European Union Agency for Network and Information Security

Work Programme 2015
Including Multi-Annual Planning

DECISION No MB/2014/12
of the Management Board of the European Union Agency for Network and Information Security

(Adopted at the MB Meeting on 28 October 2014)

enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Follow ENISA on

Facebook Twitter LinkedIn YouTube and RSS feeds

Contact details

For contacting ENISA or for general enquiries on Privacy please use the following details:

Email: info@enisa.europa.eu

Internet: http://www.enisa.europa.eu

Legal notice

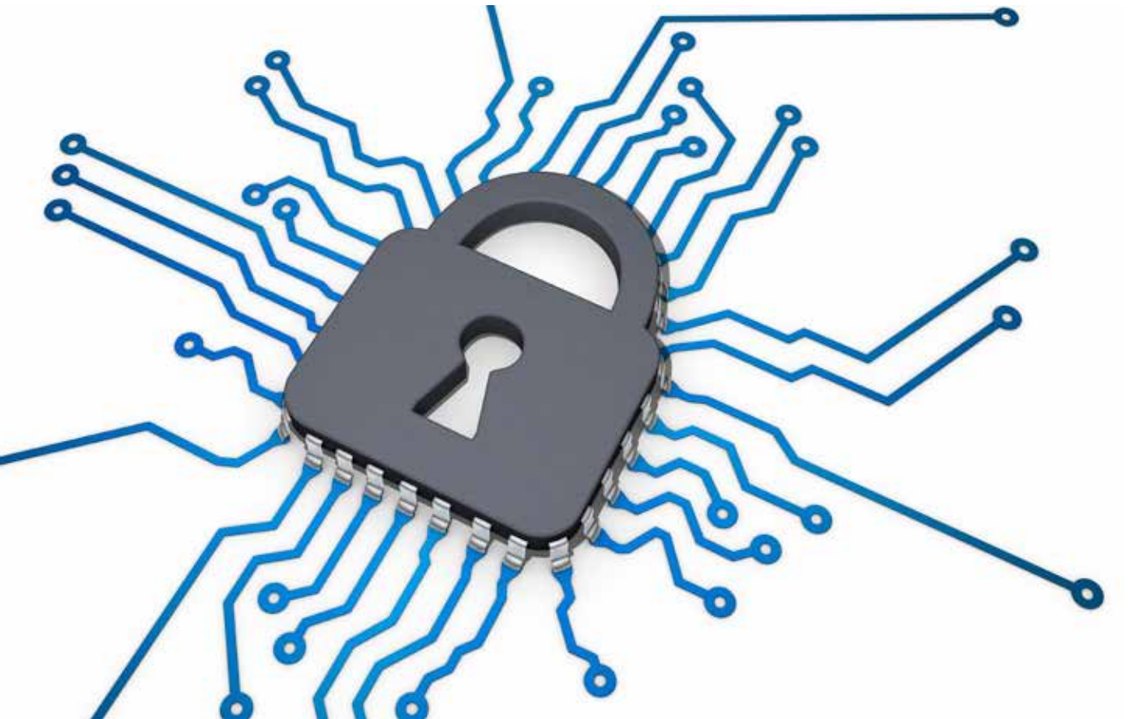
This publication details the ENISA Management Board Decision MB/2014/12 on the ENISA Work Programmeme 2015 including multi-annual planning at the time of printing. The Management Board may amend this decision at any time.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

Catalogue number: TP-AF-14-001-EN-N, ISBN: 978-92-9204-114-4,
ISSN: 2363-3115, DOI: 10.2824/097365

Contents



Acronyms

ABB: Activity Based Budgeting
APF: Annual Privacy Forum
ASA: Administration and Support Activities
ASD: Administration and Support Department
CE2014: Cyber Europe 2014
CEO: Chief Executive Officer
CEP: Cyber Exercises Platform
CERT: Computer Emergency Response Team
CII: Critical Information Infrastructures
CIIP: Critical Information Infrastructure Protection
CISO: Chief Information Security Officer
COD: Core Operations Department
CSCG: ETSI CEN-CENELEC Cyber Security Coordination Group
CSIRT: Computer Security Incidents Response Teams
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
EDPS: European Data Protection Supervisor
eID: electronic Identity
ENISA: European Union Agency for Network and Information Security
EU: European Union
FAP: Finance, Accounting and Procurement unit
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
IaaS: Infrastructure as a Service
ICC and 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 and Facilities Management Unit
ITU: International Telecommunication Union
IXP: Internet exchange point
KII: Key Impact Indicator
KPI: Key Performance Indicator
LEA: Law Enforcement Agency
MB: Management Board
MS: Member States
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
PETs: Privacy Enhancing Technologies
PPP: Public Private Partnership
PSG: Permanent Stakeholders Group
Q: Quarter
QMS: Quality Management System
RandD: Research and Development
ROSI: Return of Security Investment
SCADA: Supervisory Control And Data Acquisition
SME: Small and Medium Enterprise
SO: Strategic Objective
SOGIS: Senior Officials Group Information Systems Security
SOP: Standard Operating Procedures
TF-CSIRT: Task Force of Computer Security Incidents Response Teams
TISPAN: Telecommunications and Internet converged Services and Protocols for Advanced Networking
TRANSITS: Computer Security and Incident Response Team (CSIRT) personnel trainings
TSP: Trust Service Provider
US: United States of America
WP: Work Programmeme
WPK: Work Package

1. Introduction

1.1 Introduction

This document consists of two major components:

- A multi-annual planning for the years 2015 to 2017.
- The ENISA Work Programmeme for 2015.

The multi-annual planning has been derived from the ENISA Strategy document, which has been developed together with the ENISA Management Board. As such, the planning is based on four strategic objectives (which are presented in section 3.1). This approach ensures that future ENISA Work Programmemes reflect the strategic objectives of the Agency.

The Work Programmeme itself reflects the conclusions of the ENISA Management Board meeting of November 2013 with some minor adjustments for consistency and to facilitate smooth implementation, the results of the meetings of the ad-hoc working group on 27.02.2014 and 21.05.2014 and the comments made during the Management Board editorial meeting held on 11.09.14.

1.2 Structure

1.2.1 Strategic objectives and multi-annual planning

The strategic objectives and multi-annual planning provide the link between the ENISA Strategy document and both this and future Work Programmemes. In this section, key goals are set for each core priority for the period 2015-2017.

1.2.2 Core operational activities 2015

This section presents the core activities for 2015. Budget and resources are presented at the work package level in section 4.14 and deliverables are summarised in section 4.15.

1.2.3 Administration and Support Department, Directorate and General management activities

This section of the document summarises the activities of the Administration and Support Department (ASD) and the Executive Director. Budget and resources requirements are also identified here.

1.3 Key Performance Indicators and Key Impact Indicators

The terms Key Performance Indicator (KPI) and Key Impact Indicator (KII) are defined as follows:

Key performance indicators (KPIs) are quantifiable metrics used to evaluate objectives to reflect the performance of an organisation. KPIs measure the agency's performance during the budgetary/fiscal year. KPIs differ depending on the nature of the organisation. Different layers and dimensions should be taken into consideration. KPIs can constitute both quantitative and qualitative measures; however, the most useful and common types are quantitative based. These include amongst others a focus on metrics such as number of MS targeted, and number of hits to the website etc.

Key impact indicators (KIIs) are indicators used to evaluate long-term performance and eventually linked to the strategy foundation stone of an organisation.

In this Work Programmeme document, the Agency proposes a number of Key Impact Indicators for each work package. Measuring the subsequent impact however is a difficult and time-consuming activity, due to the fact that the impact of ENISA's work on its stakeholder communities is often indirect and involves a number of intermediate parties in the implementation process. This is particularly true for those deliverables which essentially propose recommendations to various stakeholders (these are ENISA studies).

2. Policy and Legal Context

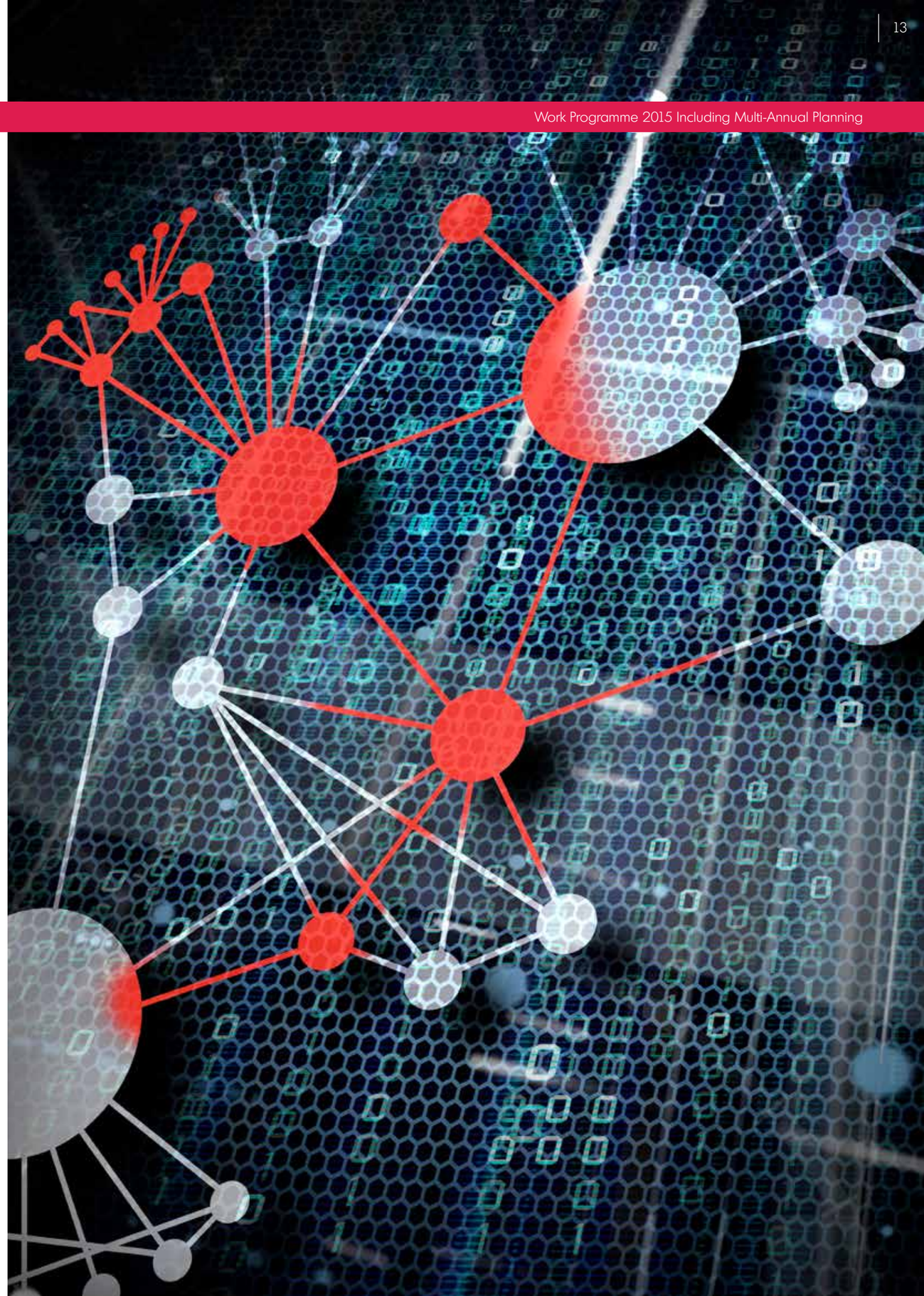
The Agency situates its work in the wider context of a legal and policy environment as pointed out below. Its activities and tasks are fulfilled as defined by its Regulation and integrated in this larger legal framework and policy context.[1]

1 Please note that this does not constitute a comprehensive listing of all relevant policy acts and the legal framework. For more detailed references of legal base and policy context of ENISA's activities in WP 2015, please refer to each WS.

Nr.	Policy document	Complete title and link
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 Cybersecurity 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 Cybersecurity Strategy**	Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, agreed by the General Affairs Council on 25 June 2013, http://register.consilium.europa.eu/pdf/en/13/st12/st12109.en13.pdf
5	**Digital Agenda**	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
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 Framework**	Telecommunications Regulatory Package (article 13a. amended Directive 2002/21/EC Framework Directive)
10	**Review of the Data Protection Framework**	Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM 2012/11 final of 25.1.2012, 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**	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

Nr.	Policy document	Complete title and link
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
24	**Telecom Ministerial Conference on CIIP**	Telecom Ministerial Conference on CIIP organised by the Presidency in Balatonfüred, Hungary, 14-15 April 2011

The Strategic Objectives that are described in this document have been developed taking account of this legal framework and context while they support this overall political agenda.



3. Strategic objectives and multi-annual planning

3.1 Strategic Objectives

The following strategic objectives (SO) originate from the ENISA strategy document:

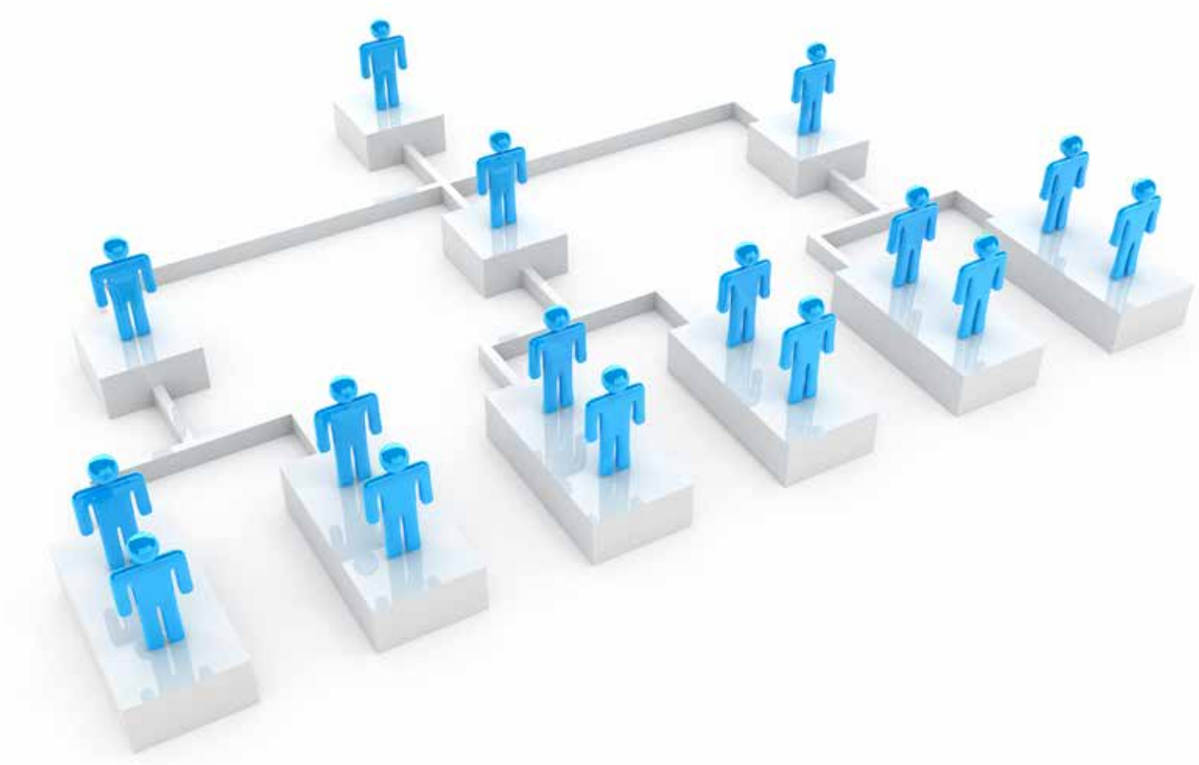
- SO1. To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network and Information Security (NIS).
- SO2. To assist the Member States and the Commission in enhancing capacity building throughout the EU.
- SO3. To assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security.
- SO4. To enhance cooperation both between the Member States of the EU and between related NIS communities.

The following sections provide a high-level, multi-annual planning for each of these objectives thereby providing a basis for the definition of future Work Programmemes of the Agency.

3.2 Strategic Objective 1

To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network and Information Security (NIS).

	2015	2016	2017
Objective	PLEASE REFER TO CHAPTER 4	• facilitate voluntary information sharing techniques to enhance quality of collection, assessment and validation of threat and risk information. • establish mutual interactions with stakeholders in the area of information sharing and threat analysis. • identify 2 emerging technology areas and perform threat and risk assessments.	• use of advanced tools to facilitate phases of knowledge management. Use of interfaces to related stakeholders to exchange information on threats and risks. Increase quality, accuracy and speed of performed assessments. • identify 2 emerging technology areas and perform threat and risk assessments.
Resources (FTEs)	PLEASE REFER TO CHAPTER 4.14	4 FTEs	4FTEs
Budget (Euro)	PLEASE REFER TO CHAPTER 4.14	200 k euros	300 k euros



3.3 Strategic objective 2

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

	2015	2016	2017
Objective	PLEASE REFER TO CHAPTER 4	• Support MS and Commission on the implementation of the NIS Directive subject to its agreement. • Analyse 1 CIIP sector and propose good practices and recommendations (e.g. health). • Assist 5 MS and 5 Private Sector companies in deploying good practices for Smart Grids (e.g. training, exercises). • Assist 5 MS in developing good practices for Internet Interconnections (e.g. training, exercises). • Assess current national NIS cooperation plans and procedures. • 20% of MS n/g CERTs attended ENISA CERT training. • 15% of MS n/g CERTs approve and apply ENISA recommendations for Baseline Capabilities. • At least one new operational community identified and, when appropriate, approached (via training of by including them in the ENISA CERT workshops). • Review and verification against the Regulation 910/2014 of definitions used in the context of TSPs in other sources. • Establish the forum of trust service providers, conformity assessment bodies and supervisory authorities. • Assist stakeholders in the deployment of ENISA"s good practices in the area of smart cities, smart homes, and big data. • engage stakeholders in the identification of new smart infrastructures and services.	• Support MS and Commission on the implementation of the NIS Directive subject to its agreement. • Analyse 1 CIIP sector and propose good practices and recommendations (e.g. transport). • Assist 3 MS and 5 Private Sector companies in deploying good practices for Finance Sector (e.g. training, exercises). • Assist 3 MS and 5 Private Sector companies in deploying good practices for Smart Cities (e.g. training, exercises). • Support Member States in improving current national NIS cooperation plans and procedures. • 25% of MS n/g CERTs attended ENISA CERT training. • 20% of MS n/g CERTs approve and apply ENISA recommendations for Baseline Capabilities. • At least one new operational community identified and, when appropriate, approached (via training of by including them in the ENISA CERT workshops). • 'Spin-off' the forum of trust service providers, conformity assessment bodies and supervisory authorities outside the APF. • develop good practices for 2 emerging smart infrastructures and services. • engage the stakeholders in the deployment of them.
Resources (FTEs)	PLEASE REFER TO CHAPTER 4.14	35,4 FTEs	35,4 FTEs
Budget (Euro)	PLEASE REFER TO CHAPTER 4.14	1.150 k euros	1.445 k euros

3.4 Strategic objective 3

To assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security.

	2015	2016	2017
Objective	PLEASE REFER TO CHAPTER 4	• Assist MS in the establishment of national PPPs (e.g. seminars, training). • Support NRAs and Commission on the implementation of article 13 a. • Support NRAs and Commission on the implementation of article 4 of the ePrivacy Directive. • Support NRAs and Commission on the implementation of article 15 of the eIDAS Directive. • Assist the Commission on the implementation of the EU Cyber Security Strategy. • Participating in H2020 project(s) reviews and evaluations, • In the scope of H2020, participating in the advisory/steering board of selected projects. • Contributing to the H2020 relevant consultations. • Organisation of consultation with industry on identifying common standardisation priorities to be supported under H2020. • Development of strategy on the adoption of best practices by industry and data controllers. • Practical Data Breach Notification mechanisms.	• Assist MS in the evaluation of NCSS (e.g. seminars, training). • Support NRAs and Commission on the implementation of article 13 a. • Support NRAs and Commission on the implementation of article 4 of the ePrivacy Directive. • Support NRAs and Commission on the implementation of article 15 of the eIDAS Directive. • Assist the Commission on the implementation of the EU Cyber Security Strategy. • Participating in H2020 project(s) reviews and evaluations. • In the scope of H2020, participating in the advisory/steering board of selected projects. • Contributing to the H2020 relevant consultations. • Contribute in setting priorities in the areas of standardisation relevant to ENISA interests. • Identify industries/sectors to target for the transfer of best practices. • Methodologies and tools for DPAs and controllers.
Resources (FTEs)	PLEASE REFER TO CHAPTER 4.14	15,8 FTEs	15.8 FTEs
Budget (Euro)	PLEASE REFER TO CHAPTER 4.14	430 k euros	505 k euros

3.5 Strategic objective 4

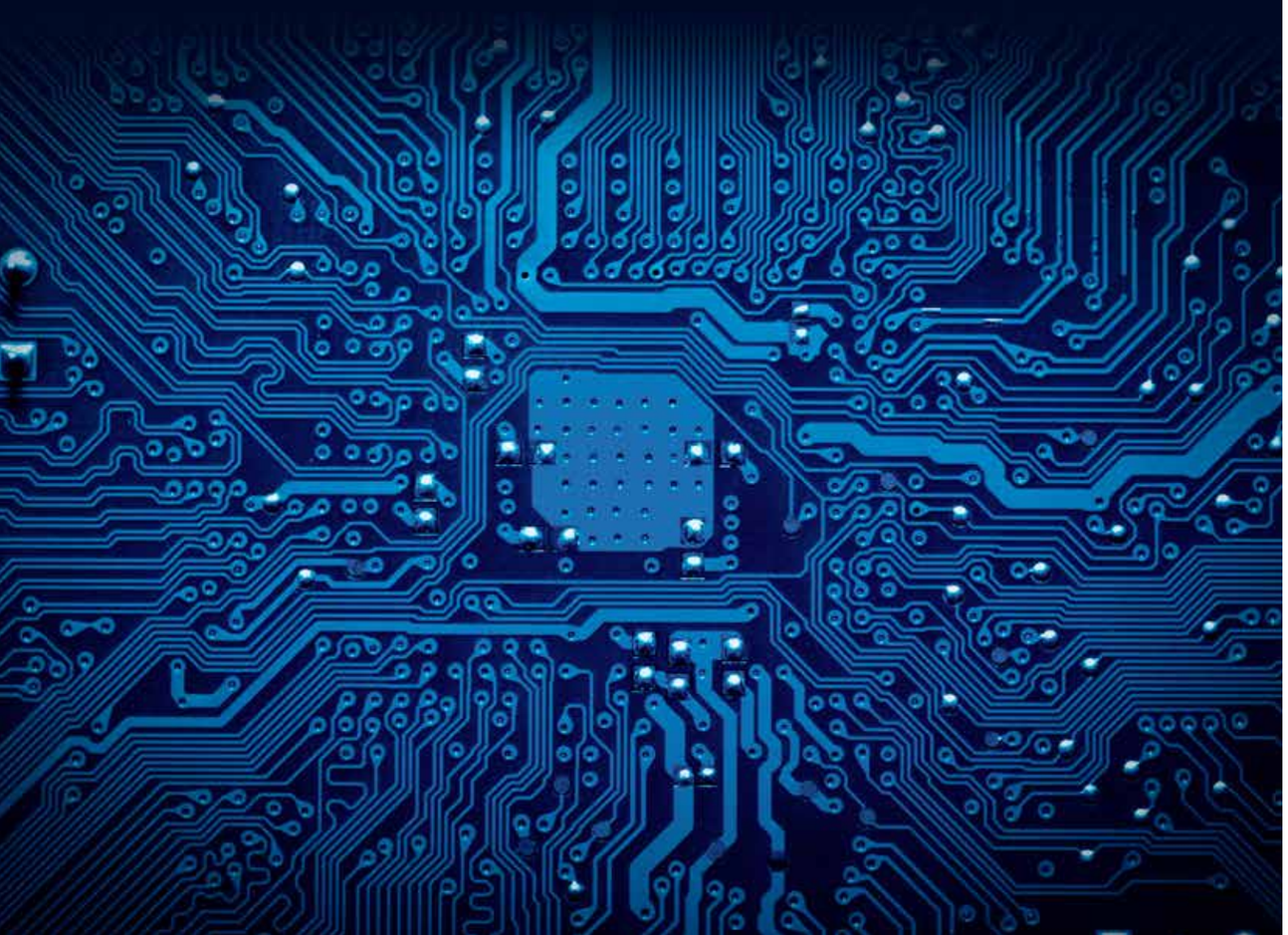
	2015	2016	2017
Objective	PLEASE REFER TO CHAPTER 4	• 15% of MS n/g CERTs approve and apply ENISA recommendations for Baseline Capabilities. • At least one new operational community identified and, when appropriate, approached (via training of by including them in the ENISA CERT workshops). • Continue planning, conducting and Evaluate more Cyber Exercises. • Adjust the direction of Cyber Europe to the needs of ENISA stakeholders. • Maintain and update the CE roadmap.	• 20% of MS n/g CERTs approve and apply ENISA recommendations for Baseline Capabilities. • At least one new operational community identified and, when appropriate, approached (via training of by including them in the ENISA CERT workshops). • Continue planning, conducting and Evaluate more Cyber Exercises. • Adjust the direction of Cyber Europe to the needs of ENISA stakeholders. • Maintain and update the CE roadmap.
Resources (FTEs)	PLEASE REFER TO CHAPTER 4.14	16,6 FTEs	16,6 FTEs
Budget (Euro)	PLEASE REFER TO CHAPTER 4.14	505 k euros	550 k euro

4. Core operational activities

4.1 Introduction

From 2015 onwards ENISAs core operational activities are aligned with the strategic objectives from the strategy and the multi annual planning. The strategic objectives effectively replace the structure of "work streams (WS)" from previous years and are as follows:

- SO1: To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network and Information Security (NIS).
- SO2: To assist the Member States and the Commission in enhancing capacity building throughout the EU.
- SO3: To assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security.
- SO4: To enhance cooperation both between the Member States of the EU and between related NIS communities.



4.2. SO1 – To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network and Information Security (NIS)

4.2.1. Overview

Justification

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

The Agency will support the MS and the Commission in their efforts to improve CIIP by fostering a common approach across the MS and by ensuring that good practice and lessons learnt are shared and properly deployed in an effective manner. The Agency will work with the MS, the Commission and the private sector in capacity building across the EU. In particular, the Agency will support the development of voluntary baseline security requirements for CIIP sectors and harmonise efforts in the area of mandatory incident reporting taking under consideration existing national and international frameworks (e.g. NIST). The approach will not be limited to securing Internet related services, but will take into consideration other networks and services as appropriate. This is also an area in which public private partnership is likely to bring significant gains and ENISA will continue to support this approach.

Where technology is concerned, information security has traditionally been viewed as an approach for securing the interaction of people, process and technology. Of these three factors, it is mainly technological evolution that impacts the way in which people's behaviour and process change. A large part of modern information security therefore boils down to adapting current methods to emerging technologies, and business models.

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

Specific Policy Context

Each work package description contains a section highlighting the specific policy context for the activities foreseen.

Overall Goals

Ensuring adequate levels of protection for modern IT systems in any context requires recognising and adapting to changes in the evolving threat environment. Whilst it is clearly not possible to foresee all future threats it is possible to predict the evolution of certain threats with a reasonable degree of accuracy based on past data.

- ENISA can support its stakeholders by compiling existing data on threat evolution and tailoring this data to the needs of specific stakeholder communities.

- The collection and analysis of security data is an important part of ENISA's existing mandate and is not limited to incident-related data. It is the intention of the Agency to develop this capacity in the future, both for data describing security incidents and other data that could be of use to MS in order to improve MS understanding of the NIS trends.
- ENISA will assist the Commission and MS in defining and implementing a framework for training professionals in NIS to meet the requirements of industry at all levels. The goal will be to align training goals with career paths for security professionals and to provide a more global background in NIS for professionals in other areas.

4.2.2. Work Packages

The following work packages constitute this Strategic Objective:

WPK 1.1 – NIS Threats Analysis

This WPK main goal is to develop the current cyber threat landscape. This information is important in the identification of NIS gaps and security needs for a wide spectrum of stakeholders.

WPK 1.2 – Improving the Protection of Critical Information Infrastructures

In this WPK ENISA aims at providing advice and assistance on request to targeted stakeholders of Critical Information Infrastructures (CIIs).

WPK 1.3 – Securing emerging Technologies and Services

This WPK aims to develop good practices on emerging smart infrastructures and services and work with relevant stakeholders to deploy them at an early stage of adoption.

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

This WPK aims at defining and implementing a framework that will allow the Agency to provide timely and high quality responses to NIS developments.

4.2.3. WPK 1.1: NIS Threats Analysis

Desired Impact

- Engage 10 public and 10 private stakeholders in the Threat Analysis/Landscape process. These stakeholder should participate in the validation of the work.
- Engage 10 public and 10 private stakeholders in the risk assessment of each emerging technologies/ sector. These stakeholder should participate in the validation of the work.
- 5 MS use by 2016 ENISA's Threat Analysis/Landscape process in their national risk management processes.
- 10 private stakeholders use by 2016 ENISA's Threat Analysis/Landscape process in their corporate risk management processes.

Description of tasks

The main goal of this work package is to develop the current cyber threat landscape. This information is important in the identification of NIS gaps and security needs for a wide spectrum of stakeholders.

The agency will collect, collate and analyse existing publicly available material on threats, risks, and trends in NIS and emerging technologies application areas. Non publicly available material can be given to ENISA via relevant stakeholders (e.g. NLOs). The data will be used for developing the annual ENISA Threat Landscape Report. In this process, ENISA will seek contributions from relevant stakeholders to enhance quality, accuracy and speed of assessed information. As was the case for the ENISA reports of previous years ENISA will use the ENISA Threats Landscape Stakeholders forum (with participation by the CERT-EU, EU institutions, national agencies, etc.) to support this activity and seek input.

In addition, in this work package ENISA will identify two emerging technology/application areas and perform detailed threat and risk assessments. The emerging technology/application areas will be crucial for society and the economy in the coming 2-4 years. Examples will be from sectors like internet infrastructures, banking and finance, health, transport, energy and public administration and could cover areas like Software Defined Networks or Security of mobile networks ("Mobile Security"). Such areas will be identified from the emerging technology trends but also from assessed threat trends. Hence, their importance for security and privacy will be considered a given.

In both areas of work ENISA will identify and consult with relevant stakeholder communities. The Agency will co-operate with stakeholders on improving its data collection framework, on analysing the collected data and on performing the sectorial risk assessments.

Outcomes and deadlines

Based on the tasks described above, the following outcomes and deliverables are envisaged:

D1: Annual Threat Analysis/Landscape Report (Q4, 2015).

D2: Risk Assessment on two emerging technology/application areas (Q4, 2015).

Stakeholder impact

The primary beneficiaries of this work package will be policy makers and organisations from public and private sectors, who will receive integrated and consolidated information about the European NIS threat landscape and how it is evolving:

- Public and private organisations will be able to use the ENISA Threat Landscape in their own risk and threat assessment in order to develop more effective security strategies, thus improving their Return of Security Investment (ROSI).
- EU Commission DG CONNECT will be able to use the ENISA output to adjust the scope of their RandD related activities.

Public and private organisations may capitalise on the ENISA output to propose innovative RandD activities, products or services.

Resources

- (see chapter 4.14)

Legal base and policy context

- ENISA regulation, article 3, particularly 3.1.(b) and 3.1.(c).
- Commission proposes Action Plan to enable further growth of Security industry[2] COM(2012) 417:

  The Commission has produced a "COMMISSION STAFF WORKING PAPER on Security Industrial Policy"[3] SWD(2012) 233 final, and "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE"[4] COM(2012) 417 final. The Commission proposes to create a true internal market for the security industry by inter alia:
  - introducing checks on the societal impact of new security technologies at the research stage. To reduce the gap between research and market, especially in European and international procurement, the Commission will use novel funding schemes foreseen in Horizon 2020 such as Pre-commercial Procurement, to test and validate results stemming from EU security research projects. This approach should unite industry, public authorities and end users from the beginning of research projects. Border security and aviation security are the most promising areas.
  - novel funding schemes such as Pre-commercial Procurement to test and validate results stemming from EU security research projects.
- COUNCIL RESOLUTION, 18/12/ 2009, on a collaborative European approach to Network and Information Security, (2009/C 321/01)[5]. In this resolution the Council recognises the potential role of ENISA to build a NIS scenario in Europe. It also underlines that the major goals of NIS are to support:
  - Quality of Information handling.
  - Collection of statistical data on NIS in MS and EU institutions.
  - Raise awareness and good practices and guidance.

EU policy development and implementation support to European Commission and MS, bridging gap between technology and policy, and following EU priorities.

2 http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item_id=6117andlang=enandtpa_id=0andtitle=Security-industry%3A-Commission-proposes-programme-to-enable-further-growth-

3 ec.europa.eu/enterprise/policies/security/files/commission_staff_working_paper_-_security_industrial_policy_-_com(2012)_417_final_en.pdf

4 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF

5 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF

4.2.4. WPK 1.2: Improving the protection of Critical Information Infrastructures

Desired Impact

- By 2017, 8 MS use ENISA's findings and good practices in their national CIIP strategies. engaging 8 public and 8 private stakeholders (ISP, IXPs, Telcos) in the development of the methodology on internet interconnections.
- By 2016, 5 MS use ENISA's government cloud good practices on in their national strategy.
- 5 MS and 5 private stakeholders use ENISA's recommendations on finance in their corporate/national risk assessment and management approach.
- 5 MS and 5 private stakeholders use ENISA's recommendations on eHealth in their corporate/national risk assessment and management approach.

Description of tasks

In this work package ENISA aims at providing advice and assistance on request to targeted stakeholders of Critical Information Infrastructures (CIIs).

More specifically ENISA will take stock of MS policies, regulations and strategies including international frameworks (e.g. US NIST) and identify gaps related to CIIs. The Agency will co-operate with public and private stakeholders to identify good practices, collect and analyse requirements and issue recommendations for improving the way MS address the protection of CIIs.

In the area of Internet Interconnections, ENISA will continue developing its methodology for the identification of critical communication networks, links, and components. ENISA will consider existing outputs from projects and initiatives on the security and resilience of Internet interconnections. In co-operation with ISPs and other public stakeholders ENISA will validate the methodology and develop a maturity assessment mechanism. This mechanism would allow MS themselves to assess their situation within their borders. The Agency will also assess whether this methodology can be extended to other CIIs and work with targeted stakeholders to customise it to their needs and requirements.

In the area of ICS-SCADA security, ENISA will co-operate with EuroScsie and other related expert groups to take stock of and analyse the cyber security maturity levels in critical sectors (e.g. transport, energy, water supply, etc.). Using ENISA's work (among others) policy makers in MS and EU Institutions can create the right secure framework for the implementation and deployment of more efficient IC-SCADA systems. Through co-operation with the public and private sector ENISA will identify, share and develop good practices, information on gaps in policies, as well as regulations and strategies at national as well as EU level. The Agency will continue promoting its work on the security of ICS-SCADA devices.

In the area of Smart Grids, ENISA will continue its work on minimum security measures and national governance security models of Smart Grids. The Agency will promote its existing minimum security measures and further co-operate with public and private stakeholders to improve their existing security governance models for Smart Grids. It should be noted that smart grid area covers more than ICS; so for this activity more areas are considered: smart cities, smart energy etc. ENISA will also continue contributing to DG ENER's Smart Grid Task Force and all relevant EU initiatives (e.g. CEN/CENELEC/ETSI, ERNCIP, DENSEK, etc.). Finally the Agency will contribute to national and EU efforts (e.g. SOGIS) related to better alignment of certification policies and strategies at EU level. Such alignment would remove barriers across EU MS and allow European industry to become more competitive and innovative.

In the area of cloud computing, ENISA will actively contribute to EU Commission's EU Cloud Computing Strategy by delivering targeted advice on cyber security matters (e.g. certification, minimum security measures, procurements, SLAs and others). The Agency will continue its work in the area of governmental clouds, assist MS to develop their national governmental strategy and deploy ENISA's good practice guide. ENISA will also work with public and private sector to widely promote its work on the certification of cloud computing components and services. The Agency aims at establishing ENISA's meta certification framework as the key model used by the users, SMEs and leading players in the market. ENISA does not aim at developing an EU wide certification scheme, but just a mapping scheme that would allow cloud users to select the most appropriate, existing certification scheme fitting their needs. That would especially help SMEs to select the most sophisticated offer from the market.

In the area of finance, ENISA, through consultation with public and private stakeholders, will identify policy, technical and regulatory barriers and challenges for using cloud, either as an infrastructure or as a service, in the finance sector. The Agency will issue recommendations for policy makers, EU MS and industry to mitigating the barriers and challenges. Aiming at removing such barriers ENISA will help the EU industry to become more competitive and innovative. Also the Agency will consult with public and private stakeholders to better understand the security and privacy challenges related with third party payments providers.

Finally in the area of eHealth, ENISA will identify all relevant public and private stakeholders, engage them in a working group to take stock and assess the security and resilience of major eHealth infrastructures and services. The Agency will then develop good practices and recommendations for policy makers, industry and EU MS on the resilience and security of eHealth infrastructures and services.

Outcomes and deadlines

Based on the tasks described above, the following outcomes and deliverables are envisaged:

D1: Stock Taking, Analysis and Recommendations on the protection of CIIs (Q3, 2015).

D2: Methodology for the identification of Critical Communication Networks, Links, and Components (Q4, 2015).

D3: Analysis of ICS-SCADA Cyber Security of Devises in Critical Sectors (Q4, 2015).

D4: Recommendations and Good Practices for the use of Cloud Computing in the area of Finance Sector (Q4, 2015).

D5: Good Practices and Recommendations on resilience and security of eHealth Infrastructures and Services (Q4, 2015).

Stakeholder impact

- Cloud Computing
  - A number of governmental clouds are being set-up. A single framework for governmental cloud computing, (1) allows MS to share and exchange knowledge on best-practices, (2) allows providers to cater for different MS more easily, without having to adjust the cloud technology to different requests in different countries, ultimately lowering the costs, (3) allows MS to move computing workloads to other countries in failover and backup scenarios.
  - By setting a single set of security requirements for procurement by public sector across the EU, the MS can improve procurement of cloud computing in the private sector as well, making it more easy for SMEs to procure cloud computing services in line with national security requirements, and also to procure cloud computing services across the EU's single digital market.
- Finance
  - Banks would benefit from having an independent analysis and set of guidelines about inter-banking communications and transactions.
  - Industry would be able to use a neutral, not vendor specific discussion platform with an improved exchange of good security and resilience practices in the area of telecommunications.
- Smart Grids and ICS-SCADA

  ENISA's recommendations on minimum security measures for smart grids are expected to provide all the relevant stakeholders with a tool for:
  - Allying of the varying levels of security and resilience of the market operators with a consistent minimum framework.
  - Providing an indication of a minimum level of security and resilience in the MS, by avoiding the creation of the "weakest link".
  - Ensuring a minimum level of harmonisation on security and resilience requirements across MS and thus reducing compliance and operational costs.
  - Setting the basis for a minimum auditable framework of controls across Europe.
  - Facilitating the establishment of common preparedness, recovery and response measures and paving the way for mutual aid assistance across operators during crisis.
  - Contributing to achieve an adequate level of transparency in the internal market.

- In the area of ICS-SCADA security ENISA's recommendations are expected to:
  - Provide a level of assurance to the stakeholders that the IT security personnel has the necessary knowledge and skills and can provide value to their organization.
  - Raise the level of awareness as regards cyber security issues within the organization.
  - Support the structured information sharing between vendors and asset owners as regards the vulnerabilities of their products.
  - Increase the transparency of the security offered by and thus increasing the trust of the public to their solutions.
  - Help vendors and asset owners in demonstrating their commitment to network and information security practices.
  - Allow policy makers in MS to create the right secure framework for the implementation and deployment of more efficient IC-SCADA systems, and for a better incident management.
  - The raised of awareness and information sharing among stakeholders will facilitate the labour of CEOs to take justified decisions on cyber security investments and will enhance the network of contact points for security and incidents management.
- Electronic communications sector (ISPs and telecommunications sector)
  - ENISA's recommendations will help NRAs and MS' Cyber Security agencies to better understand the way data communications networks in their area of responsibility are interconnected, and identify possible points of failure.
  - NRAs and MS' Cyber security agencies will be able to develop schemes to enhance the resilience of the data communication infrastructure at a regional or national level, and work together with operators of data communication networks (ISPs, IXPs) to deploy them at national level with the help of ENISA.
  - ISPs and IXPs will be able to better use the existing technology to better serve customers during crisis and offer related services.
- In the area of eHealth ENISA's recommendations are expected to:
  - allow eHealth providers to identify major gaps in the security policies they deploy to protect their systems
  - provide to MS better understand of their cyber security challenges in the area of eHealth at technical, policy and regulatory level
  - provide recommendations to EU Commission and MS on how eHealth cyber security be better dealt with
  - bring public and private sector to share information on good practices and develop together a set of good practices to be used by both of them.

Resources

- (see chapter 4.14)

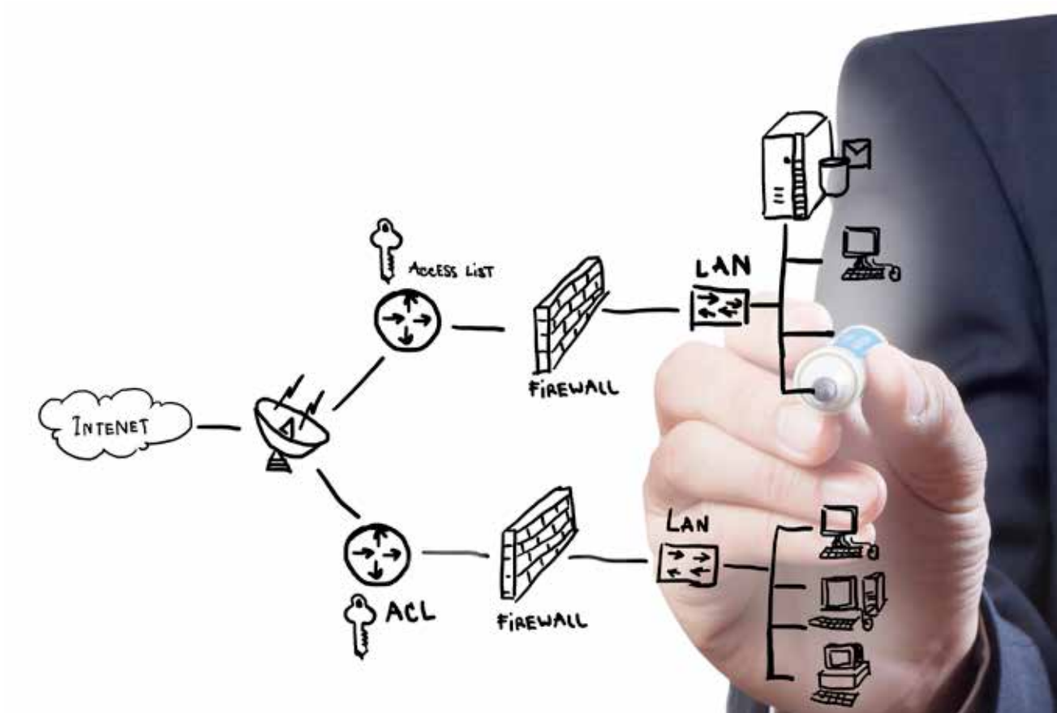
Legal base and policy context

- ENISA Regulation article 3, in particular 3.1.(c) (ii) and (iii) on promoting and sharing best practice.
- CIIP Action Plan 2009 and 2011.
- Digital Agenda 2010.
- European Strategy for Cyber Security, Cloud computing strategy.
- Council Resolution of 18 December 2009.
- Internal Security Strategy for the European Union.
- COM(2011) 202, Smart Grids: From innovation to deployment.
- EC Recommendations on preparations for the roll-out of smart metering systems.

4.2.5. WPK 1.3: Securing emerging Technologies and Services

Desired Impact

- By 2016, 5 MS and 8 private stakeholders use ENISA's recommendations on smart cities in their corporate risk assessment and management approach.
- By 2016, 5 MS and 8 private stakeholders use ENISA's recommendations on big data in their corporate risk assessment and management approach.
- By 2016, 8 MS and 8 private stakeholders use ENISA's recommendations on Smart Home Environments in their corporate risk assessment and management approach.



Description of tasks

The objective of this work package is to develop good practices on emerging smart infrastructures[6] and services and work with relevant stakeholders to deploy them at an early stage of adoption.

The main areas of work of this work package are:

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

For each area ENISA will identify all relevant public and private stakeholders, engage them in working groups and jointly take stock of and analyse the current situation in terms of cyber security and resilience. The Agency will also identify EU and national funded projects on these topics, liaise with them, assess their findings and deliverables, and further engage them in the corresponding expert groups. Special emphasis will be given to the resilience and robustness of such smart infrastructure and services.

Based on the consultation with stakeholders and desk-top analysis and research, ENISA will develop good practices and issue recommendations addressing policy makers, developers and service providers. The aim of the reports is to provide smart infrastructure service providers and developers with good security and resilience practices when designing and deploying such services in order to minimise the exposure of such network and services to all relevant cyber threat categories. The early adoption of these recommendations and good practices will boost the trust and confidence of potential users of such infrastructures and pave the way for the wide deployment of them. In such a way ENISA will help the EU industry to become more competitive and innovative. Drawing from the knowledge and expertise on each area the Agency will issue recommendations to MS and EU Commission on additional measures, including RandD, needed to address specific aspects of these smart infrastructures and services.

Outcomes and deadlines

Based on the tasks described above, the following outcomes and deliverables are envisaged:

D1: Good Practices and Recommendations on the Security and Resilience of Intelligent transportation systems (Q4, 2015).

D2: Good Practices and Recommendations on the Security and Resilience of Big Data Services (Q4, 2015).

D3: Good Practices and Recommendations on the Security and Resilience of Smart Home Environments (Q4, 2015).

Stakeholder impact

- Identify NIS issues and challenges in the area the areas mentioned above.
- Develop good practices that stakeholders could use to either improve their current operations or dosing more secure systems and services.
- Issue targeted recommendations to policy makers and MS and work with them to address them in the most practical and cost effective way.

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

Resources

- (see chapter 4.14)

Legal base and policy context

- ENISA Regulation article 3, in particular 3.1.(c) (iii), development and exchange of best practice and 3.1.(d) on support for research and development.
- CIIP Action Plan 2009 and 2011.
- Digital Agenda 2010.
- European Strategy for Cyber Security.
- Council Resolution of 18 December 2009.
- Internal Security Strategy for the European Union.
- COM(2011) 202, Smart Grids: From innovation to deployment.
- COM Recommendations on preparations for the roll-out of smart metering systems.

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

Desired Impact

- Improve information flows between the CERT EU, ENISA and the CERT community.
- Provide timely information to stakeholders, e.g. CISO, CIO level, in a coordinated manner.

Description of tasks

The objective of this work package is to define and implement a framework that will allow the Agency to provide timely and high quality responses to NIS developments. In cases of NIS issues and occurrences that reach a certain level of public and media attention it is crucial, that the Agency can give sufficient information and, where appropriate, guidelines for dealing with the issue in very short time. Such guidelines will not address immediate response, but will concentrate on medium to long term preparatory measures. Also through ability to provide an ad-hoc news items with opinions and advice on relevant NIS issues (called "Flash Notes") the Agency will have a relevant and appreciated form of "added value by outreach".

For each area ENISA will identify relevant public and private stakeholders, engage them at the operational level making sure that the timing of the information flow meets their needs.

Over the last years ENISA's news items with opinions and advice on relevant NIS issues (called "Flash Notes") proved to be a relevant and appreciated form of "added value by outreach" for the Agency. It is ENISA's intention to continue to provide these notes as a reliable and continuous service to its stakeholders by identifying "Flash Notes" (to be renamed in the future "Info Notes") again as an explicit deliverable. The overall goal for each Note should be to highlight fundamental facts and shortcomings behind specific NIS issues and occurrences, to give advice to its key stakeholders (in accordance to the agencies' mandate) and to provide an independent and "calm" opinion.

Outcomes and deadlines

Based on the tasks described above, the following outcomes and deliverables are envisaged:

D1: Establish necessary procedures, workflows, tools, etc. to enable ENISA to carry out the Info Notes service (Q2/2015).

D2: Info Notes on a specific NIS issue (ongoing service with pilot from Q2/2014; conclusions on first year of activity in Q4/2015).

Stakeholder impact

The impact on stakeholders will be as follows:

- More effective information flows between the CERT EU, ENISA and the CERT community.
- Timely information provided to key stakeholders on NIS incidents and significant developments in the field.

Resources

- (see chapter 4.14)

Legal base and policy context

- ENISA Regulation article 3, in particular 3.1.(a), 3.1.(b)(vi), 3.1.(c)(iv) on assistance, on analysis, and of maintaining the awareness.

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

4.3.1. Overview

Justification

ENISA will work together with MS and EU institutions to assist them in capacity building across the EU. In particular, the Agency will work together with national bodies that have been mandated to carry out this task within the MS, with private sector representatives and with European Commission to ensure that the approach is coherent across the EU. In that respect ENISA will continue supporting national regulatory authorities (e.g. NRAs and DPAs) and the Commission in the harmonised implementation of EU regulations related to incident reporting across the EU. Such de-facto, bottom – up harmonisation based on good practices and guidelines will reduce the cost of operation of the private sector in the EU.

Where private sector capacity building is concerned, ENISA will continue to ensure that this is aligned with public sector objectives. The Agency will also assist industry in ensuring that capacity building efforts are correctly integrated into the organisational structures of the benefited organisations.

By supporting initiatives such as the EU cybersecurity month, the implementation of an NIS driving licence and MS' efforts to introduce NIS topics into educational for a at all levels, ENISA will contribute to increasing the level of participation of the EU citizen in activities aiming to improve the level of NIS throughout the Union.

In 2015, the European Cyber Security Month (ECSM) will be further developed. The ECSM'2015 organisation follows up on the actions required in order to translate into practice the principle of shared responsibility in NIS security, as stated in section 1.2 of the Cybersecurity Strategy: "All relevant actors, whether public authorities, the private sector or individual citizens, need to recognise this shared responsibility, take action to protect themselves and if necessary ensure a coordinated response to strengthen cyber security."

Specific Policy Context

Each work package description contains a section highlighting the specific policy context for the activities foreseen.

Overall Goals

ENISA will work together with MS and EU institutions to assist them in capacity building across the EU in terms of government, private sector and wider public sector. In particular the Agency will work together with national bodies (NRAs, CERTs, etc.) that have been mandated to carry out this task within the MS, with private sector representatives and with European Commission to ensure that the approach is coherent across the EU. The Agency will continue to support the Commission and the MS in the implementation of methods and tools for ensuring adequate privacy protection and adherence to EU Data Protection legislation. By supporting initiatives such as the EU cybersecurity month, the implementation of an NIS driving licence and MS' efforts to introduce NIS topics into educational for a at all levels, ENISA will contribute to increasing the level of participation of the EU citizen in activities aiming to improve the level of NIS throughout the Union.

4.3.2. Work Packages

The following work packages constitute this Strategic Objective:

WPK 2.1 – Assist in public sector capacity building

This Work Package aims at helping operational bodies and communities (namely CERTs, but other communities where appropriate) to develop and extend the necessary capabilities in order to meet the ever growing challenges to secure their networks.

WPK 2.2 – Assist in private sector capacity building

This WPK aims at helping private sector developing their capacities in the area of cyber security (e.g. in the area of Network and Information Security driving licence).

WPK 2.3 – Assist in improving awareness of the general public

This WPK aims at further developing ENISA's multi-stakeholder facilitation approach and public-private activities.

4.3.3. WPK 2.1: Assist in public sector capacity building

Desired Impact

- By 2017, 8 MS use ENISA's recommendations and good practices on National Cyber Security Strategies.
- By 2017, continued CERT training will be provided to a minimum of 20 participants of different organisations in 5 MS.
- By 2017, Improved operational practices of CERTs in at least 15 MS (on-going support with best practices development).
- More streamlined CERT exercise and training material with CERT and other operational communities' services and methodologies.

Description of tasks

This Work Package aims at helping the EU MS and other ENISA stakeholders, such as the EU bodies, to develop and extend the necessary capabilities in order to meet the ever growing challenges to secure their networks. A special emphasis in this WPK is laid on supporting operational bodies and communities (namely CERTs, but other communities where appropriate) by concrete advice (like good practice material) and concrete actions (like CERT training).

Part of the activities in this work package aim at maintaining and extending the collection of good practice in various areas of capability building: guidelines for national strategies and exercises, good practice collection and training material for operational communities like CERTs.

The Agency will support and advise MS on the development and implementation of National Cyber Security Strategies (NCSS) including identifying the key elements to consider, the most appropriate process to follow and the suitable assessment methods to adopt. The second big part is an active support of MS in capability building, namely by rolling-out training for IT specialists (CERTs, etc.) and supporting MS to carry out national exercises.

ENISA will continue supporting MS in the development of their capabilities in the area of national Public Private Partnerships. The Agency, building on its work in the area of PPPs and Trusted Information Sharing, will provide targeted and customised assistance (e.g. in a form of a seminar, training). ENISA will also continue supporting the Commission in the management of the NIS platform by engaging more targeted public and private stakeholders (especially experts from small industry players), assisting in the formation of virtual groups of experts, and contribute its expertise to position papers developed within the working groups of the NIS platform. The last component of this Work Package is planning forward by looking back: how successful have specific measures or even specific documents been in the past and throughout the year. The results of this on-going impact assessment will (in the spirit of multi-annual planning) support the development of ENISA Work Programmemes for future years.

Outcomes and deadlines

Based on the tasks described above, the following outcomes and deliverables are envisaged:

D1: Support and Advise Member States on the establishment and evaluation of National Cyber Security Strategies (NCSS) (Q4/2015).

D2: Assistance in National CERTS training and education (ongoing).

D3: Maintaining CERT good practice and training library (Q4/2015).

D4: Building upon the evaluation update ENISA's methods in CERT capacity building and propose a roadmap (Q4/2015).

D5: Impact evaluation on the usefulness of the ENISA guidelines on capacity building. (Q4/2015).

Stakeholder impact

National/Governmental and other CERTs and other operational entities will benefit from training and capability enhancement actions specially tailored for those communities.

Resources

- (see chapter 4.14)

Legal base and policy context

- ENISA Regulation, in particular Article 3.1.b and 3.1.c on capacity building and cooperation.
- Council Resolution on "A Collaborative European Approach to Network and Information Security" (2009/C 321/01).
- European Commission's Communication on "Critical Information Infrastructure Protection 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience'" (COM(2009) 149 final), esp. chapters 3.4.3, 5.1, 5.2 and 5.3.
- European Commission's Communication on "A Digital Agenda for Europe" (COM(2010) 245 final/2).
- European Commission's Communication on "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe" (COM(2010) 673 final).
- European Commission's Communication on "Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security'" (COM(2011) 163 final).

4.3.4. WPK 2.2: Assist in private sector capacity building

Desired Impact

- 10 public- private stakeholders from MS follow up on the recommendations from the Roadmap on the NIS in Education.
- Further develop an effective work process to involve more universities and certifications providers (NIS in Education).

Description of tasks

The EU Cyber Security Strategy "An Open, Safe and Secure Cyberspace" suggests the development of a roadmap for a "Network and Information Security driving licence" as a voluntary certification programme to promote enhanced skills and competence of IT professionals. Based on this requirement ENISA has carried out a consultation to involve the stakeholders and guide the drive for quality results released in late 2014 in a roadmap report. It describes pilot courses, comparative curricula analysis and the main message that e-skills and certifications are an essential path to follow.

ENISA is well equipped to further respond to this thematic challenge taking into consideration the brokerage achieved in the NIS environment for example with NIS in education for the last 4 years. The main objective of this work is to further provide brokerage services between stakeholders in order to implement the recommendations from the roadmap with emphasis in areas of work where ENISA is active already for a number of years and also where established collaborations with the academic community (e.g. NIS in education) exist. At the same time during 2014 ENISA has developed a quiz to test user's knowledge of ENISA recommendations. In the course of 2015 ENISA will continue to build upon this basis using the feedback received by the users.

ENISA will also support MS in their own decision making process, by providing advice and referencing the appropriate ENISA studies in the area. This will be done on an on-demand basis.

Outcomes and deadlines

Based on the tasks described above, the following outcomes and deliverables are envisaged:

D1: ENISA report "Status of Privacy and Network and Information Security course curricula in MSs" (Q4/2015).

D2: Further development of ENISA application "NIS self-assessment" (dissemination material) (Q4/2015).

D3: On-request support for MS decision making (Q4/2015).

Stakeholder impact

The direct beneficiaries of the results of this work package will be the policy makers, standardisation bodies and the end user organisations from public and private sectors, in particular in the area of EU NIS education.

Resources

- (see chapter 4.14)

Legal base and policy context

- ENISA regulation, article 3, particularly 3.1.(c)(v).
- Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace – JOIN(2013) 1 final – 7/2/2013 (Section 2.1).
- EC proposal for an NIS Directive.

4.3.5. WPK 2.3: Assist in improving awareness of the general public

Desired Impact

- Engage the 28 EU MS or representatives from the EU 28 MS for ECSM and general NIS messages for citizens.
- Collaboration, for better coordination, with at least 3 international stakeholders (ECSM).
- Engage at least 5 representatives from at least 3MSs in the development of basic cyber hygiene guidelines for recognizing and using trustworthy security and privacy products for the general public.

Description of tasks

In 2015, the European Cyber Security Month (ECSM) will be further developed following its basic principles, namely:

- Support the multi-stakeholder governance approach.
- Encourage common public-private activities.
- Assess the impact of activities, optimising and adapting to new challenges.

The ECSM'2015 organisation follows up on the actions required in order to translate into practice the principle of shared responsibility in NIS security, as stated in section 1.2 of the Cybersecurity Strategy: "All relevant actors, whether public authorities, the private sector or individual citizens, need to recognise this shared responsibility, take action to protect themselves and if necessary ensure a coordinated response to strengthen cyber security."

In addition, following the concept of shared NIS responsibility, ENISA will engage in 2015 in basic cyber hygiene by the development of guidelines that will allow the web users (general public) to recognize and use tools for online privacy and security. The ultimate scope will be the development of a citizens' web portal, listing existing up-to-date and trustworthy open source/freeware tools that will be easily applied by the non-expert user who wishes to protect himself/herself online (ex. in web browsing, email, instant messaging, e-payment systems, etc). The envisaged future deployment of such a portal will be a self-sustained platform of privacy tools supported, under ENISA's auspices, by a greater online community of privacy experts from different sectors (academia, Data Protection Authorities, NGOS, etc).

Outcomes and deadlines

Based on the tasks described above, the following outcomes and deliverables are envisaged:

D1: Provide guidance and support for European Cyber-Security Month (dissemination material, Q4 2015).

D2: Basic Cyber hygiene: guidelines for recognizing and using trustworthy security and privacy products for the general public (Q4/2015).

Stakeholder impact

The direct beneficiaries of the results of this work will be the EU citizens, targeted by different categories. ENISA's role will be to provide technical guidance on priorities and suitable subject matter and to promote stakeholder involvement. These stakeholders are expected to reap the following benefits:

- Receive targeted information on the security dimension in the use of ICTs.
- Develop knowledge and corresponding ICT skills by being part of a best practice sharing community.
- Improve and enhanced contacts with stakeholders of similar interests and profiles.

Resources

- (see chapter 4.14)

Legal base and policy context

- ENISA Regulation in particular 3.1.(c) (iv) and (v) supporting voluntary cooperation.
- ENISA Stakeholder Strategy.
- Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace – JOIN(2013) 1 final – 7/2/2013 (Section 2.1).

4.4. SO3 – To assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security

4.4.1. Overview

Justification

ENISA will continue to provide the Commission and the MS with high quality information, data and advice to support policy making having an EU dimension.

In the area of privacy and data protection, ENISA will help the Commission and MS to move the privacy and data protection debate towards implementation strategies and new business models, building on EU data protection laws. We will provide feedback to those working on the legislative framework as to what is feasible and what is not feasible from an operational perspective. The Agency will also identify existing methods and tools that could be used to implement the proposals of the regulation and suggesting which methods and tools could provide the best cost/benefit based on current operational experience. In addition, ENISA will identify 'gaps', where current methods and tools do not fulfil the requirements of the legal proposal.

Since its creation ENISA has tracked the development of standards in the area of Network and Information Security, maintaining close contacts and collaboration with International Standardisation Organisations. In 2015, the Agency will monitor NIS standards EU wide and globally. This approach enables ENISA to keep its activities up-to-date with the latest developments as well as informing its stakeholders on new NIS standardisation activities and to flag opportunities and/or risks as they develop. The collaboration with CSCG will continue, with an aim to improving the links between Standardisation Organisations in the area of NIS and industry and in particular EU SMEs.

Research and development will play a key role in deciding how successful the EU is in adapting to future NIS and cyber security challenges. ENISA will continue to support such efforts by acting in an advisory role to the Commission for future Frame Work Programmeme initiatives in this area. The strategic approach will be to assist the Commission in selecting projects that are both aligned with the policy framework and produce clear added value for the target stakeholder communities. ENISA will also continue to liaise with academia and to provide a bridge between academic communities and its own stakeholder communities. In the areas of interest to the ENISA Work Programme the Agency will continue to collaborate with and to support EU funded RandD projects (H2020). The main aim of this activity is to align the objectives of policy initiatives in the area of NIS and the relevant EU funded RandD projects (H2020).

Specific Policy Context

Each work package description contains a section highlighting the specific policy context for the activities foreseen.

Overall Goals

- ENISA will continue to provide the Commission and the MS with high quality information, data and advice to support policy making having an EU dimension.
- The Agency will also take into consideration policy and legislative requirements that are not directly related to cyber security, but which have a bearing on how cyber security principles are integrated.
- ENISA will continue to support research and development by acting in an advisory role to the Commission for future Frame Work Programmeme initiatives in this area.
- ENISA will work together with the public sector, standards organisations and industry representatives to identify ways for improving the process for agreeing on suitable NIS standards and for promoting their uptake in a cross-border environment.
- ENISA will continue its work on Privacy enhancing technologies.

4.4.2. Work Packages

The following work packages constitute this Strategic Objective:

WPK 3.1 – Provide information and advice to support policy development

This WPK aims at supporting work on regulation especially in the area of eID.

WPK 3.2 – Assist EU MS and Commission in the implementation of EU NIS regulations

This WPK aims at supporting EU MS in implementing regulation, especially in the area of reporting according to Article 13a of the Telecoms Directive.

WPK 3.3 – Assist EU MS and Commission in the implementation of NIS measures of EU data protection regulation

This WPK aims at supporting developing and implementing regulation in the area of Data Protection and Privacy.

WPK 3.4 – RandD, Innovation and Standardisation

This WPK aims at supporting work on Standardisation (i.e. collaborating with standardisation bodies) and Research and Development (especially in the area of H2020).

4.4.3. WPK 3.1: Provide information and advice to support policy development

Desired Impact

- Engage at least 5 key sector actors in launching and establishment of a forum that brings together 3 communities, namely: trust service providers from the EU Trusted List, conformity assessment bodies and supervisory authorities. The degree of activity of the relevant key sector actors in the forum is of importance to its success.
- Validations by at least 5 representatives from different MS of the contribution to the implementation of the Regulation on electronic identification and trusted services for electronic transactions.

Description of tasks

In order to remove existing barriers for cross-border e-ID based services, a new Regulation (914/2014) on electronic identification and trust services for electronic transactions in the internal market has been published on the 28th August 2014. ENISA has contributed to the work on its implementing measures. The new Regulation strengthens the provisions for interoperability and mutual recognition of electronic identification schemes across borders, enhances current rules for electronic signatures and provides a legal framework for other types of trust services.

ENISA has contributed to this area since 2013 by providing recommendations in the areas of:

- Mechanisms for reporting security breaches by the trust service providers to the competent bodies.
- Minimum security measures and good security practices for trust services providers.
- Common audit schemes for trust services providers in MS.

In 2015 ENISA will continue to support activities in this field by the following actions:

- Studying technological measures used by trust services.
- Review and verification against the Regulation 910/2014 of definitions used in the context of TSPs in other sources. This action will include clarification and specification of definitions used in the Regulation.
- Review and evaluation of the technologies and standards related to TSPs and eIDs (also developed under mandate M-460 and in frame of the new Regulation).

ENISA in collaboration with the Commission will also launch the creation of a forum that brings together 3 communities, namely: trust service providers from the EU Trusted List, conformity assessment bodies and supervisory authorities. A report on the establishment work of the forum of trust service providers, conformity assessment bodies and supervisory authorities will be included as a separate section in the report of WPK3.3 D3 of the APF'2015.

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

Outcomes and deadlines

Based on the tasks described above, the following outcomes and deliverables are envisaged:

D1: Analysis of standards related to eID and/or TSPs (Report, Q4/2015).

D2: Report analysing the terminology and definitions used by eIDAS (including recommended technological means used by TSPs) (Report, Q4/2015).

Stakeholder impact

- Supporting the implementation of the Regulation on electronic identification and trusted services, which will enable the achievement of a harmonized market.
- Supporting the EU MS on the provision of secure eGovernment services in all levels of public administration.

Resources

- (see chapter 4.14)

Legal base and policy context

- ENISA regulation article 3, in particular 3.1.(a), support the development of Union policy and law.
- Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace – JOIN(2013) 1 final, 7/2/2013.
- Regulation 910/2014 on electronic identification and trusted services for electronic transactions in the internal market.

4.4.4. WPK 3.2: Assist EU MS and Commission in the implementation of EU NIS regulations

Desired Impact

- By 2017, 12 MS make direct use of the outcomes of article 13 a work by explicitly referencing it or by adopting it at nationally level.
- By 2017, 10 MS implement recommendations by ENISA on implementing and enforcing article 4.
- By 2017, 10 MS implement ENISA's recommendations on article 15.

Description of tasks

This Work Package focuses on assisting regulatory authorities and Commission in the implementation of EU regulations related to incident reporting. It builds on successful work done in this area for several years namely in the area of article 13 a.

The main tasks of this Work Package are to support:

- NRAs and EU MS on the implementation of Article 13a (security breach notification) and article 4 (personal data breach notification) and the development of synergies among the two.
- NRAs and EU MS on the implementation of article 15 of new Regulation on electronic identification and trusted services (eIDAS).
- the Commission and MS on the implementation of the proposal for NIS Directive.

ENISA will continue collecting and analysing annual, national reports of security breaches from NRAs in accordance with Article 13a of the Framework Directive on electronic communications. The Agency, in co-operation with experts from NRAs and private sector (e.g. NIS Platform), will analyse the reports, compare them with previous years, identify good practices and lessons learnt and where needed make recommendations to NRAs and private sector to mitigate these threats in the future. Also the Agency will assess the impact of incident reporting schemes (mostly art 13 a and art 4) from technical and socio-economic point of view. ENISA will identify lessons learnt, evaluate the value for money of such schemes and issue recommendations for targeted stakeholders.

Additionally, ENISA will continue bringing NRAs, DPAs and the Commission together to agree on a harmonised implementation of the security and data breach articles (art. 13a and art. 4). In that respect the Agency will assess the two incident reporting schemes (article 13a and article 4), identify common elements (e.g. parameters and thresholds) and propose to NRAs and DPAs the most harmonised and cost efficient way of implementing the two articles avoiding at the same time potential overlaps. A harmonised implementation of these articles will simplify the internal business processes of the affected private sector and reduce the cost of compliance to them.

ENISA has already contributed to the area of electronic identification and trusted services (eIDAS) by providing recommendations on incident reporting by the trust service providers to the competent bodies. In 2015, ENISA will continue its efforts to bring together all relevant stakeholders from MS including the competent regulatory bodies of MS and debate with them on the development of a consistent implementation scheme/framework of article 15 and relevant minimum security measures. The Agency will build on the work of FESA and relevant standardisation bodies (e.g. ETSI) and will expand it to cover all relevant stakeholders. This work with ENISA's support will properly define the scope of incident reporting,

the parameters and thresholds as well as the affected services. It will also consider the requirements of Article 7a of the eIDAS Regulation. The Agency will also try to exploit all possible implementation and conceptual synergies with article 13a and article 4.

Subject to the approval of the NIS Directive, ENISA can assist the Commission and MS in the implementation of the NIS Directive. In areas where the Agency is called for to take action it can develop the constituency, debate about the scope and the key objectives of the actions, identify the key elements and players to engage and facilitate in the implementation of the next steps by always leveraging existing knowledge and expertise (e.g. incident reporting, minimum security measures, NCSS, exercises, etc.)

Outcomes and deadlines

D1 – Analysis of Annual 2014 Incident Reports (report) (Q3, 2015).

D2 – Recommendations on addressing root causes of specific incidents (report) (Q3, 2015).

D3 – Guidelines on Minimum Security Measures for Trusted Service Providers[7] (workshops, report) (Q4, 2015).

D4 – Impact assessment on the effectiveness of incident reporting schemes (e.g. Art13a and Art 4); (Q4, 2015).

D5 – Guidelines on Incident Reporting Scheme for Article 15 (report, Q4 2015).

Stakeholder impact

Telecommunications Sector

- NRAs, DPAs and the EDPS will have practical references and technical guidelines to implement the legislation.
- Within the area of Article 13a, the industry, NRAs and the European Commission will be able to develop a better understanding of the significant incidents at European level as well as a comparison with earlier years and recommendations, which will support mitigation decisions and actions.
- EU Commission (DG CONNECT, HOME and JUSTICE) will achieve harmonization of incident reporting, breach notifications and security measures, following international standards and can in this way forego further detailing of the legislative text.
- Industry (network providers, ISPs, cloud providers, etc.) will be able to adopt a single framework of incident reporting/breach notification and security measures, so there is a level playing field across the EU countries and no complications for working cross borders.

Regulation on electronic identification and trusted services

- NRAs and DPAs will be able to implement an efficient reporting scheme very similar to the Article 13a scheme currently in place, and in this way lay the basis for a coherent and holistic picture of security incidents across key service providers.

A single reporting scheme will allow trust service providers to more easily operate across borders, effectively paving the road for a single market of trust service providers across the EU. In turn this facilitates cross border online services, such as eCommerce and eGovernment.

7 In the next years work in this area will be extended to other market actors (in relation to the proposal for NIS Directive);

Resources

- (see chapter 4.14)

Legal base and policy context

- ENISA Regulation article 3, in particular art. 3.1.(a), 3.1.(b) on capacity building and 3.1.(c).
- Cybersecurity Strategy of the European Union Council Resolution of 18 December 2009.
- CIIP Action Plan 2009 and 2011.
- Internal Security Strategy for the European Union.

4.4.5. WPK 3.3: Assist EU MS and Commission in the implementation of NIS measures of EU data protection regulation

Desired Impact

- At least 5 representatives from different MSs contributing to ENISA guidelines and best practice recommendations regarding Privacy Enhancing Technologies.
- At least 10 actors in the field validating the results of the studies.
- More than 80 participants in APF'15 (researchers, policy makers and industry participants).

Description of tasks

In 2015, ENISA will intensify its efforts in the field of privacy and trust. The approach is three-fold:

Firstly, based on the outcome of the best practice guide for privacy enhancing technologies in 2014, the readiness of the industry, as well as the public and private sectors for the adoption and evolution of privacy technologies will be analysed. This will help to understand why in the current practice of web services PETs are rarely used. Special attention will be paid to technologies for data minimization that still allow for complex business models, e.g., privacy enhanced location based services. The report will study the technical possibility as well as economic incentives which could help further market penetration of such services.

Secondly, privacy enhancing technologies are mentioned in several policy documents, e.g., the draft data protection regulation proposal. They are based on complex cryptographic building blocks. The security of these building blocks is constantly challenged by new attacks. Furthermore, new building blocks are invented by the research community. For system developers it is hard to keep track with this development. In the past ENISA provided recommendations for algorithms and parameters of such building blocks. ENISA will, in its work in this field, point to already established EU policies and processes.

Thirdly, emerging technologies in the areas of online information sharing, data merging and data mining create new possibilities for the processing of personal data and, thus, new privacy risks. To this end, ENISA will provide a state-of-the art analysis of the data protection threats, risks and protection measures in the emerging big and open data landscape exploiting, as in the past, synergies between security technologies and data protection. Data protection legislation more and more mentions technological protection

mechanisms. The policy makers are partially aware of protection mechanisms whereas the research community might lag on requirements legislation. ENISA will bring together policy makers, researchers and data privacy practitioners to debate about the challenges of data protection and privacy. This would be in the form of the third annual privacy forum.

In 2014 ENISA produced a report entitled "Indicative list of appropriate cryptographic protection measures" aiming to support the Commission publication of an indicative list of measures in the light of Article 4 of the EC regulation 611/2013. This report will be used by the Commission as a main reference document for the publication of a list of appropriate technological protection measures pursuant to Article 4(3) of Commission Regulation (EU) No 611/2013 (hereinafter referred to as the "List"). Based on the latest scientific evidence at the moment of publication, technological breakthroughs may occur that compromise the recommended protection measures. Therefore it is important that ENISA performs an annual review of the aforementioned report with a view, among others, to keep the list up to date, pointing to already established EU policies and processes. Such a report should serve as a reference material, with technical protective measures for personal data, for the interested reader at MS level or in private sector. As was the case in previous years, in the context of this work ENISA will collaborate with well recognised experts in the field (also ensuring high quality peer reviews). In addition, ENISA will involve experts in the fields from National Authorities (BSI, ANSSI, etc.).

Outcomes and deadlines

Based on the tasks described above, the following outcomes and deliverables are envisaged:

D1: Readiness analysis for the adoption and evolution of privacy enhancing technologies (Q4 2015).

D2: Building blocks for PETs update (Q4 2015).

D3: Annual Privacy Forum 2015, APF'2015 (Q4 2015).

D4: State-of-the-art analysis of data protection in big data architectures (Q4 2015).

D5: 2015 edition of the annual report on 'Indicative list of appropriate cryptographic protection measures' (Q4 2015).

Stakeholder impact

- Supporting the development of clear guidelines for service provider in the light of the new data protection Regulation in close collaboration with DPAs, NRAs, Article 29 and EDPS, European Commission (DG JUS, DG CONNECT and DG HOME), covering topics such privacy seals, personal data protection – data security, etc.
- Supporting the implementation of digital agenda, data protection Regulation for Industry Providers (network operators, service providers) etc.
- Harmonisation of practices regarding data security and data protection across MS and service providers (i.e. minimum security requirements).

Resources

- (see chapter 4.14)

Legal base and policy context

- ENISA regulation article 3, in particular 3.1.(a)(ii) and (iii) as well as 3.1.(e) addressing data protection issues.
- Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace – JOIN(2013) 1 final, 7/2/2013, available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667.
- 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 on privacy and electronic communications" online: https://ec.europa.eu/digital-agenda/en/eprivacy-directive-data-breach-notifications.
- 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.

4.4.6. WPK 3.4: R&D, Innovation and Standardisation

Desired Impact

- Support at least 10 key sector actors involved in EU funded R&D programs (H2020) in the area of NIS in defining priorities.
- Engage at least 5 MS representatives from at least 3 MSs in the work of the ETSI CEN CENELEC Cyber Security Coordination Group (CSCG).
- Engage at least 5 MS representatives through at least 1 workshop organized in collaboration with the research (H2020) and standardization communities.

Description of tasks

Since its creation ENISA tracks the development of standards in the area of Network and Information Security maintaining close contacts and collaboration with International Standardisation Organisations. In 2015, the Agency will monitor NIS standards EU wide and globally. This approach enables ENISA to keep its activities up-to-date with the latest developments as well as informing its stakeholders on new NIS standardisation activities and to flag opportunities and/or risks as they develop.

Since 2012 ENISA contributes actively to the creation and work of the ETSI CEN-CENELEC Cyber Security Coordination Group (CSCG). This collaboration with CSCG will continue and ENISA will try to further exploit synergies between CSCG and its Work Programmeme. The Agency will also involve standards bodies in the different work packages in as far as this is appropriate. In the context of the CSCG activities one of the areas that further work is required is in improving the links between Standardisation Organisations in the area of NIS and industry and in particular EU SMEs. ENISA will work in 2015 in identifying core set of cybersecurity standards (comparing it against the relevant NIS policy developments).

In the areas of interest to the ENISA Work Programme the Agency will continue to collaborate with and to support EU funded R&D projects (H2020). The main aim of this activity is to align the objectives of policy initiatives in the area of NIS and the relevant EU funded R&D projects (H2020). Such collaboration may be in the form of:

- Participation in the panel of reviewers that are supporting the Commission in reviewing the progress of a project and steering the project's future work.
- Participation in the advisory/steering board of selective projects accepted by the Commission for funding. Obviously ENISA may contribute to only a small number of projects. In this context, emphasis will be given to the areas of important to the ENISA Work Programme as presented in this document.
- Contributions to the various consultations launched by the Commission in the areas of interest to ENISA. Such consultations may be conducted in the context of setting the research priorities for future calls for proposals or in the context policy initiatives launched or about to be launched by the Commission.

As was the case in previous years, ENISA will continue to support the Commission by providing experts at the evaluations of the calls of proposals that are published in the context EU funded R&D programs. In this context, emphasis will be given to the areas of important to the ENISA Work Programme as presented in this document. It should be envisaged that ENISA may contribute up to 2 experts for the evaluation of calls of proposals during 2015.

Outcomes and deadlines

Based on the tasks described above, the following outcomes and deliverables are envisaged:

D1: Good Practice Guide for aligning Policy, Industry and Research (Q4/2015).

D2 Standardisation Gaps in Cyber Security (Q4/2015).

D3: Guide to standardisation for the SME Community (Q4 2015).

Stakeholder impact

The direct beneficiaries of the results of this work package will be the policy makers, frame Work Programmes of EU funded RandD, standardisation bodies and the end user organisations from public and private sectors, in particular in the areas of:

- Standardisation related to NIS, Privacy, Cloud Computing and Smart Grids.
- Harmonisation of EU funded research and policy initiatives.

Resources

- (see chapter 4.14)

Legal base and policy context

- ENISA regulation, article 3.1.(d) support research and development and standardisation.
- COUNCIL RESOLUTION, 18/12/ 2009, on a collaborative European approach to Network and Information Security, (2009/C 321/01)40. In this resolution the Council recognises the potential role of ENISA to build a NIS scenario in Europe. It also underlines that the major goals of NIS are to support:
  - Security standards.
  - Raise awareness and good practices and guidance.
  - Serve as EU Centre of expertise in EU related Network and Information Security matters.
- Commission proposes Action Plan to enable further growth of Security industry37 COM(2012) 417: The COM has produced a "COMMISSION STAFF WORKING PAPER on Security Industrial Policy"38 SWD(2012) 233 final, and "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE"39 COM(2012) 417 final. The Commission proposes to create a true internal market for the security industry by inter alia:
  - harmonising standards and certification procedures for security technologies.
  - introducing checks on the societal impact of new security technologies at the research stage. To reduce the gap between research and market, especially in European and international procurement, the Commission will use novel funding schemes foreseen in Horizon 2020 such as Pre-commercial Procurement, to test and validate results stemming from EU security research projects. This approach should unite industry, public authorities and end users from the beginning of research projects. Border security and aviation security are the most promising areas.
  - novel funding schemes such as Pre-commercial Procurement to test and validate results stemming from EU security research projects.
  - The priority will be to overcome fragmentation of the EU security market, by harmonising standards and certification procedures for security technologies. European standardisation organisations will be asked to establish concrete and detailed standardisation roadmaps on the next generation of technologies. In this context, to achieve mutual recognition of certification systems, the Commission intends to issue two legislative proposals, to establish an EU wide harmonised certification system for airport screening (detection) equipment, and an EU wide harmonised certification system for alarm systems.
  - The Commission will introduce checks on the societal impact of new security technologies at the research stage. In addition, the Commission will issue a mandate to European standardisation organisations to develop a standard for the integration of privacy issues, from design to production process phases.

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

4.5.1. Overview

Justification

The work packages in this area are designed to enhance cooperation between MS and NIS communities. ENISA will continue in its efforts to build up targeted NIS communities to meet policy goals. In some cases (e.g. The NIS Platform, as referenced by the EU Cyber Security Strategy), ENISA will support other institutions in creating such communities, whilst in other areas it will seek to build such communities itself when requested to do so by the Commission or the MS.

In the area of exercises, ENISA continues to support the MS in 'learning by doing'. Since the inception of this stream of work in 2010 the pan-European exercise has moved to increasing levels of sophistication. In 2015 ENISA will facilitate the planning of the next pan European Cyber Exercise efforts, initiating the planning process for Cyber Europe 2016 and organising focused exercises, such as communications checks etc. In addition, the Agency will further enhance its methodology, seminars, trainings and technical capabilities on the organisation and management of large-scale cyber crisis exercises.

Specific Policy Context

Each work package description contains a section highlighting the specific policy context for the activities foreseen.

Overall Goals

- ENISA will continue in its efforts to build up targeted NIS communities to meet policy goals. In some cases (e.g. The NIS Platform, as referenced by the EU Cyber Security Strategy), ENISA will support other institutions in creating such communities, whilst in other areas it will seek to build such communities itself when requested to do so by the Commission or the MS.
- ENISA will build on the work it has carried out in the area of the pan-European exercise, the EU-US exercise and support of the TRANSITS training in the area of CERTs in order to build communities through a 'learn by doing' approach.

4.5.2. Work Packages

The following work packages constitute this Strategic Objective:

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

This WPK aims at leveraging on the positive experience of ENISA in supporting CERTs, the CERT communities and Law Enforcement communities to come up with mutually satisfactorily ways to collaborate in NIS.

WPK 4.2 – European cyber crisis cooperation through exercises

This WPK seeks to facilitate the planning of the next pan European Cyber Exercise in 2015-2016. ENISA will further enhance its methodology, training outreach and technical capability to organise large-scale cyber crisis exercises.

4.5.3. WPK 4.1: Support for EU cooperation initiatives amongst NIS–related communities in the context of the EU CSS

Desired Impact

- At least 2 new operational communities will be identified and contacted for the purpose of identifying a mutually satisfactory ways to collaborate (CERTs, LEA, EU Financial service, Data Protection, CIIP community, etc.)
- By 2016, at least 15 MS are familiar with practices in addressing different sector regulation challenges of managing cyber security issues.

Description of tasks

This WPK deals with leveraging on the good experiences ENISA made in supporting the CERTs, the CERT communities and Law Enforcement communities to find mutually satisfactory ways to collaborate.

ENISA will develop and provide guidance based on best practice for cooperation between key stakeholder communities (CERTs, CIIP community, Law Enforcement, Financial Services; Data Protection, etc.). The Agency will continue its work and support of the TRANSITS training in the area of CERTs in order to build communities through a 'learning by doing' approach. ENISA will also continue to support the collaboration between CERT and law enforcement communities, based on the recent policy and technical developments in this area in MS. This work will include a close collaboration with other institutions which are active in this field, namely the EC3. Activities agreed upon in the collaboration agreement between ENISA and EC3 will be further developed, for example in the area of encouraging more operational and systematic flows of information between CERTs and law enforcement communities, the exchange of specific knowledge and expertise, elaboration of general situational reports, reports resulting from strategic analyses and best practice, strengthening capacity building through training and awareness raising in order to safeguard network and information security at EU level. For better coordination and in order to avoid overlaps ENISA will stay engaged in the EC3 programme board. The very well established, commonly organised ENISA-EC3 workshop will be continued.

To achieve this, previous work will be leveraged (where applicable) and experiences made will be used to reach out to other communities, for the purpose of supporting CERTs to collaborating with them, and helping them build up their capabilities. Emphasis will be given to the cross border collaboration aspects.

Where possible, synergies with other ENISA collaboration- and community-supporting efforts like the NIS platform will be extended and, where needed, developed.

Outcomes and deadlines

Based on the tasks described above, the following outcomes and deliverables are envisaged:

D1: Develop and provide guidance based on best practice for cooperation between key stakeholder communities (Trust building for and reaching out to new communities) (CERTs, CIIP community, Law Enforcement, Financial Services; Data Protection, etc.) (Q4/2015).

D2: Identify practices of Member States in addressing different sector regulation challenges of managing cyber security issues (Q4/2015).

Stakeholder impact

The direct beneficiaries of the results of this Work Programmeme will be CERTs and Member States' policy makers, LEA units and other operational communities' IT managers.

The benefits that they will get are capability enhancement actions specially tailored for those communities. A special emphasis shall be put on supporting the EU Cyber Crime Centre, and on cross-border collaboration aspects.

Resources

- (see chapter 4.14)

Legal base and policy context

- ENISA Regulation, in particular Article 3.1.a-c on development of EU policy and law as well as capacity building and cooperation.
- Council Resolution on "A Collaborative European Approach to Network and Information Security" (2009/C 321/01).
- European Commission's Communication on "Critical Information Infrastructure Protection 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience'" (COM(2009) 149 final), esp. chapters 3.4.3, 5.1, 5.2 and 5.3.
- European Commission's Communication on "A Digital Agenda for Europe" (COM(2010) 245 final/2), esp. chapter 2.3.
- European Commission's Communication on "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe" (COM(2010) 673 final), esp. objective 3.
- European Commission's Communication on "Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security'" (COM(2011) 163 final).
- European Council, "The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens" (2010/C 115/01), e.g. par. 2.5. (Protecting citizen's rights in the information society), 4.2.3. (Mobilising the necessary technological tools), and 4.4.4. (Cyber crime).
- Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.
- European Commissions' Communication on "Towards a general policy on the fight against cyber crime", COM(2007) 267 final.
- European Commission's Communication on 'Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre', COM(2012) 140 final.

4.5.4. WPK 4.2: European cyber crisis cooperation through exercises

Desired Impact

- At least 25 EU MS and EFTA countries confirm their support for pan European Cyber Exercises.
- At least 25 MS are familiar with and use the cross border cyber crisis EU Standard Operational Procedures by 2016.

Description of tasks

This work package focuses on the following topics:

- Pan-European cyber exercises management (Cyber Europe and EuroSOPEx).
- Enhance the capacity to support and organise cyber exercises.
- Promote maintain and improve EU cyber crisis cooperation plans and procedures (e.g., EU SOPs), including bringing closer the cyber crisis cooperation community.

Pan-European cyber-exercises management

In 2014, ENISA organised the third pan-European cyber exercise, Cyber Europe 2014 (CE2014) was more ambitious than previous efforts, e.g., technical depth, scenarios, stakeholders involved, objectives, procedures to be tested, complexity etc. The exercise lasted until the end of 2014. In 2015 ENISA will perform an in depth analysis of the evaluation data gathered from the exercise. This will result in the detailed evaluation report that will be shared with the participating countries.

In addition, in 2015 ENISA will facilitate the planning of the next pan European Cyber Exercise efforts, initiating the planning process for Cyber Europe 2016 and organising focused exercises, such as communications checks etc. The lessons learned from CE2014 will help to draw the roadmap for the next exercise Cyber Europe 2016.

Enhance the capacity to support and organise cyber exercises

ENISA will further enhance its methodology, seminars, trainings and technical capabilities on the organisation and management of large-scale cyber crisis exercises.

The Agency will continue enhancing its capabilities for managing complex, distributed exercises, by building on previous efforts in tools and methods and by facilitating strategic partnerships. The maintenance and improvement of the Cyber Exercise Platform (CEP) will be one of the main tasks.

EU-US cyber security exercise

In 2014 ENISA supported the Commission and the MS in their efforts towards planning an EU-US cyber security exercise. The effort was focused mainly on exploratory discussions between involved parties: the Commission, EU MS and the US.

In 2015, ENISA will continue to support the efforts in the area of pan-European exercises and will prepare initial background work analysing the options for a potential EU-US cyber exercise that would be proposed at EU political level and submit to the ENISA Management Board for decision. ENISA will follow up to any decision taken by its Management Board and facilitate the actual planning of the exercise with representatives (planners) from the involved parties (EU MS and US). If the exercise is decided by the Management Board, after it is conducted ENISA will support the production of an after-action report.

Promote, maintain and improve EU cyber-crisis cooperation plans and procedures (e.g., EU SOPs), including bringing closer the cyber crisis cooperation community

ENISA will continue to support MS in the maintenance and training of operational procedures for cyber crisis cooperation. ENISA will analyse the EU cross border cyber crisis cooperation procedures and plans, given the inputs from previous efforts, such as cyber exercises, reports such as the work of the ECCCF working group, etc. Also ENISA will continue to consult with all EU MS on the actions, plans and tools needed for improving the cross border cooperation and will also propose mechanisms for a possible implementation, closely involving MS.

ENISA will continue the effort to bring the cyber crisis cooperation community closer in order increase the trust building the potential synergies. To that end in 2015 ENISA will organise the next event in the series of the International Conferences on Cyber Crisis Cooperation and Exercises.

Outcomes and deadlines

D1 – Evaluation Analysis and Actions from CE2014 (restricted report) (Q2/2015).

D2 – Pan European Cyber Exercises Roadmap for CE2016 (restricted report) (Q4/2015).

D3 – EU-US Cybersecurity Exercise after-action Report[8] (public/restricted report) (Q4/2015).

D4 – Evaluation and recommendations for improved communication procedures between EU Member States (public/restricted report) (Q4/2015).

Stakeholder impact

The direct beneficiaries of the results of this Work Programmeme will be:

- EU and MS' National Cyber Security Agencies, Cyber Crisis Management Units, National Cyber Crisis Structures and Partnerships:
  - Assess the current level of preparedness for large-scale events and cooperation capacities.
  - Develop an overview of pan European and International efforts in the area.
  - Obtain input, insights and recommendations for future actions in policy and technical measures.
- EU Commission:
  - Obtain insight and expert basis for current and future policy efforts in: cyber crises cooperation, contingency plans, cyber exercises and other areas related to the EU Cybersecurity Strategy.
- Private sector:
  - Obtain input on current level of internal preparedness for large-scale events and inter-operator cooperation as well as public-private sector cooperation and coordination.
  - Obtain insights on which requirements future actions may bring in the area of preparedness measures and continuity planning.

Resources

- (see chapter 4.14)

Legal base and policy context

- ENISA Regulation Article 3.1.b and 3.1.c.
- Cybersecurity Strategy of the European Union Council Resolution of 18 December 2009.
- CIIP Action Plan 2009 and 2011.
- Internal Security Strategy for the European Union.

8 ENISA will do all the necessary background work to prepare a proposal analysing the options for a potential EU-US cyber exercise and submit to the MB for decision. ENISA will follow up to any decision taken by its Management Board and facilitate the actual planning of the exercise with representatives (planners) from the involved parties (EU MS and US).

4.6. Management Board, Executive Board and PSG Secretariat

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

For the MB, ordinary meeting will be organised during 2015 and informal meetings will be held, one with the PSG, if appropriate. The existing electronic newsletter will be continued throughout 2015, as will support for the MB Portal. For the PSG also, two formal meetings will be organised.

For the Executive Board, formal meetings will be organised during 2015.

ENISA will continue to explore additional ways of supporting the Agency's statutory bodies in the most effective way, including the possible use of new technologies and modifications to existing processes as required.

4.7. National Liaison Officer Network

Since 2014, ENISA has initiated a number of activities with the aim to strengthen cooperation within the National Liaison Officers' (NLO) Network. NLOs are key actors for the Agency's daily work and interaction, assuring in terms of outreach effective liaison to the MS and dissemination of ENISA activities. It expands the NLO-Network with contact points from governmental and public agencies/organisations (e.g. CERTs and Regulatory Bodies/Agencies, etc.).

In 2015, ENISA will build upon these efforts and improve its cooperation with the NLO Network, the first Point of Contact for ENISA in the MS. In particular, the Agency will continue working on the following actions:

- An NLO meeting will be organised (possibly in conjunction with a MB meeting) where possible improvements of the collaboration will be discussed.
- Information will be send to the members of the NLO network at regular intervals on upcoming ENISA project related tenders, vacancy notices, and events organised by ENISA or where the Agency contributes to (for example co-organiser, etc.).
- Organisation of at least one Ad hoc meeting on a specific topic of interest that will be identified in collaboration with the NLOs.
- Maintaining an information dbase containing all relevant information on active ENISA project (e.g. unit responsible for the project, relevant tender results, etc.).

4.8. EU Relations

The Agency will carry out the bulk of its EU relations work with the statutory stakeholders; Commission, EU Parliament, Council (working groups) and MS, by using senior management for developing relations. This approach will take due account of the management structure of the Agency so that the level of participation in any particular meeting is appropriate. A similar approach is taken for speaking engagements.

In general, contacts at the highest level will be managed by the ED with the Heads of Department as backups depending on the subject to be discussed.

4.9. Corporate Communication

To be effective, ENISA needs to communicate the findings and recommendations of its documented output to a wide range of stakeholders across Europe. In 2015, the focus of corporate communications will be on increasing the outreach and impact through media relations, agency branding, marketing advocacy, and web communications, to help ensure that ENISA's work reaches the right audiences and has a real impact in making Europe's information society even more secure.

In addition to its annual High Level Event in Brussels, the Agency will continue to progressively build digital relations with all EU MS relevant authorities, as to make the cooperation even closer in terms of communicating results across Europe, and being a hub of exchange of the latest reports that are useful for other EU MS.

The Agency will continue developing various tools and channels such as info graphics, the web site, social media, and social networking, videos.

4.10. Dissemination activities

Dissemination activities are the responsibility of the project managers, who will work closely with the NLO contact point and the spokesman.

4.11. Quality Management System and Project Office

The Quality Management System (QMS) of the Agency aims at responding to a mix of regulatory and stakeholder requirements in an effort to improve organisational performance and compliance. Scheduled annual activities associated with the promulgation and maintenance of standard operating procedures (SOP) and a methodology, support the operational processes of the Agency. The primary goal of the QMS is to improve performance across the Agency, while reducing operational costs and enhancing stakeholder satisfaction. The methodology is based on the Plan-Do-Check-Act (PDCA) cycle, and it features SMART goals and KPIs. Change management is carried out by the process owners and the Quality Control Advisor.

In 2015 the Agency will re-engineer selected operational processes, align organisational requirements with actual implementation and pursue process improvements across the board. Measuring the performance of recently designed processes, e.g. the ENISA Project Management Guide, for the purpose of proposing suitable adjustments will be a priority. A risk assessment methodology will be implemented for Agency-wide risks. A set of tools such as electronic signatures, electronic workflows and enterprise resource management tools are likely to be further integrated to facilitate collaboration. Regular presentations and updates are made available to provide guidance and promote the performance of the quality management system.

ENISA will also create a project office in COD in order to better coordinate the increasing number of activities that cut across a number of operational areas within the Department. Such activities include the preparation of briefings on global issues and coordinating the coherence of recommendations across the Department.

4.12. Article 14 Requests

Article 14 requests are a mechanism that allow the MS or EU institutions to make direct requests to ENISA for carrying out particular activities. This mechanism has become increasingly popular in the last few years and has grown in significance to the extent that the Agency believes that it needs to be explicitly planned for in the annual Work Programmeme.

Although, by definition, it is not possible to predict the exact nature of the requests that the Agency will receive in 2015, based on past experience the allocated resources are indicated in chapter 4.14.

4.13. Data Protection Officer

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

1. inform and advise ENISA of its obligations pursuant to Regulation 45/2001/EC and to document this activity and the responses received
2. monitor the implementation and application of ENISA's policies in relation to the protection of personal data
3. monitor the implementation and application of Regulation 45/2001/EC at ENISA, including the requirements for data security, information of data subjects and their requests in exercising their rights under the Regulation, as well as the requirements for prior check or prior consultation with EDPS
4. monitor the documentation, notification and communication of personal data in the context of ENISA's operations
5. act as ENISA's contact point for EDPS on issues related to the processing of personal data; to co-operate and consult with EPDS whenever needed.

4.14. Summary of core operational activities[9]

Core Operational Activities: Strategic Objectives 14		Operational Activities – FTE	Total Cost of Activities ABB
SO1	**To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network and Information Security (NIS)**		
WPK 1.1	NIS Threats Analysis	2,3	245.806
WPK 1.2	Improving the Protection of Critical Information Infrastructures	6,6	688.253
WPK 1.3	Securing emerging Technologies and Services	5,3	486.603
WPK 1.4	Short- and mid-terms sharing of information regarding issues in NIS	2,7	183.301
Total SO 1		**16,8**	**1.603.963**
SO2	**To assist the Member States and the Commission in enhancing capacity building throughout the EU**		
WPK 2.1	Assist in public sector capacity building	6,6	788.253
WPK 2.2	Assist in private sector capacity building	2,4	185.971
WPK 2.3	Assist in improving awareness of the general public	2,0	167.476
Total SO 2		**11,0**	**1.141.700**
SO3	**To assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security**		
WPK 3.1	Provide information and advice to support policy development	2,7	233.301
WPK 3.2	Assist EU MS and Commission in the implementation of EU NIS regulations	5,3	506.603
WPK 3.3	Assist EU MS and Commission in the implementation of NIS measures of EU data protection regulation	4,0	404.952
WPK 3.4	RandD, Innovation and Standardisation	2,7	248.301
Total SO 3		**14,6**	**1.393.157**
SO4	**To enhance cooperation both between the Member States of the EU and between related NIS communities**		
WPK 4.1	Support for EU cooperation initiatives amongst NIS-related communities in the context of the EU CSS	4,6	439.777
WPK 4.2	European cyber crisis cooperation through exercises	6,0	617.428
Total SO 4		**10,6**	**1.057.205**

9 Remark: Full time equivalents (FTE) and costs of activities are reported on Activity Based Budget basis – see section 5.5

Horizontal Operation Activities			
Stakeholder Relations, Corporate Communication, Project Support Activities		**Operational Activities – FTE**	**Total Cost of Activities ABB**
SR1	MB and PSG Secretariat	1,3	271.651
SR2	National Liaison Officers Network	0,7	77.825
SR3	EU Relations	0,7	45.825
SR4	Stakeholders Communication	1,3	91.651
CC1	Corporate Communication	1,3	329.651
PS1	Quality control and Project Office	7,3	735.079
PS2	Article 14 requests	0,7	45.825
PS3	Data Protection Officer	0,7	45.825
Total		**13,9**	**1.643.332**

Total Operational Activities	**67,0**	**6.839.357**

4.15. Summary of core operational activities with deliverables

SO1	To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network and Information Security (NIS)
WPK 1.1	**NIS Threats Analysis**
D1	Annual Threat Analysis/Landscape Report (Q4/2015)
D2	Risk Assessment on two emerging technology/application areas (Q4/2015)
WPK 1.2	**Improving the Protection of Critical Information Infrastructures**
D1	Stock Taking, Analysis and Recommendations on the protection of CIIs (Q3/2015)
D2	Methodology for the identification of Critical Communication Networks, Links, and Components (Q4/2015)
D3	Analysis of ICS-SCADA Cyber Security of Devices in Critical Sectors (Q4/2015)
D4	Recommendations and Good Practices for the use of Cloud Computing in the area of Finance Sector (Q4/2015)
D5	Good Practices and Recommendations on resilience and security of eHealth Infrastructures and Services (Q4/2015)
WPK 1.3	**Securing emerging Technologies and Services**
D1	Good Practices and Recommendations on the Security and Resilience of Intelligent transportation systems (Q4/2015)
D2	Good Practices and Recommendations on the Security and Resilience of Big Data Services (Q4/2015)
D3	Good Practices and Recommendations on the Security and Resilience of Smart Home Environments (Q4/2015)
WPK 1.4	**Short- and mid-term sharing of information regarding issues in NIS**
D1	Establish necessary procedures, workflows, tools, etc. to enable ENISA to carry out the Info Notes service (Q2/2015)
D2	Info Notes on a specific NIS issue (ongoing service with pilot from Q2/2014; conclusions on first year of activity in Q4/2015)

SO2	To assist the Member States and the Commission in enhancing capacity building throughout the EU
WPK 2.1.	**Assist in public sector capacity building**
D1	Support and Advise Member States on the establishment and evaluation of National Cyber Security Strategies (NCSS) (Q4/2015)
D2	Assistance in National CERTS training and education (ongoing)
D3	Maintaining CERT good practice and training library (Q4/2015)
D4	Building upon the evaluation update ENISA's methods in CERT capacity building and propose a roadmap (Q4/2015)
D5	Impact evaluation on the usefulness of the ENISA guidelines on capacity building. (Q4/2015)
WPK 2.2.	**Assist in private sector capacity building**
D1	ENISA report "Status of Privacy and Network and Information Security course curricula in MSs" (Q4 2015)
D2	Further development of ENISA application "NIS self-assessment" (dissemination material, Q4 2015)
D3	On-request support for MS decision making (Q4/2015)
WPK 2.3.	**Assist in improving awareness of the general public**
D1	Provide guidance and support for European Cyber-Security Month (dissemination material, Q4 2015)
D2	Basic Cyber hygiene: guidelines for recognizing and using trustworthy security and privacy products for the general public (Q4/2015)

SO3	To assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security
WPK 3.1.	**Provide information and advice to support policy development**
D1	Analysis of standards related to eID and/or TSPs (Report, Q4 2015)
D2	Report analysing the terminology and definitions used by eIDAS and (including recommended technological means used by TSPs) (Report, Q4 2015)
WPK 3.2.	**Assist EU MS and Commission in the implementation of EU NIS regulations**
D1	Analysis of Annual 2014 Incident Reports (report) (Q3/2015)
D2	Recommendations on addressing root causes of specific incidents (report) (Q3/2015)
D3	Guidelines on Minimum Security Measures for Trusted Service Providers[1] (workshops, report) (Q4/2015)
D4	Impact assessment on the effectiveness of incident reporting schemes (e.g. Art13a and Art 4) (Q4/2015)
D5	Guidelines on Incident Reporting Scheme for Article 15 (report, Q4 2015)
WPK 3.3.	**Assist EU MS and Commission in the implementation of NIS measures of EU data protection regulation**
D1	Readiness analysis for the adoption and evolution of privacy enhancing technologies (Q4 2015)
D2	Building blocks for PETs update (Q4 2015)
D3	Annual Privacy Forum 2015, APF'2015 (Q4 2015)
D4	State-of-the-art analysis of data protection in big data architectures (Q4 2015)
D5	2015 edition of the annual report on 'Indicative list of appropriate cryptographic protection measures' (Q4 2015)
WPK 3.4	**RandD, Innovation and Standardisation**
D1	Good Practice Guide for aligning Policy, Industry and Research (Q4/2015)
D2	Standardisation Gaps in Cyber Security (Q4/2015)
D3	Guide to standardisation for the SME Community (Q4/2015)

SO4	To enhance cooperation both between the Member States of the EU and between related NIS communities
WPK 4.1.	**Support for EU cooperation initiatives amongst NIS –related communities in the context of the EU CSS**
D1	Develop and provide guidance based on best practice for cooperation between key stakeholder communities (Trust building for and reaching out to new communities) (CERTs, CIIP community, Law Enforcement, Financial Services; Data Protection, etc.) (Q4/2015)
D2	Identify practices of Member States in addressing different sector regulation challenges of managing cyber security issues (Q4/2015)
WPK 4.2.	**European cyber crisis cooperation through exercises**
D1	Evaluation Analysis and Actions from CE2014 (restricted report, Q2 2015)
D2	Pan European Cyber Exercises Plan: CE2016 (restricted report, Q4 2015)
D3	EU-US Cybersecurity Exercise after-action Report[2] (public/restricted report, Q2 2015)
D4	Evaluation and recommendations for improved communication procedures between EU MSs (public/ restricted report, Q4 2015)

5. Management, Administration and Support Activities

5.1. Executive Director's office

The Executive Director's office consists of the Executive Director and his personal assistant.

The Executive Director is responsible for the overall management of the Agency.

The two Heads of Department (Administration and Support Department and Core Operations Department), the Corporate Communications Officer and the Management Board and Permanent Stakeholders Group Secretariat report directly to the Executive Director.

5.2. Administration and Support Department

The Administration and Support Department (ASD) consists of Finance, Accounting and Procurement Unit (FAP), Human Resources Section (HR), IT Unit (ITU), and the team supporting the Department.

The Administration and Support Department is responsible for ensuring that the management of the Agency is in line with the regulatory framework established by the competent EU Institutions, the Management Board, and the Executive Director. The regulatory framework is composed of the Financial Regulation and the Staff Regulations and their respective implementing rules, as well as administrative procedures, the internal control framework and other control mechanisms put in place to ensure compliance with the rules.

The ASD monitors the Agency control and risk framework. Constant upgrading of the internal systems and revision of the operating standards set the grounds for continuous optimisation of the internal processes and procedures. Benchmarking with other organisations, as well as recommendations of the European Court of Auditors and the Internal Audit Service are used as internal performance indicators and relevant possibilities of improvement are considered.

The Head of ASD develops the Agency strategy for the Administration and Support activities in line with the Work Programme and with the required compliance with the above mentioned bodies and rules. He is also the main contact point as regards administrative matters, with external stakeholders such as European Commission Services and DG's, European Parliament, Council, ENISA Executive Board, ENISA Management Board, Hellenic Authorities, etc. The Head of Department is supported by the Legal Officer and two assistants who also support the Units in the Department.

5.3. Activities

5.3.1. ASA 0 Executive Director's office and General management

The activities of Executive Director's office and General Management consist of defining and implementing the Agency's strategy, planning, decision making, and overall management activities.

5.3.2. ASA 1 General Administration

The main activities of General administration include support to Agency management, coordination of translations, Legal Officer services, Internal Control Coordination and Internal Audit Capability (ICC and IAC).

In 2015, the ICC and IAC function will monitor the Agency's activity in administrative transactions, assess the risk framework and the controls in place, contribute to mapping and monitoring the key risk areas, follow up of the implementation of the auditors' recommendations (European Court of Auditors – CoA and Internal Audit Service – IAS) and issue exception management reports.

The ICC and IAC will also ensure that procedures defined are effectively implemented and will carry out spot checks (ex-post controls) as required under the Agency's Financial Regulation.

In 2015, General administration activities' will mainly focus on optimisation of internal tools used for management processes and the integration of such tools across the Agency.

In summary, the following activities are folded under the General Administration:

- Overall administrative and support management, both strategic and operational, of the Agency.
- Legal Officer activities/services.
- Internal Control Coordination and Internal Audit Capability (ICC and IAC) – Coordination of audits (IAS).
- Strategic definition and review of the internal IT systems.
- Liaison between Management and the Staff Committee.
- Relations with Hellenic Authorities.
- Annual Report preparation.
- Management of mail and post services.
- Management of Internal meetings and related expenditures.
- Management of translation services' requests.
- Strategic management of the internal support systems of the Agency.
- Internal Communication strategy.
- Facilities Management, building management and logistics.
- Any other task of general or strategic administrative nature.

5.3.3. ASA 2 Finance, Accounting and Procurement

The activities of Finance, Procurement and Accounting (FAP) Unit consist of managing the Budget of the Agency, conducting all procurement procedures and accounting.

The mission of the Accounting Officer, who is functionally independent, is to execute payments and recover funds in accordance with the instructions of the responsible authorising officer, to manage the treasury of the Agency, validate the accounting systems and provide quality annual accounts, in compliance with the applicable financial and accounting rules.

The activities of the Unit are listed below:

- Financial Transactions' Initiation.
- Operational and Financial Verifications.
- Budget Preparation and Management.
- Missions Management and Helpdesk.
- Financial Helpdesk and Reporting.
- Accounting activities.
- Statutory reporting activities, including discharge procedure.
- Procurement procedures' overall management, including procurement planning.
- Overall contracts' management.
- Coordination of audits (CoA) and support to all other audit assignments.
- Internal Trainings related to FAP activities.
- Single point of contact for financial management matters to DG BUDG (e.g. ABAC implementation).
- Drafting Internal Financial Policies.
- Introducing solutions to optimise internal financial workflows.

5.3.4. ASA 3 Human Resources

The activities of Human Resources section (HR) consist in managing rights and obligations of ENISA Staff, recruitment and training.

- Management of Individual staff Rights and Obligations, according to the stipulations of the Staff Regulation (SR).
- Recruitment procedures.
- Entitlements and leave management.
- Drafting Internal HR Policies and Implementing Rules of the SR.
- Medical Services and Health in work environment.
- Training plan and career development.
- Management of Interim services.
- Work environment and welfare.

5.3.5. ASA 4 Information and Communication Technology

IT Unit delivers quality IT systems and services to the Agency, across its two fully functional offices, as well as to a highly mobile user-base. The IT team uses ITIL (IT Infrastructure Library) Framework as a source of good practise in service management. Both human and financial resources are organised according to ITIL, as shown in the table below.

The IT team also provides infrastructure services for operational systems, e.g. Cyber Exercise Platform.

The activities of IT include help desk, operations and monitoring, services management and infrastructure management, solutions and development. Activities have been aligned with ITIL, including budget lines, as follows:

- Service Strategy and Development.
- Service Transition.
- Service Security.
- Service Operations.
- Services External.
- Service Support.

5.3.6. ASA 5 Facilities Management (FM) – within the scope of the activities of General Administration

Facilities' Management services cater for a quality working environment and infrastructure across its two fully functional offices, ensuring proper working conditions for the staff of the Agency. Activities include the following:

- Logistics, Transport and Delivery Services.
- Buildings and Inventory Management.
- Purchase of stationery and consumables.

5.4. Summary of Administration and Support Activities[10]

Administration and Support Activities			
ASA	**Administration and Support Activities**	**Administration Activities – FTE**	**Total Cost of Activities ABB**
ASA 0	Executive Director's office and Management activities	1,1	83.985
ASA 1	General Administration activities	0,7	131.840
ASA 2	Finanace, Accounting and Procurement activities	2,6	180.538
ASA 3	HR Activities (excluding salaries)	1,6	976.836
ASA 4	IT Activities	1,5	514.353
ASA 5	Facility Management Activities	0,5	930.651
Total ASA		**8,0**	**2.818,203**

Missions		**Total cost**
Missions of all staff		443.849

5.5. Activity Based Budget (ABB)

The Work Programmeme 2015 activities consist of well-defined actions to which resources are allocated and converted into outcomes. Core activities are those aiming to creating the impact in the core field of NIS, required by the Regulation of ENISA and interpreted in the current Policy and Legal context. Administration and Support Activities, on the other hand, aim to provide strategic and overall management orientations, support the core activities with infrastructure and competence, and ensure compliance with the regulatory framework.

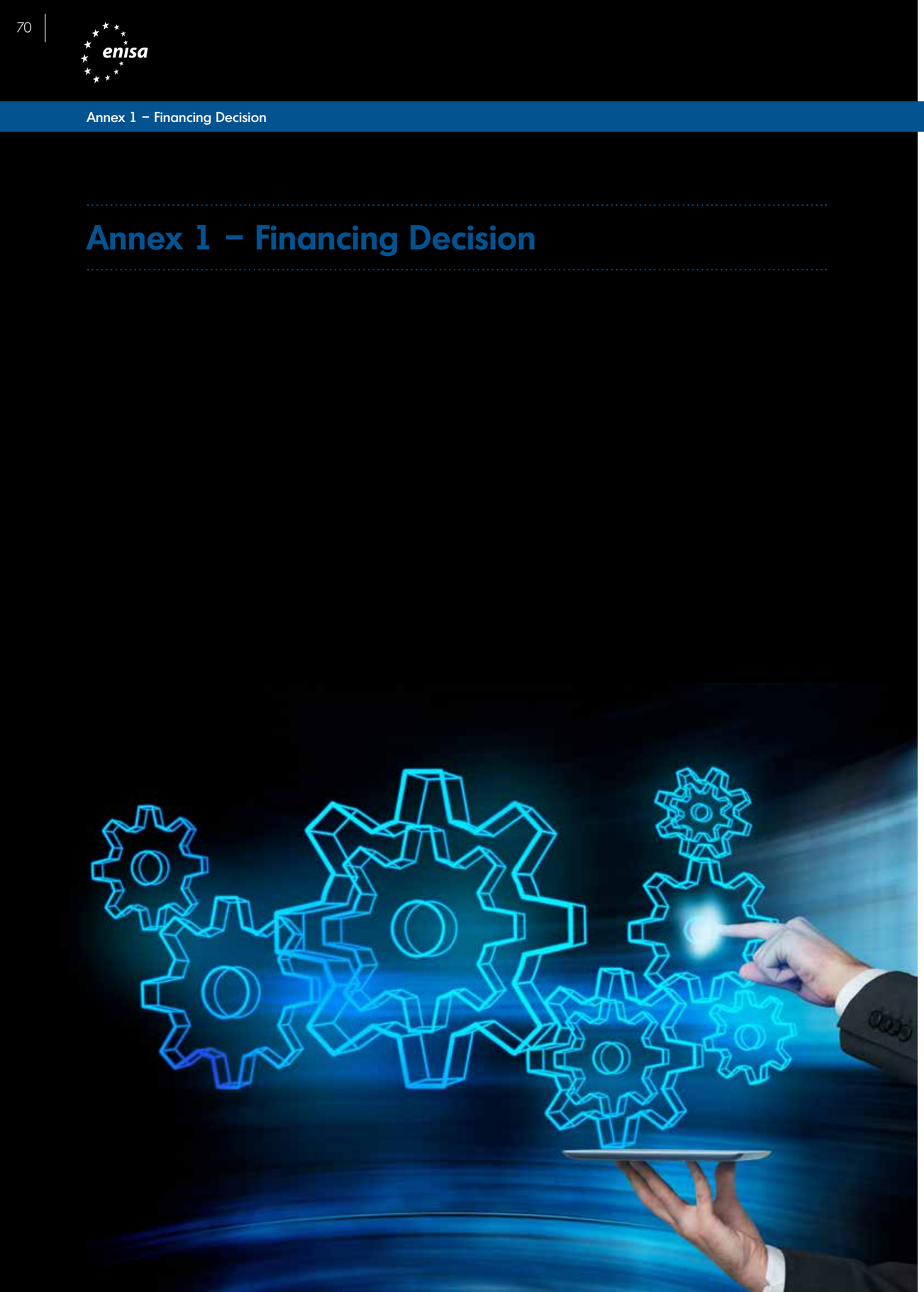
The purpose of ABB is to ensure that resource allocation is consistent with the activities of the Agency, as described in the annual WP.

To this regard, resources engaged in Administration and Support Activities are re-allocated to Core and Horizontal Operational Activities in a way that the effort and the respective human resources costs engaged to the support of the Operational Activities (e.g. procurement procedures to award a contracts related to a WPK/Deliverables) are attributed to the latter.

While the European Commission job screening methodology used for benchmarking resources employed across EU Agencies is looking at human resources allocated to functions and gives weight to job profiles and descriptions (Operational, Neutral, Administration), the ABB concept allocates the Administrative and Support resources according to their contribution to the Agency's work. Therefore the figures in table 5.4 refer to the Administration and Support resources necessary to ensure the smooth operation of the Agency, with focus to the strategic as well as day to day management of the Agency and compliance to the legal and regulatory framework (e.g. risk management, internal controls, engagement with European Court of Auditors and Internal Audit Service, statutory reporting).

10 Remark: Full time equivalents (FTE) and costs of activities are reported on Activity Based Budget basis – see section 5.5

Annex 1 – Financing Decision



	Deliverable description	Budget by Deliverable / WPK	Unit	Specific procurement procedure plans (Title of tender)	Budget for 2015 tenders	Budget expenditure – existing FWC or CEI lists of Experts	Planned contract start date	Planned deliverable date
	Core Operational Activities							
SO1		**€440.000**			**€405.000**	**€35.000**		
WPK 1.1		**€90.000**			**€90.000**	**€0**		
D1	Annual Threat Analysis/Landscape Report (Q4/2015)	€40.000	COD2	Annual ENISA Threat Landscape Report	€40.000		01/03/15	15/11/15
D2	Risk Assessment on two emerging technology/ application areas (Q4/2015)	€50.000	COD2	Tender 1: Sectorial Threat Landscape – Sector A	€25.000		01/03/15	15/11/15
				Tender 2: Sectorial Threat Landscape – Sector A	€25.000		01/03/15	15/11/15
WPK 1.2		**€230.000**			**€210.000**	**€20.000**		
D1	Stock Taking, Analysis and Recommendations on the protection of CIIs (Q3/2015)	€50.000	COD1	Stock Taking, Analysis and Recommendations on the protection of CIIs (tender)	€45.000		01/03/15	31/10/15
				Workshop		€5.000	01/03/15	31/10/15
D2	Methodology for the identification of Critical Communication Networks, Links, and Components (Q4/2015)	€50.000	COD1	Methodology for the identification of Critical Communication Networks, Links, and Components (tender)	€45.000		01/03/15	31/10/15
				Workshop		€5.000	01/03/15	31/10/15
D3	Analysis of ICS-SCADA Cyber Security of Devices in Critical Sectors (Q4/2015)	€50.000	COD1	Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors (tender)	€45.000		01/03/15	31/10/15
				Workshop		€5.000	01/03/15	31/10/15
D4	Recommendations and Good Practices for the use of Cloud Computing in the area of Finance Sector (Q4/2015)	€40.000	COD1	Recommendations and Good Practices for the use of Cloud Computing in the area of Finance Sector (tender)	€35.000		01/03/15	31/10/15
				Workshop		€5.000	01/03/15	31/10/15
D5	Good Practices and Recommendations on reselience and security of eHealth Infrastructures and Services (Q4/2015)	€40.000	COD1	Security and Resilience in eHealth Infrastructures and Services (tender)	€40.000		01/03/15	31/10/15

	Deliverable description	Budget by Deliverable / WPK	Unit	Specific procurement procedure plans (Title of tender)	Budget for 2015 tenders	Budget expenditure – existing FWC or CEI lists of Experts	Planned contract start date	Planned deliverable date
WPK 1.3		**€120.000**			**€105.000**	**€15.000**		
D1	Good Practices and Recommendations on the Security and Resilience Intelligent transportation systems (Q4/2015)	€40.000	COD1	1) An architecture model of the transport sector in Smart Cities. (Tender)	€35.000		01/03/15	01/07/15
				2) Good Practices and Recommendations on the Security and Resilience of Intelligent transportation systems (workshop)		€5.000	15/10/15	15/10/15
D2	Good Practices and Recommendations on the Security and Resilience of Big Data Services (Q4/2015)	€40.000	COD1	Good Practices and Recommendations on the Security and Resilience of big data (tender)	€35.000		01/03/15	31/10/15
				Workshop		€5.000	01/03/15	31/10/15
D3	Good Practices and Recommendations on the Security and Resilience of Smart Home Environments (Q4/2015)	€40.000	COD1	Good Practices and Recommendations on the Security and Resilience of Smart Home Environments (Tender)	€35.000		01/03/15	31/10/15
				Workshop		€5.000	01/03/15	31/10/15
WPK 1.4		**€0**			**€0**	**€0**		
D1	Establish necessary procedures, workflows, tools, etc. to enable ENISA to carry out the Info Notes service (Q2/2015)	€0	COD3	None				
D2	Info Notes on a specific NIS issue (ongoing service with pilot from Q2/2014; conclusions on first year of activity in Q4/2015)	€0	COD3	None				
SO2		**€381.000**			**€300.000**	**€70.000**		
WPK 2.1		**€330.000**			**€275.000**	**€45.000**		
D1	Support and Advise Member States on the establishment and evaluation of National Cyber Security Strategies (NCSS) (Q4/2015)	€40.000	COD1	Development of online training material for NCSS (tender)	€35.000		01/03/15	31/10/15
				Workshop		€5.000	01/03/15	31/10/15

	Deliverable description	Budget by Deliverable / WPK	Unit	Specific procurement procedure plans (Title of tender)	Budget for 2015 tenders	Budget expenditure – existing FWC or CEI lists of Experts	Planned contract start date	Planned deliverable date
D2	Assistance in National CERTS training and education (ongoing)	€0	COD3	None				
D3	Maintaining CERT good practice and training library (Q4/2015)	€100.000	COD3	D3.1. New set of CERT training material (Framework Contract)	€70.000		01/03/15	31/10/15
				D3.2. Maintenance of CERT training repository (Framework Contract)	€30.000		01/03/15	31/10/15
D4	Building upon the evaluation update ENISA's methods in CERT capacity building and propose a roadmap (Q4/2015)	€140.000	COD3	D4.1. Good practice guide and material (Framework Contract)	€90.000		01/03/15	31/10/15
				D4.2.Training event for trainers and multipliers		€10.000	N/A	N/A
				D4.3. CERT Workshops		€10.000	N/A	N/A
				D4.4.Support TRANSITS		€20.000	N/A	N/A
D5	Impact evaluation on the usefulness of the ENISA guidelines on capacity building. (Q4/2015)	€50.000	COD3	Update CERT Impact Assessment (Framework Contract)	€50.000		01/03/15	31/10/15
WPK 2.2		**€21.000**			**€10.000**	**€10.000**		
D1	ENISA report "Status of Privacy and Network and Information Security course curricula in MSs" (Q4 2015)	€11.000	COD2	Survey on Privacy and Network and Information Security course curricula in MSs	€10.000		01/03/15	15/11/15
D2	Further development of ENISA application "NIS self-assessment" (dissemination material, Q4 2015)	€10.000	COD2	Further development of ENISA application "NIS self-assessment" (dissemination material)		€10.000	01/03/15	15/11/15
D3	On-request support for MS decision making (Q4/2015)	€0	COD2	None	€0	€0		
WPK 2.3		**€30.000**			**€15.000**	**€15.000**		
D1	Provide guidance and support for European Cyber-Security Month (dissemination material, Q4 2015)	€10.000	COD2	Provide guidance and support for European Cyber-Security Month (dissemination material)		€5.000	01/03/15	15/11/15
				Web Development (ECSM)		€5.000	01/03/15	15/11/15

	Deliverable description	Budget by Deliverable / WPK	Unit	Specific procurement procedure plans (Title of tender)	Budget for 2015 tenders	Budget expenditure – existing FWC or CEI lists of Experts	Planned contract start date	Planned deliverable date
D2	Basic Cyber hygiene: guidelines for recognizing and using trustworthy security and privacy products for the general public (Q4/2015)	€20.000	COD2	Basic Cyber hygiene: guidelines for recognizing and using trustworthy security and privacy products for the general public (Tender)	€15.000		01/03/15	15/11/15
				Basic Cyber hygiene: Web Development		€5.000	01/03/15	15/11/15
SO3		**€385.000**			**€230.000**	**€155.000**		
WPK 3.1		**€50.000**			**€40.000**	**€10.000**		
D1	Analysis of standards related to eID and/ or TSPs (Report, Q4 2015)	€20.000	COD2	Survey of standards related to eID and/ or TSPs (tender)	€20.000		01/03/15	15/11/15
D2	Report analysing the terminology and definitions used by eIDAS and (including recommended technological means used by TSPs) (Report, Q4 2015)	€30.000	COD2	Terminology and definitions used by eIDAS (tender)	€20.000		01/03/15	15/11/15
				Workshop		€10.000	01/03/15	15/11/15
WPK 3.2		**€140.000**			**€100.000**	**€40.000**		
D1	Analysis of Annual 2014 Incident Reports (report) (Q3/2015)	€15.000	COD1	Workshops	€15.000		01/01/15	15/12/15
D2	Recommendations on addressing root causes of specific incidents (report) (Q3/2015)	€40.000	COD1	Recommendations on addressing root causes of specific incidents (Tender)	€40.000		01/03/15	31/10/15
D3	Guidelines on Minimum Security Measures for Trusted Service Providers[1]	€25.000	COD1	Guidelines on Minimum Security Measures for Trusted Service Providers: Workshops and external support		€25.000	01/01/15	15/12/15
D4	Impact assessment on the effectiveness of incident reporting schemes (e.g. Art13a and Art 4) (Q4/2015)	€45.000	COD1	Impact assessment on the effectiveness of incident reporting schemes (e.g. Art13a and Art 4) (Tender)	€45.000		01/03/15	31/10/15
D5	Guidelines on Incident Reporting Scheme for Article 15 (report, Q4 2014)	€15.000	COD1	Guidelines on Incident Reporting Scheme for Article 15: Workshops		€15.000	01/01/15	15/12/15

	Deliverable description	Budget by Deliverable / WPK	Unit	Specific procurement procedure plans (Title of tender)	Budget for 2015 tenders	Budget expenditure – existing FWC or CEI lists of Experts	Planned contract start date	Planned deliverable date
WPK 3.3		**€130.000**			**€35.000**	**€95.000**		
D1	Readiness analysis for the adoption and evolution of privacy enhancing technologies (Q4 2015)	€40.000	COD2	Expert Working Group		€25.000	01/03/15	15/11/15
				Workshop		€15.000	01/03/15	15/11/15
D2	Building blocks for PETs update (Q4 2015)	€25.000	COD2	Expert Working Group		€20.000	01/03/15	15/11/15
				Workshop		€5.000	01/03/15	15/11/15
D3	Annual Privacy Forum 2015, APF'2015 (Q4 2015)	€10.000	COD2	Cooperation Agreement: APF'2015	€10.000		01/03/15	15/11/15
D4	State-of-the-art analysis of data protection in big data architectures (Q4 2015)	€30.000	COD2	Expert Working Group		€20.000	01/03/15	15/11/15
				Workshop		€10.000	01/03/15	15/11/15
D5	2015 edition of the annual report on 'Indicative list of appropriate cryptographic protection measures'	€25.000	COD2	Indicative list of appropriate cryptographic protection measures (Tender)	€25.000		01/03/15	15/11/15
WPK 3.4		**€65.000**			**€55.000**	**€10.000**		
D1	Good Practice Guide for aligning Policy, Industry and Research (Q4/2015)	€40.000	COD2	Good Practices in aligning Policy, Industry and Research in NIS	€40.000		01/03/15	15/11/15
D2	Standardisation Gaps in Cyber Security (Q4/2015)	€10.000	COD2	Expert Working Group		€10.000		
D3	Guide to standardisation for the SME Community (Q4/2015)	€15.000	COD2	Guide to standardisation for the SME Community	€15.000		01/03/15	15/11/15

	Deliverable description	Budget by Deliverable / WPK	Unit	Specific procurement procedure plans (Title of tender)	Budget for 2015 tenders	Budget expenditure – existing FWC or CEI lists of Experts	Planned contract start date	Planned deliverable date
SO4		**€324.000**						
WPK 4.1		**€119.000**			**€110.000**	**€9.000**		
D1	Develop and provide guidance based on best practice for cooperation between key stakeholder communities (Trust building for and reaching out to new communities)(CERTs, CIIP community, Law Enforcement, EU Financial Services; Data Protection, etc.) (Q4/2015)	€79.000	COD3	D1.1.Report "Lessons learned from CERT/ LEA cooperation, and the cooperation with the FI sector, and how to apply them to new communities"	€70.000		01/03/15	01/10/15
				D1.2. Update of "CERT baseline capabilities"		€9.000	N/A	N/A
D2	Identify practices of Member States in addressing different sector regulation challenges of managing cyber security issues (Q4/2015)	€40.000	COD3	Report "Stocktaking on MS regulatory approaches for Cyber Security, with an emphasis on cross-sector info sharing" (Framework Contract)	€40.000		01/03/15	31/10/15
WPK 4.2		**€205.000**			**€120.000**	**€85.000**		
D1	Evaluation Analysis and Actions from CE2014 (restricted report, Q2 2015)	€60.000	COD2	Analysis of the CE2014 Evaluation Data and Recommendations (Framework Contract)	€25.000		01/01/15	01/07/15
				Strategic-level and Evaluation Workshops (x2)		€15.000	01/01/15	01/07/15
				Cyber Exercise Platform Enhancements Lessons Learned from CE2014		€20.000	01/01/15	01/07/15
D2	Pan European Cyber Exercises Plan: CE2016 (restricted report, Q4 2015)	€60.000	COD2	Development of Scenario and Incidents for CE2016 (Framework Contract and/or Expert Group)	€25.000		01/05/15	01/12/15
				Planning Workshops (x2)		€15.000	01/05/15	01/12/15
				Cyber Exercise Platform Preparation for CE2016		€20.000	01/05/15	01/12/15
D3	EU-US Cybersecurity Exercise after-action Report[2] (public/ restricted report, Q2 2015)	€40.000	COD2	Exercise Scenario, Support and Moderation (Framework Contract and/or CEI)	€25.000		01/05/15	01/12/15
				Workshops (x2)		€15.000	01/05/15	01/12/15

	Deliverable description	Budget by Deliverable / WPK	Unit	Specific procurement procedure plans (Title of tender)	Budget for 2015 tenders	Budget expenditure – existing FWC or CEI lists of Experts	Planned contract start date	Planned deliverable date
D4	Evaluation and recommendations for improved communication procedures between EU MSs (public/ restricted report, Q3 2015)	€45.000	COD2	A) Analysis Report of the Policy Framework and the Existing Proposals for EU Cyber Crisis Cooperation (Framework Contract)	€25.000		01/01/15	01/12/15
				B) Requirements for Tools Supporting EU Cyber Crisis Cooperation (Framework Contract)	€20.000		01/01/15	01/12/15
	Total Budget for Strategic Objectives 1-4 (WP 2015)	**€1.530.000**			**€935.000**	**€260.000**		
	Horizontal Operational Activities							
SR1	**MB and PSG Secretariat**	**€180.000**			**€0**	**€180.000**		
D1	Management Board, Executive Board and PSG meetings	€180.000		Use of existing Framework Contract for events' organisation (multiple meetings) and reimbursement to participants		€180.000	n/a	n/a
SR2	**National Liaison Officers Network**	**€32.000**			**€0**	**€32.000**		
D1	National Liaison Officers Network meeting	€32.000	COD4	Use of existing Framework Contract for events' organisation (1 meeting)		€32.000	n/a	n/a
CC1	**Corporate Communication**	**€238.000**			**€136.000**	**€102.000**		
D1	Media support and press release distribution, and outreach	€50.000	CC	Use of existing Framework Contract for media support		€50.000	n/a	n/a
D2	Crisis communication training and workshops	€20.000	CC	Tender Crisis communication training	€20.000		Q3	Q4
D3	Corporate communications services and workshop	€20.000	CC	Use of existing Framework Contract		€20.000	n/a	n/a
D4	High Level Event, brochures, design, printing, catering, food,	€18.000	CC	Use of existing Framework Contracts		€18.000	n/a	n/a
D5	Europe Day 9th May (print, design)	€2.000	CC	Use of existing Framework Contracts		€2.000	n/a	n/a

	Deliverable description	Budget by Deliverable / WPK	Unit	Specific procurement procedure plans (Title of tender)	Budget for 2015 tenders	Budget expenditure – existing FWC or CEI lists of Experts	Planned contract start date	Planned deliverable date
D6	Digital Communications-video clips	€40.000	CC	Tender for Provision of digital communication services (production of video clips)	€40.000		Q3	Q4
D7	Digital software for monitoring media	€3.500	CC	Negotiated Procedure – 1 offer	€3.500		Q2	Q2
D8	Corporate brand marketing	€50.000	CC	Tender for Corporate brand marketing	€50.000		Q3	Q4
D9	Photographic services	€2.500	CC	Negotiated Procedure – 1 offer	€2.500		Q1	Y2015
D10	Graphic design services	€12.000	CC	Use of existing Framework Contracts		€12.000	n/a	n/a
D11	Local media marketing	€5.000	CC	Negotiated Procedure – 1 offer	€5.000		Q3	Q3
D12	Corporate brand marketing material (new ENISA logo and name)	€15.000	CC	Tender for Corporate brand marketing material	€15.000		Q4	Q4
PS1		**€100.000**			**€14.000**	**€86.000**		
D1	Web Hosting	€15.100	COD4	Use of existing Framework Contract		€15.100	n/a	n/a
D2	Web Development 1000H	€35.000	COD4	Use of existing Framework Contract		€35.000	n/a	n/a
D3	CRM Licences and support	€5.000	COD4	Use of existing Framework Contract		€5.000	n/a	n/a
D4	Security assessments	€5.000	COD4	Negotiated Procedure – 1 offer	€5.000		n/a	n/a
D5	Cloud infrastructure	€6.000	COD4	Negotiated Procedure – 1 offer	€6.000		n/a	n/a
D6	Cloud service licences	€3.000	COD4	Negotiated Procedure – 1 offer	€3.000		n/a	n/a
D7	Extra projects provision	€30.900	COD4	Use of existing Framework Contract		€30.900	n/a	n/a
	Total Operational Budget (Title 3) for Horizontal Operational Activities (WP 2015)	**€370.000**			**€150.000**	**€220.000**		
	Missions of ENISA staff – Operational Budget (Title 3)	**€443.849**		**Use of existing Framework Contract on travel agency services**		**€443.849**	**n/a**	**Y2015**

European Union Agency for Network and Information Security

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

Athens Office
1 Vasilissis Sofias Str.
ENISA building
Marousi 151 24, Athens, Greece

enisa.europa.eu

Catalogue Number: TP-AF-14-001-EN-N, ISBN: 978-92-9204-114-4, ISSN: 2363-3115, DOI: 10.2824/097365