´s Office dsn@dsn.presidencia.gob.es	National Security Department, Spanish Prime Minister´s Office dsn@dsn.presidencia.gob.es

Member State	Representative	Alternate
Sweden	Jörgen **SAMUELSSON** **CHAIR OF ENISA MANAGEMENT BOARD** Deputy Director Division for Information Technology Policy Ministry of Enterprise, Energy and Communications jorgen.samuelsson@gov.se	Annica **BERGMAN** Network Security Department Swedish Post and Telecom Agency (PTS) annica.bergman@pts.se
United Kingdom	Rachael **BISHOP** BIS Assistant Director of Cyber EU and International Policy Rachael.bishop@bis.gsi.gov.uk	Colin **WHORLOW** Head of International Relations CESG colin.whorlow@cesg.gsi.gov.uk

EEA-country representatives (observers)

Iceland	Björn **Geirsson** Director of Legal Division 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	Knut Anders **MOI** Deputy Director General Ministry of Justice and Public Security knut.moi@jd.dep.no

G. List of policy documents

Nr.	Policy document	Complete title and link ([10])
1	**The new ENISA Regulation (EU) No 526/2013**	REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:L:2013:165:TOC Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.
2	**The ccyber security strategy of the EU**	Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, available at: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
3	**The proposal for NIS directive**	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf
4	**Council conclusions on the cyber security strategy**	Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, agreed by the General Affairs Council on 25 June 2013, http://register.consilium.europa.eu/pdf/en/13/st12/st12109.en13.pdf
5	**Digital agenda**	A Digital Agenda for Europe, COM(2010)245, May, 2010
6	**Directive on ECIs**	Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

[10] Available links as of October 2014.

Nr.	Policy document	Complete title and link [10]
7	**The CIIP action plan**	The Commission Communication 'Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience' COM(2009)149, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF
8	**Commission communication on critical information infrastructure protection**	The Commission Communication on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security' adopted on 31 March 2011 and the Council Conclusion on CIIP of May 2011, http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf
9	**Electronic communications regulatory rramework**	Telecommunications Regulatory Package (article 13a. amended Directive 2002/21/EC Framework Directive)
10	**Review of the data protection framework**	Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM 2012/11 final of 25.1.2012, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
11	**Regulation on electronic identification and trusted services for electronic transactions in the internal market (eIDAS regulation)**	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
12	**Commission Regulation on the measures applicable to the notification of personal data breaches**	Commission Regulation (EU) No 611/2013, of 24 June 2013, on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF
13	**Framework to build trust in the Digital single market for e-commerce and online services**	European Commission, 'A coherent framework for building trust in the Digital Single Market for e-commerce and online services' COM(2011)942, 11.1.2012, http://ec.europa.eu/internal_market/e-commerce/communication_2012_en.htm
14	**Council Framework Decision on attacks against information systems**	Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems
15	**Communication on EC3**	Commission Communication 'Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre', European Commission, COM(2012) 140 final, 28.3.2012, available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/communication_european_cybercrime_centre_en.pdf
16	**Council Resolution of December 2009 on a collaborative approach to Network and Information Security**	Council resolution of 18 December, 2009 on a collaborative approach to network and information security (2009/C 321 01), available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:C:2009:321:TOC
17	**Council conclusion on CIIP of May 2011**	Council Conclusion on CIIP of May 2011, available at: http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf
18	**Action plan for an innovative and competitive security industry**	Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee regarding an Action Plan for an innovative and competitive Security Industry, COM(2012) 417 final
19	**Single Market Act**	Single Market Act — Twelve levers to boost growth and strengthen confidence 'Working Together To Create New Growth', COM(2011)206 Final
20	**Internet of things — An action plan for Europe**	Communication of the Commission to the Parliament, the Council, the EU Economic and Social Committee and the Committee of Regions on the Internet of Things, COM(2009)278 final of 18. June 2009.
21	**European cloud computing strategy**	The Communication COM(2012)529 'Unleashing the potential of cloud computing in Europe', adopted on 27 September 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF
22	**Internal security strategy for the European Union**	An internal security strategy for the European Union (6870/10), http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/113055.pdf
23	**Telecom Ministerial Conference on CIIP**	Telecom Ministerial Conference on CIIP organised by the Presidency in Balatonfüred, Hungary, 14-15 April 2011
24	**Data Protection Directive**	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
25	**ENISA work programme 2014 Amendment**	Amendment of the ENISA 2014 work programme updating the deliverables list https://www.enisa.europa.eu/publications/programmes-reports/work-programme-2014-amendment

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
  via EU Bookshop (http://bookshop.europa.eu);
- more than one copy or posters/maps:
  from the European Union's representations (http://ec.europa.eu/represent_en.htm);
  from the delegations in non-EU countries (http://eeas.europa.eu/delegations/index_en.htm);
  by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm) or
  calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

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

TP-AB-15-001-EN-N

Publications Office

ISBN 978-92-9204-124-3
doi:10.2824/521040