WORK PROGRAMME 2014

29 NOVEMBER 2013

Contents

ACRONYMS

AD: Administration Department
ADA: Administration Department Activity
APCERT: Asia-Pacific CERT
APT: Advanced Persistent Threat
CA: Certification Authority
CEO: Chief Executive Officer
CEP: Cyber Exercises Platform
CERT: Computer Emergency Response Team
CII: Critical Information Infrastructures
CIIP: Critical Information Infrastructure Protection
CIP: Competitiveness and Innovation Programme
CISO: Chief Information Security Officer
COM: European Commission
CSIRT: Computer Security Incidents Response Teams
D: Deliverable
DG: Directorate-General
DPA: Data Protection Authorities
EC: European Union Commission
ED: Executive Director
EDPS: European Data Protection Service
EGC: European Government CERTs
EFMS: European Forum for Member States
EFTA: European Free Trade Association
eID: electronic Identity
EISAS: European Information Sharing and Alert System
ENISA: European Union Agency for Network and Information Security
EP3R: European Public Private Partnership for Resilience
ERNCIP: EU Reference Network for Critical Infrastructure Protection
EU: European Union
EuroSCSIE: European SCADA and Control Systems Information Exchange
FAP: Finance, Accounting & Procurement section
FIRST: Forum of Incident Response and Security Teams
FP (7): Framework Programme (7)

IaaS: Infrastructure as a Service 5 **ICS:** Industrial Control Systems

ICT: Information and Communication Technologies

IDABC: Interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens

IS: Information Systems

ISAC: Information Sharing & Analysis Centre

ISO: International Organization for Standardization

ISO: Information Security Officer

ISP: Internet Service Providers

ITFMU: Information Technology & Facilities Management Unit

ITU: International Telecommunication Union

IXP: Internet exchange point

LEA: Law Enforcement Agency

LHR: Legal & Human Resources section

MB: Management Board

MISS: Missions

n/g CERT: National / Governmental CERT

NCO: National Contact Officer

NCP: National Contigency Plans

NIS: Network and Information Security

NISHA: Network for Information Sharing and Alerting

NLO: National Liaison Officer

NRA: National Regulatory Authority

PaaS: Platform as a Service

PAU: Public Affairs Unit

PKI: Public Key Infrastructure

PPP: Public Private Partnership

PSG: Permanent Stakeholders Group

Q: Quarter

R&D: Research and Development

RIM: Research In Motion

SaaS: Software as a Service

SCADA: Supervisory Control And Data Acquisition

SME: Small and Medium Enterprise

SOC: Security Operations Centres 6

SR: Stakeholder Relations

STORK: Secure *IdenTity* AcrOss BordeRs LinKed

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

TISPAN: Telecommunications and Internet converged Services and Protocols for Advanced Networking

US: United States of America

WP: Work programme

WPK: Work Package

1 Introduction

1.1 Introduction

As in previous years, the work programme for 2014 reflects the results of the consultation process with the ENISA Permanent Stakeholder Group (PSG) and Management Board that was carried out in November 2012 and February 2013. This version also takes account of comments submitted by Member States following the March Management Board meeting and includes modifications to resources and budget following confirmation of the latter by the EU Commission.

The structure of the 2014 work programme is fundamentally different to that of previous work programmes. Whilst core operational activities are still structured into three streams of work, these streams reflect the way in which the work supports the EU policy goals of the Member States rather than areas of activity that are based on the content. The result is a work programme that is a natural continuation of the evolution of the Agency's work over the last few years, but organised according to new criteria.

Estimates for resources and budget have been adapted to reflect the fact that ENISA will have new activities to perform during 2014 as a result of the new mandate and the Cybersecurity Strategy for the European Union.

1.2 Structure

1.2.1 Core operational activities

The core operational activities covered by the 2014 Work Programme have been structured as three separate work streams. These work streams are as follows.

- WS1: Support EU policy building
- WS2: Support capacity building
- WS3: Support co-operation.

In addition, supporting work will continue in the form of a set of horizontal activities.

1.2.2 Horizontal activities

As in previous years, this work programme also regroups a number of activities into a single chapter, under the general heading of 'Horizontal Operational Activities':

- Management Board, Executive Board & PSG Secretariat
- National Liaison Officer Network
- EU Relations
- Corporate Communication
- Dissemination activities
- Quality control

The Project Support Activities cover Dissemination Activities, Quality Management and Public Relations support for COD.

1.2.3 Administration and support department, Directorate and General management activities

Support activities have been further streamlined by integrating facility management and IT support activities within the Administration and Support department .

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 Member States 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.

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]

ENISA-Regulation[2,3]

Prior to the adoption of the new regulation, all activities and tasks carried out by the Agency were fulfilled on the basis of the founding ENISA-Regulation. This basis was laid down in Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Union Agency for Network and Information Security.

The new Regulation builds on ENISA's achievements in areas such as supporting Computer Emergency Response Teams (CERTs) in Member States and facilitating the pan-European cybersecurity exercises. It provides ENISA with a strong interface to Europol's European Cybercrime Centre (EC3) to enable the Agency to contribute to the fight against cybercrime, focusing on prevention and detection. It also foresees a more proactive role for the Agency in supporting the development of EU cybersecurity policy and legislation. This is also true for the areas of research, development and standardisation, where EU standards for risk management and the security of electronic products, networks and services are cited as key aspects. Finally, ENISA is also given a stronger role in cooperating with third countries.

The Cybersecurity Strategy of the EU[4] and the proposal for an NIS Directive

Information and communications technology has become the backbone of our economic growth and is a critical resource which all economic sectors rely on. It now underpins the complex systems which keep our economies running in key sectors such as finance, health, energy and transport; while many business models are built on the uninterrupted availability of the Internet and the smooth functioning of information systems.

Recent years have seen that while the digital world brings enormous benefits, it is also vulnerable. Cybersecurity incidents, be it intentioal or accidental, are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile services. Threats can have different origins — including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes.

The Commission has proposed the Cybersecurity strategy of the European Union, which outlines the EU's vision in this domain, clarifies roles and responsibilities and sets out the actions required based on strong and effective protection and promotion of citizens' rights to make the EU's online environment the safest in the world.

This strategy is accompanied by a proposal for legislation[5] to:

[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 2014, please refer to each WS.
[2] 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.
[3] 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
[4] http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf
[5] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final

- Establish common minimum requirements for NIS at national level
- Set up coordinated prevention, detection, mitigation and response mechanisms, enabling information sharing and mutual assistance amongst the national NIS competent authorities.
- Improve preparedness and engagement of the private sector.

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[6]

These Council Conclusions, agreed by the General Affairs Council on 25 June 2013, summarises actions to be carried out by various actors in the cybersecurity field.

Digital Agenda[7]

The Digital Agenda for Europe is one of the seven flagship initiatives of the Europe 2020 Strategy, and provides an action plan for making the best use of ICT to speed up economic recovery and lay the foundations of a sustainable digital future. The Digital Agenda for Europe outlines seven priority areas for action, in the context of which it also attributes a significant role to ENISA as well as to its stakeholders.Council Directive on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection[8].

This Directive establishes a procedure for the identification and designation of European Critical Infrastructures ('ECIs'), and a common approach to the assessment of the need to improve the protection of such infrastructures in order to contribute to the protection of people.

The CIIP Action Plan

The Commission Communication "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" calls upon ENISA to support the Commission and Member States in implementing the CIIP Action Plan to strengthen the security and resilience of CIIs.

The Commission Communication on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security" adopted on 31 March 2011[9]

In this communication, the Communication takes stock of the results achieved since the adoption of the CIIP action plan in 2009 launched to strengthen the security and resilience of vital Information and Communication Technology infrastructures. The next steps the Commission proposes for each action at both European and international level are also described.

Electronic Communications Regulatory Framework[10]

The review of the EU electronic communications regulatory framework and, in particular, the new provisions of articles 13a and 13b of the Framework Directive and the amended article 4 of the e-Privacy Directive aim at strengthening obligations for operators to ensure security and integrity of their networks and services, and to notify breaches of security, integrity and personal data to competent national authorities and assign to ENISA specific tasks.

---

[6] Available at http://register.consilium.europa.eu/pdf/en/13/st12/st12109.en13.pdf
[7] A Digital Agenda for Europe, COM(2010)245, May, 2010.
[8] 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
[9] "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)
[10] Telecommunications Regulatory Package (article 13a. amended Directive 2002/21/EC Framework Directive)

Review of the Data Protection Framework[11]

In 2012, the European Commission published its proposal for a regulation on data protection. This regulation will replace the existing Data Protection Directive. It encompasses many of the concepts described above, promoting privacy by design and data protection by default while including provisions for remedies, liability and administrative sanctions in case of non-compliance. ENISA will support the implementation of the new regulation on data protection.

Electronic identification and trusted services for electronic transactions in the internal market[12]

The new framework for electronic identification and electronic trust services ensures mutual recognition and acceptance of electronic identification across borders, gives legal effect and mutual recognition to trust services including enhancing current rules on e-signatures and provides a legal framework for electronic seals, time stamping, electronic document acceptability, electronic delivery and website authentication.

This proposal represents the first milestone in the implementation of the objectives of the Legislation Team (eIDAS) Task Force set up by the Commission in order to to deliver a predictable regulatory environment for electronic identification and trust services for electronic transactions in the internal market to boost the user convenience, trust and confidence in the digital world.

Commission Regulation on the measures applicable to the notification of personal data breaches

In June 2013, the European Commission has put in place new specific rules to ensure that personal data breaches in the EU telecoms sector are notified in the same way in each Member State[13].

The 2002 ePrivacy Directive requires telecommunications operators and Internet service providers to keep personal data confidential and secure. To ensure consistent implementation of the data breach rules across Member States, the Commission has adopted "technical implementing measures" – practical rules to complement the existing legislation – on the circumstances, formats and procedures for the notification requirements. These rules will help ensure ensure that all customers receive equivalent treatment across the EU in case of a data breach, and that businesses can take a pan-EU approach to these problems if they operate in more than one country.

A coherent framework to build trust in the Digital single market for e-commerce and online services[14]

The European Commission adopted the Communication on e-commerce and other online services announced in the ”Digital Agenda“ and the ”Single Market Act“. Based on an in-depth public consultation, this Communication sets out the Commission's vision for the potential represented by online services in growth and employment, identifies the principal obstacles to the development of e-commerce and online services, and establishes 5 priorities, accompanied by an action plan.

Council Framework Decision on attacks against information systems[15]

[11] 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

[12] Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, COM(2012) 238/2

[13] Commission Regulation 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

[14] 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, available at: http://ec.europa.eu/internal_market/e-commerce/communication_2012_en.htm

[15] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

This Framework Decision proposes the approximation of criminal law systems and the enhancement of cooperation between judicial authorities. It forms a part of the information society and of the eEurope Action Plan16 in general. The Framework Decision will be replaced by a new Directive on attacks against information systems, that is expected to be adopted shortly. This Directive retains the Framework Decision´s current provisions – the penalisation of illegal access, illegal system interference and illegal data interference – and notably includes new offences, such as illegal interception and the use of tools to commit large-scale attacks.

Commission Communication 'Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre'[17]

In this Communication, the Commission proposes a European Cybercrime Centre (EC3), which will be part of Europol and act as the focal point in the fight against cybercrime in the EU. This Communication drawing on the feasibility study outlines the proposed core functions of the European Cybercrime Centre, explains why it should be located in Europol, and how it can be established. The EC3 was officially launched on 11 January 2013.

Council Resolution of December 2009[18]

The Council Resolution on a collaborative European approach on Network and Information Security of 18 December 2009 builds on a number of EU strategies and instruments developed in recent years. It provides political direction on how the Member States, the Commission, ENISA and stakeholders can play their part in enhancing the level of network security in Europe.

Council conclusion on CIIP of May 2011[19]

These Council Conclusion take stock of the results achieved since the adoption of the CIIP action plan in 2009, launched to strengthen the security and resilience of vital Information and Communication Technology Infrastructures.

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[20]

The Commission has produced a Commission Staff Working Paper on Security Industrial Policy”21 SWD(2012) 233 final, and a Communication regarding an Action Plan for an innovative and competitive Security Industry. The underlying idea of the Commission is the creation of a true internal market for the security industry by suggesting clear measures. A dedicated expert group set up by the Commission will meet at least once per year to monitor the implementation of proposed policy measures and bring together all relevant actors in the field of security.

Single Market Act[22]

In April 2011, the European Commission adopted a Communication, the Single Market Act, a series of measures to boost the European economy and create jobs. This includes notably the key action entitled ‘Legislation ensuring the mutual recognition of electronic identification and authentication

[16] http://europa.eu/legislation_summaries/information_society/strategies/l24226_en.htm
[17] European Commission, " Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre" , 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
[18] Council resolution of 18 December, 2009 on a collaborative approach to network and information security (2009/C 321 01)
[19] Council Conclusion on CIIP of May 2011 (http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf)
[20] 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
[21] Available at ec.europa.eu/enterprise/policies/security/files/commission_staff_working_paper_-_security_industrial_policy_-_com(2012)_417_final_en.pdf
[22] Single Market Act – Twelve levers to boost growth and strengthen confidence “Working Together To Create New Growth”, COM(2011)206 Final

across the EU and review of the Directive on Electronic Signature's. The objective is to make secure, seamless electronic interaction possible between businesses, citizens and public authorities, thereby increasing the effectiveness of public services and procurement, service provision and electronic commerce (including the cross-border dimension).

Internet of Things – An Action Plan for Europe[23]

This Communication from the Commission addresses several main trends and challenges in the evolution of the Internet: Scalability, Mobility, Heterogeneity, complexity and interoperability, such as the role of public authorities, governance, personal data protection and public and private rights and duties.

European cloud computing strategy

The Communication COM(2012)529 'Unleashing the potential of cloud computing in Europe' was adopted on 27 September 2012. It constitutes the European policy in the area of cloud computing and addresses areas such as standards, certification, trust and security, data protection, cross-border services, contractual terms, consumer protection, interoperability and portability and adoption of cloud services by public authorities. Furthermore it recognises the need for awareness raising and international cooperation. This document is the European policy baseline on cloud computing and it includes a specific action for ENISA on EU-wide voluntary certification schemes."

Internal Security Strategy for the European UnionInternal Security Strategy for the European Union[24]

The Internal Security Strategy lays out a European security model, which integrates among others action on law enforcement and judicial cooperation, border management and civil protection, with due respect for shared European values, such as fundamental rights. This document includes a number of suggested actions for ENISA.

Council Resolution on a collaborative approach to Network and Information Security [25]

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, awareness raising and serving as a center of expertise.

Telecom Ministerial Conference on CIIP organised by the Presidency in Balatonfüred, Hungary

This conference took place on 14-15 April 2011 and was a natural extension of the "Tallinn process" initiated by the 2009 Ministerial CIIP Conference in Estonia under the Czech Presidency of the EU. On this occasion, Vice President of the European Commission, Neelie Kroes, Digital Agenda Commissioner, acknowledged the progresses made by Member States but also called upon for further actions and stressed the importance of international cooperation. In particular, as a follow-up to the Conference, VP Neelie Kroes called on ENISA to intensify its activity of promoting existing good practices by involving all Member States in a peer-learning and mutual support process with the aim to promote faster progress and bring all Member States on par. VP Neelie Kroes called on ENISA to establish a highly mobile dedicated team to support such process.

[23] 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.
[24] An internal security strategy for the European Union (6870/10), http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/113055.pdf
[25] Council Resolution on a collaborative European approach to Network and Information Security, 2009/C 321/01 of 18 December 2009.

The work streams (WS) that are described in this document have been developed in this legal framework and context while they support this overall political agenda.

3 Core operational activities

3.1 Introduction

The core activities of ENISA for 2014 have been grouped into three work streams (WS):

- WS1 : 'Support EU policy building' will support the policy making process by making available to policy makers consolidated information on the emerging threat landscape and by formulating key messages to the Member States on how to ensure that their policies and capabilities are aligned with EU objectives taking into account lessons learned within the different Member States. This will involve the unification of available information sources under a common context and will also require the involvement of important stakeholders in the areas of threat assessment, risk mitigation and policy definition.
- WS2 : 'Support capacity building' foresees a number of activities designed to assist both the public sector and private sector in the Member States in protecting Critical Information Infrastructures (CIIP). By facilitating cooperation and coordination between public and private sectors within the Member States, ENISA will continue to support the development of policies and measures and implementable preparedness, response and recovery strategies, to meet the challenges of a continuously evolving threat environment.
- WS3 : 'Support cooperation' is about strengthening NIS in the European single market. Cooperation strengthens the capacities of Member States, EU institutions and third countries and helps them to deal with crises. The approach will be to build upon existing collaboration in existing communities, further enhancing community building in Europe and beyond. This work also looks at the development of tools to facilitate and improve the international communication and interchange of security relevant information within communities sharing the same interest in different MS.

3.2 WS1- Support EU policy building

3.2.1 Overview

Justification

This work stream consists of work packages that are designed to assist COM and Member States in building EU policy in the area of Network & Information Security. When specifically requested by Member States, the Agency will also assist in ensuring that national policies are aligned with EU objectives.

This support to the policy building activities in EU can be addressed in different steps:

- Analysis and research of the evolving threat environment.
- The promotion of standards / best practises.
- Support to the EU and Member States in the fields of education, research and standardisation.

The following benefits are foreseen:

- Coherent and meaningful data on the emerging threat landscape and trends is a valuable tool for NIS professionals, decision and policy makers.
- Dissemination of current best practises and standards contributes to interoperability, provides technical references for the harmonisation of technologies, and augments the protection level for NIS infrastructures and services in the EU. This is expected to lead to more effective risk mitigation stratergies.
- NIS knowledge transferred to education, research and standardisation activities, contributes to EU-wide harmonisation in these areas.

Specific Policy Context

Specific policy references for this work stream are as follows:

- Proposal No COM(2010) 521 final, 2010/0275 (COD) of 30 September 2010 for a Regulation of the European Parliament and of the Council concerning the European Union Agency for Network and Information Security (ENISA).
- Commission proposed Action Plan to enable further growth of Security industry[26] COM(2012) 417.
- The Cybersecurity Strategy for the EU

Overall Objectives

The objectives of this Work Stream are:

- Analysis of the evolving threat environment, both from the stakeholder and EU policy makers' perspective.
- Identification of gaps in NIS technologies and policies, and the support in the development of strategies, best practises, frameworks and standards.
- Mobilisation of relevant stakeholders, the development of a roadmap for the creation of an "NIS Drivers License", and support for the implementation of the roadmap.

3.2.2 Work Packages

The following work packages constitute the Work Stream:

[26] http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item_id=6117&lang=en&tpa_id=0&title=Security-industry%3A-Commission-proposes-programme-to-enable-further-growth-

- WPK1.1. Identifying evolving threats, risks and challenges: The main objective of this work package is to collect and collate current data in order to develop the ENISA threat landscape. It includes current threats, as well as threat trends in NIS and emerging technologies. The threat landscape is based on existing publicly available material on threats, risks and trends.
- WPK1.2. Contributing to EU policy initiatives: The main objective of this work package is to provide input to new policy initiatives (in areas such as Cloud computing, smart grids, etc.) before they are launched and also to assist the COM and the Member States in implementing such policies in an effective way and in learning from this experience so that problems can be avoided in future policy statements.
- WPK1.3. Supporting the EU in education, research & standardisation: In the context of this activity ENISA will continue its efforts to support EU funded R&D initiatives such as FP7 and H2020 and standardisation activities including EU initiatives such as the ETSI CEN CENELEC Cyber Security Coordination Group (CSCG). Finaly, this work will support the activities in the area of education described in the NIS Cyber Security Strategy such as NIS driving license and European Cyber Security Month 2014 (ECSM'2014).

3.2.3 WPK 1.1: Identifying evolving threats, risks and challenges

Desired Impact

- The ENISA Threat Landscape becomes an important point of reference for security experts worldwide and is referenced in at least 10 security related information sources world wide.
- It is referenced by 5 stakeholders from the 2 sectors covered.
- Identified emerging threats and trends have been taken into consideration in at least 5 R&D projects in EU.

Description of tasks

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

In addition to the global threat analysis (the ENISA threat landscape), this work will include detailed threat and risk assessments for at least two particular areas/sectors. These will be detailed analyses of particular areas that are crucial for society, industry or research. Examples of such areas are key internet infrastructures, banking and finance, health, transport, energy and public administration. During the preparatory phases of the Work Programme execution, ENISA will select these areas by consulting relevant stakeholder communities and by identifying current priorities. This work package will involve the analysis of three main sources of information:

- Consultations with different players in the security field will support the data collection work and will also be used as a basis for selecting the areas/sectors of interest.
- An analysis of innovative projects and activities being supported by COM or Member States in research or early development phases. This will have impact on future uses of technologies and may require analysis of potential new threats and associated risks.
- Analysis of reported and publicly known incidents in the subject matter areas.

This approach will allow ENISA to develop a perspective of the European landscape of the NIS gaps and needs for a wide spectrum of stakeholders. The Agency will match identified threats with existing minimum security measures and suggest amendments of existing and publicly known measures to better mitigate these threats.

To achieve these objectives, the following tasks will be carried out:

- Development of the ENISA Threat Landscape 2014, as continuation of the work started in 2012 on a yearly basis, and improving the results in the following areas:
    - Derivation of the European perspective based collected threats (e.g. incorporating information on European companies such as size, type of business, etc.).
    - Improvement of the quality of threat information collection within related organisations.
    - Liaison with sources of threat information to establish effective dissemination of generated information.
    - Analysis and assessment of previous year forecasts.

Outcomes & deadlines

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

- WPK1.1-D1 – Annual EU CyberSecurity Threats Landscape.

- WPK1.1-D2 – Identification of trends, security challenges, associated risks and required countermeasures, for emerging technologies (with special attention to selected areas/sectors).

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 R&D related activities.
- Public and private organisations may capatilise on the ENISA output to propose innovative R&D activities, products or services.

Resources

- 100 kEuro
- 20,9 person months

Legal base & policy context

- Commission proposes Action Plan to enable further growth of Security industry[27] COM(2012) 417:
  The COMhas produced a "COMMISSION STAFF WORKING PAPER on Security Industrial Policy"[28] SWD(2012) 233 final, and "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE"[29] 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)30. 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 Member States and EU institutions

[27] http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item_id=6117&lang=en&tpa_id=0&title=Security-industry%3A-Commission-proposes-programme-to-enable-further-growth-

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

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

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

- Raise awareness and good practices and guidance
- EU policy development and implementation support to COM and Member States, bridging gap between technology and policy, and following EU priorities.

3.2.4 WPK 1.2: Contributing to EU policy initiatives

Desired Impact

- 10 Cloud Computing Providers and 5 Member States support ENISA's recommendations for improving NIS aspects of Cloud Computing
- 15 Smart Grids providers and 5 Member States competent authorities support ENISA's guidelines for implementing the Smart Grids Strategy
- 5 Member States eID competent bodies/authorities, 5 Independent Auditing Bodies and 5 Trust Service Providers take part in the development of a common audit framework for trust service providers.
- ENISA recommendations on algorithms and parameters for secure services for the protection of personal data in the context eGov services supported by competent authorities in at least 5 Member States;

Description of tasks

The tasks carried out in this work package are designed both to provide input to new policy initiatives before they are launched and also to assist COM and the Member States in implementing such policies in an effective way and in learning from this experience so that problems can be avoided in future policy statements.

EU's Cloud Computing Strategy and Partnership

ENISA will continue to play an active role in the implementation of the EU's cloud computing strategy and partnership. The Agency will provide technical advice, recommendations and good practices to Commission's Special Interest Groups (SIGs) and the European Cloud Partnership (ECP) in the areas of certification, public procurement guidelines, SLAs and incident reporting mechanisms. In all these areas ENISA will engage with all relevant public and private stakeholders and make sure that these efforts properly align with EU's ECP, ETSI and CEN/CENELEC initiatives.

EU's Smart Grids Strategy

ENISA will assist the Commission, the Member States and the private sector in the implementation of the EU's Smart Grids strategy. The Agency will provide technical advice, recommendations and good practices in the area of Minimum Security Measures for Smart Grids, certification of Smart Grid components, privacy profile of Smart Meters, and incident reporting mechanisms. ENISA will engage with all relevant stakeholders, provide contributions to COM policy intiatives (e.g. EU CSS, DG ENER Expert Group 2 (EG2), CEN/CENELEC's M490) and make sure that these efforts properly align with EU's overall Smart Grid Policy.

Algorithms and parameters for secure services

Technical protection measures, specified in legal documents, need to be matched with technical specifications in order to secure personal data[31]. During 2013, ENISA initiated a new activity in the area of cryptography with an emphasis on providing technical specifications for cryptographic algorithms to protect personal data in e government (eGov) services. The algorithms are analysed

[31] ENISA is expected to assist the EC in establishing an indicative list of appropriate technological protection measures, including encryption schemes, according to the recently published EC regulation 611/2013 (https://ec.europa.eu/digital-agenda/en/eprivacy-directive-data-breach-notifications) on the measures applicable to the notification of personal data breaches. Article 4 of the ePrivacy directive and Article 29 of the proposed data protection regulation also mention technical measures, which have an impact on the notification procedure in the case of data breaches.

and ranked based on two criteria: usage (relevant and widely deployed algorithms) and security (clear identification of the security of the scheme with appropriately selected parameters and key sizes).

Hence, ENISA will continue this activity during 2014, by reviewing the cryptographic recommendations annually to ensure appropriate data security, taking into account of similar work carried out in the Member States[32,33]. Furthermore, ENISA will extend its efforts to cover application scenarios, such as cloud computing and mobile devices. Other aspects such as the security requirments of network end points and on how to establish trust relationships (cf, secure computing base and new public key infrastructures) could also be investigated.

Best practice guide for prevention of data leakage and appropriate controls for the access of data using Security and Privacy by Design and by Default

The increasing use of online services has led to significant growth in the amount of citizens' personal data being transmitted over public networks (e.g. the Internet) and stored within applications that are accessible from anywhere on the Internet. Data leakage or security breaches in such systems have a direct impact on the right to privacy and may have legal implications. Moreover, citizens are exposed to financial risks, if financial information (e.g. banking details) is disclosed. Lastly, due to the quality and the quantity of data, leakages expose citizens to various risks and can cause substantial reputational damage to official bodies.

Since 2010 ENISA is actively working on the subject of data leakage and notifications about breaches. In 2014 this work will be complemented by a best practice guide addressed to the interest of the businesses containing recommendations for prevention of data leakage and appropriate controls for the access of data.

EU electronic identification and trust services framework

The European Commission adopted on June 4th 2012 a proposal for a Regulation[34] on electronic identification and trusted services for electronic transactions in the internal market that will replace the existing Directive 1999/93/EC[35] on a community framework for electronic signatures was the legal recognition of electronic signatures. The proposal 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 (electronic seals, electronic delivery services, electronic documents, time stamping services and web site authentication).

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

- Mechanisms for reporting security breaches by the trust service providers to the competent bodies.
- Minimum security measures and security best practices for trust services providers.

In 2014, ENISA will continue to support related activities relevant to the implementation of the provisions of the proposal, with a focus on the areas of:

[32] Commission Regulation 611/2013 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

[33] ETSI SR 002 176 "Algorithms and Parameters for Secure Electronic Signatures"

34 Proposal for a Regulation "on electronic identification and trusted services for electronic transactions in the internal market": http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:EN:HTML

[35] Directive 1999/93/EC on a community framework for electronic signatures was the legal recognition of electronic signatures: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

- Common audit schemes for trust services providers in Member States. Technical guidelines for independent auditing bodies and supervisory authorities. The work will refer to and take into account relevant regulatory frameworks [36]

At the end of 2012 ENISA organised the first Annual Privacy Forum (APF'2012) http://privacyforum.eu/ in partnership with DG CONNECT, -Cyprus Presidency of the Council of the EU and the University of Cyprus. The main objective of the APF, is to establish a forum fostering the exchange of information and experiences between the research and academic communities, and the EU policy and industry representatives. The response to the organisation of the first edition of the conference in 2012 indicates that APF can become an established reference event in the area of privacy putting emphasis on the need to bring together the policy and research communities.

Due to the delay in the new ENISA mandate decision process in 2013 it was premature to organise the 2013 edition of the Annual Privacy Forum. In this light, in Q3 2013 it was agreed to organise the 2nd edition of APF'2014 in the context of the Greek Presidency of the EU. Experience from APF'2012 clearly indicates that the collaboration model between DG CONNECT and ENISA in the joint organisation of APF is the way forward.

Outcomes & deadlines

The outcome of this work package will be:

- WPK 1.2-D1 : Engaging Cloud Computing Stakeholders in the EU's Cloud Computing Strategy and Partnership (workshops, contributions to Commission's SIGs and ECP work, Q2-Q4 2014)
- WPK 1.2-D2 – Engaging with stakeholders for the secure implementation of EU's Smart Grids policies (workshops, contributions to COM's EG 2 and MS actions, Q2-Q4 2014)
- WPK 1.2-D3 - Algorithms and parameters for secure services (study, Q4)
- WPK 1.2-D4 - Best practice guide for Privacy and Security by Design and Default for the prevention of data leakage and appropriate controls for the access of data (report, Q4)
- WPK 1.2-D5: Auditing framework for trust services: Technical guidelines for independent auditing bodies and supervisory authorities on the implementation of audit schemes for trust service providers in MS. (Report, Q3 2014)
- WPK 1.2-D6: Annual Privacy forum 2014 (APF'2014) (Workshop, report, Q2-Q4 2014)

Stakeholder impact

- Supporting the development of EU's Cloud Computing Strategy and Partnership especially in the areas of certification of sectorial cloud computing infrastructures, mapping of standards, rating of cloud computing services, pre-commercial procurement guidelines and incident reporting mechanisms.
- Supporting the development of EU's Smart Grids Strategy in the areas of Minimum Security Measures for Smart Grids, certification of Smart Grid components, privacy profile of Smart Meters, and incident reporting mechanisms.
- Supporting the development of EU's Incident Reporting Activities for CIIP sectors in the context of the Cybersecurity Strategy for the EU.
- 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.

[36] REGULATION (EC) No 765/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 July 2008, setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:en:PDF

- 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 Member States and service providers (i.e. minimum security requirements).
- Supporting the implementation of the Regulation on electronic identification and trusted services, which will enable the achievement of a harmonized market.
- Supporting the MS on the provision of secure eGovernment services in all levels of public administration.

Resources

- 140 kEuro
- 46,4 person months

Legal base & policy context

- ENISA regulation article 3
- European Commission's proposal on a comprehensive reform of data protection rules http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
- 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
- Proposal for a Regulation "on electronic identification and trusted services for electronic transactions in the internal market" adopted by the Commission on 4th June 2012.
- Commission Regulation 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

3.2.5 WPK 1.3: Supporting EU in education, research and standardisation

Desired Impact

- At least 5 members of the R&D community integrates NIS components in their activities and projects.
- 2 seminars or workshops organised to validate the usefulness of NIS Driving License material, addressed to different target audiences, with a minimum of 10 participants from several Member States.

Description of tasks

Inventory of standardisation activities in NIS, Privacy, Cloud Computing & Smart Grids

ENISA tracks the development of standards from a global perspective in the area of Network and Information Security. The Agency will monitor NIS standards EU wide and globally, including areas that are not specifically related to the ENISA work programme. This approach will enable ENISA to keep its stakeholders informed 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 during 2014 seeking out synergies with the Agency's work programme and involve standards bodies in the different work packages in as far as this is appropriate.

Moreover in 2014, ENISA will develop an inventory of relevant standardisation activities in the areas of NIS and privacy . ENISA will assess whether there is a gap between these standardisation activities and state of the art developments in NIS (including ENISA results).

Contribution/participation at the evaluation of the calls of proposals for EU funded R&D published by the European Commission

As was the case in previous years, ENISA will continue to support COM 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 Program 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 2014.

Collaboration with EU funded R&D projects

In the areas of interest to the ENISA Work Program the Agency wil continue to collaborate with and to support EU funded R&D projects. Such collaboration may be in the form of:

- Participating in the panel of reviewers that are supporting COM 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 COM 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 Program as presented in this document.
- Contributions to the various consultations launched by COM 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 intitiatives launched or about to be launched by the COM.

Early Warning and Response System against cyber-attacks and disruptions

In the context of the publication of the Cybersecurity Strategy for the EU and the Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high

common level of network and information security across the Union (COM(2013) 48 final), the European Commission has launched a feasibility study on the implementation of a European-wide Early Warning and Response System (EWRS) against cyber-attacks and disruptions.

The scope of this EWRS would be focused on major incidents with transnational impact on the functioning of the ICT infrastructure or services that require a coordinated response from several Member States. In addition, this platform would encourage the sharing of best practices between the competent authorities and their constituency.

Subject to the approval of the NIS Directive, ENISA will collaborate with COM in the implementation of this study providing advice and input to the study team when called upon and according to the needs of COM.

Contribution to the 'EU NIS Driving Licence'

Together with relevant stakeholder community, ENISA will drive the development of a roadmap for the implementation of a "Network and Information Security driving licence". This roadmap will cover the needs of different levels of education, e.g. primary, secondary and tertiary education. The roadmap will exploit existing material and synergies among relevant training bodies. Within this activity, ENISA, in cooperation with COM, will assist in:

- identifying partners to produce the material for the defined curricula,
- identifying partners to lecture courses and seminars implementing this curricula, and
- upon feasibility, organising pilot courses and seminars related to the "NIS driving licence".

Outcomes & deadlines

The outcome of this work package will be:

- WKP1.3-D1 – Inventory of standardisation activities in NIS and Privacy (Workshops, report, Q1-Q4, 2014)
- WPK1.3-D2 – Roadmap for the implementation of the "NIS Driving license"

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 areas of:

- Standardisation related to NIS, Privacy, Cloud Computing and Smart Grids,
- Harmonisation of EU-wide NIS education.

Resources

- 40 kEuro
- 21,9 person months

Legal base & policy context

- 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

[37] http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item_id=6117&lang=en&tpa_id=0&title=Security-industry%3A-Commission-proposes-programme-to-enable-further-growth-

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, andan 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.

- 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. EU institutions should seek its opinion on policy implementation.
- Council Conclusions on CIIP Action Plan (May 2011)

3.3 WS2- Support capacity building

3.3.1 Overview

Justification

This work stream aims at supporting ENISA's key stakeholders in developing new operational and policy capabilities to address the various challenges in cybersecurity and to extend existing capabilities (where appropriate). This will be achieved by collecting and disseminating good practice for public and private sectors and for the European citizen in general. Where applicable,

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

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

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

ENISA will actively support EU Member States and institutions to apply these good practices, for example by contributing to local awareness raising events, delivering technical training to CERT staff, and other means.

Protecting Critical Information Infrastructure (CIIP) is a key priority for Member States, the Commission and industry (operators, service providers, manufacturers). By facilitating cooperation and coordination among Member States, ENISA will continue to support all in developing sound and implementable preparedness, response and recovery strategies, including those policies and measures that are necessary to meet the challenges of a continually evolving threat environment.

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

The Agency assists EU Member States, the Commission and the private sector in sharing knowledge and experience with each other in key sectors (e.g. Cloud Computing, Smart Grids, ICS-SCADA), on key information security topics (e.g. minimum security measures) and to develop good practices and recommendations that would be of mutual benefit to all. This way public and private stakeholders will be better prepared to coordinate and cooperate with each other durinng a cyber crisis.

Key action 3 of the European cloud strategy [ref. COM(2012)529] aims at supporting Member States, associated countries and industry in preparing sound approaches for cloud computing adoption. This will be achieved by setting up a European Cloud Partnership (ECP) bringing together leading public sector actors from all over Europe cooperating with industry consortia. It will address issues such as safe and secure cloud usage, data protection and others. ENISA's work will be aligned with the work in the European Cloud Partnership.

The Agency also will also offer targeted assistance to EU Member States that wish to improve their security standing in certain areas (e.g. training on national exercises, cyber security strategies).

The private sector is the main owner of current critical information infrastructures. The effective co-operation between public and private sector is important for the swift implementation of ICT security measures in relevant sectors and services. The NIS Platform will be an important instrument in enabling such co-operation to flourish.

Specific Policy Context

Specific policy references for this work stream are as follows:

- ENISA Regulation article 3
- CIIP Action Plan 2009 and 2011
- Council Conclusions on CIIP Action Plan (May 2011)
- Digital Agenda 2010
- EU 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
- COM Recommendations on preparations for the roll-out of smart metering systems.Overall Objectives

Overall Objectives

The objectives of this Work Stream are to:

- Support Member States in developing capabilities in important areas (e.g. exercises, strategies, CERTs, governmental clouds, etc.)
- Leverage the NIS Platform as a tool to enhance public private co-operation
- Provide advice and assistance to targeted stakeholder communities (e.g. cloud computing, Smart Grids, ISPs, etc.)
- Develop minimum security measures in the areas of cloud computing, Smart Grids, ISPs
- Keep up to date and enhance the operational capabilities of Member States' institutions by helping the CERT community to increase its level of efficiency and effectiveness.
- Develop and promote the use of training and exercise material

3.3.2 Work Packages

The following work packages constitute the Work Stream:

- WPK 2.1 : Support Member States' Capacity Building: The objective of this work package is to support the development of prevention, detection, analysis and response capabilities within Member States institutions and EU institutions.
- WPK 2.2 : Support Private Sector Capacity Building: The objectives of this work package is to enhance the capabilities of the private sector through co-operation with the public sector in several areas namely smart grids, ICS-SCADA, Cloud Computing, Finance and electronic communication networks.
- WPK 2.3: Raising the level of preparedness of EU citizens: The objective of this work package is to (a) support awareness raising and training activities in Member States to develop the security dimension in the use of ICTs and (b) support the organization of the cyber security month by providing expertise related to the activities of ENISA.

3.3.3 WPK 2.1: Support Member States' Capacity Building

Desired Impact

- 10 Member States and 5 private companies support ENISA's conclusions on national cyber security strategies
- Improved operational practices of CERTs (on-going support with best practices development) training provided to a minimum of 20 participants of different organisations
- 6 Member States and 10 private companies support ENISA recommendations on national PPPs

Description of tasks

The objective of this work package is to support the development of prevention, detection, analysis and response capabilities within Member States institutions and EU institutions. Corresponding actions aimed at the private sector are detailed in WPK 2.2.

Cyber Security Strategies - CSS

ENISA will continue to support Member States in developing their capabilities in the area of National Cyber Security Strategies (NCSS). The Agency, building on previous work in the area of NCSS, will act as facilitator among Member States and foster the sharing of good practices. ENISA will continue offering targeted assistance to Member States on the development of new NCSS, evaluation of existing ones or the development of elements of a NCSS. The Agency will also bring Member States and the private sector together to share experiences and good practices on NCSS or invidual elements of an CSS. This work will be summarised by a status report about the deployment of NCSS in the EU.

ENISA will take stock of existing evaluation/assessment mechanisms of NCSS, identify good practices, validate them with public and private sector and finally issue a white paper with practical recommedations on the evaluation and update of existing NCSS.

Developing CERT Capabilities

Whilst the EU Member States acknowledge the need to establish competent national/governmental CERTs on national level, the level of those capabilities vary greatly from Member State to Member State. In addition, the EU has recently established its own CERT in form of the CERT-EU, whose goal is to protect the EU institutions.

It is one of ENISA's primary goals to support all Member States and EU institutions in their efforts to build up effective CERTs, to reach a specific level of capabilities and, where possible, extend those to provide even better services. Underpinning this work is a set of "Baseline capabilities", which are competencies defined in four key areas (operational, technical, mandate and cooperation). These are agreed with the CERT teams in the Member States, and constantly monitored and updated by ENISA. To help CERTs to implement these baseline capabilities ENISA provides support in the form of good practice material, training and exercises.

In 2014, ENISA will build upon its work in this area, but will also take stock of its work in the area of CERTs in the last 8 years. The goal will be to concisely draw "lessons learned" through a dialogue with relevant stakeholders, and to draw a roadmap of CERT activities for the coming years.

Concrete Activities in this area are as follows:

- Take stock of achievements, good practice and experiences from 8 years of work in the area of CERT, with the goal to develop a roadmap and plan the work ahead.
- Enhance training and exercising methodology ("learning loop") to improve the competencies of trainers. This will be supported by a collection of "use cases" and "lessons learned" from existing trainings and team exercises

- To support above mentioned action, further actively support capability building for CERTs by delivering (on request) trainings and suitable exercises to technical staff from EU Member States, EU institutions and other appropriate audiences
- Extend good practice collection with new training and exercise material for CERTs and (potentially) communities in the four areas of the "Baseline capabilities"
- Together with suitable stakeholder groups (like the FIRST Education SIG) investigate how to best apply ENISAs training material, and how to integrate suitable trainings and material from other communities (NIST, ISACA, etc.)One of the topics for new good practice/training material will be to Identify suitable mechanisms for gathering, processing and exchange of actionable information (format, channels, etc.) to support the effective and efficient exchange of operational data among teams

Support of regional, sector-specific and national cyber exercises

In the past, the Agency has supported national, regional and sectorial cyber exercises efforts upon request (Art14 of the ENISA regulation). This effort will continue in 2014 in line with the ENISA regulation, the EU Cybersecurity Strategy and the EU Member States' needs. Where appropriate the Agency will collaborate with and support regional or sectorial cyber exercises in a cost efficient manner, for example by re-using exercise planning and management knowledge and tools from other exercises and efforts.

National and European PPPs

ENISA will continue supporting Member States 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 advice on national PPPs (e.g. in a form of a seminar or training). In certain areas ENISA will try to transfer experiences from existing, successful Member States to other Member States. ENISA will also try to engage National PPPs into the NIS platform.

Outcomes & deadlines

- WPK2.1 - D1 : Assisting MS in building capabilities on NCSS (workshops, Q1-Q4)
- WPK 2.1 – D2 : White Paper – How to Evaluate a National Cyber Security Strategy (report, Q3 2014)
- WPK2.1 - D3 : Good practice guide on training methodologies, etc. for operational teams and communities like CERTs ("Train the trainers handbook") derived from experiences from delivering suitable CERT training (Q4 2014)
- WPK2.1 - D4 : Regular update of "Baseline capabilities" definition and status and conclusions for new training material (Q4, 2014)
- WPK2.1 - D5 : New set of CERT exercise material with at least five new scenarios from the four areas of the "Baseline capabilities", including the topic of processing of actionable operational information (Q4 2014)
- WPK2.1 - D6 : Stocktaking of achievements in the area of CERTs and a draft roadmap to plan future work in this area, in close cooperation with the CERT community and the Member States (Q4 2014)
- WPK2.1 – D7 : Assisting MS in building capabilities on national PPPs (workshops, Q1-Q4)

Stakeholder impact

Member States will benefit from the experience of their peers through a process of collaboration that will be established by the Agency. In addition, the report in this area will serve as a point of reference for those Member States who choose to develop a strategy at a later date.

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

Member States will also develop capacity on national PPP. ENISA will help advanced Member States to assess or improve existing policies, measures or actions through the co-operation and information sharing with their peers.

In the area of CIIP and Resilience, ENISA will share knowledge and expertise with Member States and the private sector on testing frameworks for ICS-SCADA systems or on minimum security measures for Smart Grids or on how to develop governmental clouds.

Finally, through its expertise in the area of article 13 a and article 4, ENISA will be able to assist NRAs with the proper implementation of incident reporting schemes at national level. This will involve participating in workshops organised by NRAs at national level with ISPs and Telecommunications organisations to better explain how article 13 a and article 4 can be implemented.

Resources

- 290 kEuro
- 66,0 person months

Legal base & policy context

- ENISA Regulation, in particular art. 3 (Tasks)
- 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)
- European Commissions' Communication on "Towards a general policy on the fight against cyber crime", COM(2007) 267 final

3.3.4 WPK 2.2: Support Private Sector Capacity Building

Desired Impact

- 10 Member States and 20 Private Companies contribute to NIS Platform Working Groups
- 10 ICS-SCADA providers/manufacturers support ENISA's conclusions on the the Certification of Cyber Security Skills of ICS-SCADA experts
- 15 Cloud Computing Providers and 5 Member States competent authorities contrinute to ENISA's study on minimum security measures for cloud computing
- 12 Cloud Computing Providers and 5 Member States competent support ENISA's conclusions on Procurement Guidelines for Cloud Computing Providers
- 10 Finance Sector IT Security/IT Auditors agree on ENISA's recommendations on secure inter-banking communications and transactions.
- 10 e-comms providers support the Harmonised Minimum Security Measures for ISPs

Description of tasks

The initiatives described below are intended to improve the capacity of the Member States for dealing with large scale cyber incidents, by improving the state of preparedness of the private sector community. ENISA will assist Member States in achieving this by providing assistance and advice but will not become engaged in operational work.

Leverage the NIS Platform as a tool to enhance public private co-operation

From 2011-2013, the European Public Private Partnership for Resilience (EP3R) has covered a number of key areas mostly in the areas of Internet, telecommunications infrastructure, cloud computing and Smart Grids.

In 2014, ENISA will continue supporting the NIS platform, the successor of EP3R, with the goal of engaging more targeted public and private stakeholders, especially experts from small industry players. ENISA will support the working groups and their chairpersons (e.g. via the resilience portal, conference calls), contribute to the outcomes of the working groups, and ensure its quality. The Agency will keep the working groups informed about the latest developments in their respective areas including deliverables done by the Agency (e.g. art. 13 a Working Group).

Through such interactions with the stakeholders ENISA will identify new topics in emerging areas (e.g. mobile applications, eHealth, insurance or finance sector) and investigate ways to analyse them in the future.

Provide advice and assistance to targeted stakeholder communities

In 2014, we will focus on the following areas:

Smart Grids: ENISA will promote to relevant stakeholders its existing work on "Minimum Security Measures for Smart Grids" and will aim at aligning them with the work of CEN/CENELEC/ETSI (M/490 SG-CG/SGIS Working Group), ERNCIP and other EU initiatives. These measures might be the basis of a Commission Recommendation. ENISA will also work with relevant public and private stakeholders to assess the challenges and requirements of national certification schemes for Smart Grids, consult with them (e.g. SOGIS) and issue a white paper with practical recommendations on the matter. In addition the Agency will take stock of existing initiatives on the certification of cyber security skills of ICS-SCADA experts and issue practical recommendations to stakeholders for the wide deployment of such schemes. Finally ENISA will analyse the area of proactive operational preparedness measures for ICS-SCADA (e.g. intrusion detection, honeypots, etc.) and consult with public and private stakeholders on the proper deployment of them.

Electronic communications sector (ISPs and telecommunications companies): ENISA, building on its relevant work carried out in previous years, will develop one single, integrated set of minimum security measures for electronic communications providers taking into consideration the requirements of both article 13 a and article 4. This will enable providers to address security, privacy and confidentiality issues in an integrated manner. The Agency will also take stock of existing methodologies to identify critical assets and services of data communication networks. In co-operation with ISPs and public stakeholders, ENISA will identify good practices, assess them and develop guidelines on the identification of critical services, assets and links at national and cross country levels. In addition ENISA will continue serving as advisor to the EU sponsored project on botnets (ACDC[41]). The Agency will provide technical expertise on several issues related to botnets (e.g. how to mitigate and response to cyber attacks, how to disinfect wide-scale and systematic malware threats).

Cloud Computing: ENISA, in co-operation with public and private stakeholders, will develop and agree on a set of Minimum Security Measures and adequate maturity levels for cloud computing providers. Providers will then have a baseline of measures and maturity levels to use for improving their security. The Agency will also continue its work in the area of critical clouds by analysing how cloud computing can be securely used in specific critical sectors like ehealth, insurance and finance. Finally the Agency, in consultation with public and private stakeholders, will take stock of existing corporate, national, EU and international procurement guidelines for the secure deployment of cloud computing and issue relevant recommedations in the form of a white paper.

Finance: ENISA will identify relevant experts from the financial sector to analyse the security and resilience of inter-banking communications and transactions. The Agency, through a dedicated expert group consisting of experts from public and private sector, will assess the challenges of inter-banking communications and transactions, identify possible areas of improvement and issue recommedations that will improve the security of such transactions.

Outcomes & deadlines

- WPK2.2-D1 : Support the Working Groups of the NIS Platform (workshops, contributions, technical support, Q1-Q4, 2014)
- WPK2.2-D2 : White Paper on the Certification of Smart Grids (report, Q3, 2014)
- WPK2.2-D3 : White Paper on the Certification of Cyber Security Skills of ICS SCADA experts (report, Q3 2014)
- WPK2.2-D4 : Harmonised Minimum Security Measures for ISPs (report, Q4 2014)
- WPK2.2-D5 : Minimum Security Measures for Cloud Computing (report, Q4, 2014)
- WPK2.2-D6 : White Paper - Procurement Guidelines for Secure Cloud Computing Deployment (report, Q4, 2014)
- WPK2.2-D7 : Guidelines for the Identification of Critical Services, Assets and Links in Electronic Communication Networks (report, Q4, 2014)
- WPK2.2-D8 : Guidelines for Secure Inter-Banking Communications and Transactions (report, Q4, 2014)

[41] http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=325188

Stakeholder impact

- Cloud Computing
  - A number of governmental clouds are being set-up. A single framework for governmental cloud computing, (1) allows Member States to share and exchange knowledge on best-practices, (2) allows providers to cater for different Member States more easily, without having to adjust the cloud technology to different requests in different countries, ultimately lowering the costs, (3) allows Member States to move computing work loads 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 Member States 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 Member States, by avoiding the creation of the "weakest link";
  - Ensuring a minimum level of harmonisation on security and resilience requirements across Member States 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;
  - Provide guidance to certificate providers on the content of ICS-SCADA security courses and curricula;
  - Raise the level of awareness as regards cyber security issues within the organization.
  - Provide guidance to vendors and asset owners on how to manage and then disclose discovered vulnerabilities.
  - 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 Member States and at EU level 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 Member States' 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 Member States' 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.

Resources

- 185 kEuro
- 41,5 Person Months

Legal base & policy context

- ENISA Regulation article 3
- 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
- COM Recommendations on preparations for the roll-out of smart metering systems.

3.3.5 WPK 2.3: Raising the level of preparedness of EU citizens

Desired Impact:

- At least 20 of the EU Member States involved in the European Cyber Security Month;
- Ensure that a minimum of 5 Member States support the cyber security championship;
- Improved consultation process in order to feed the activities of next years;

Description of tasks

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

This work package is in line with the principle of shared responsibility to ensure security, as stated in section 1.2 of the Cybersecurity Strategy for the EU[42], which calls for empowering users "*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*."

Statistics show[43] that although Internet users express high levels of concern about cyber security and becoming victims of cyber-attacks, it is difficult to get them to adopt enhanced security behaviour. In many cases, this change occurs too late to avoid incidents.

Through its NIS expertise, ENISA will participate together with different stakeholders in actively promoting cybersecurity awareness.

The Agency will support the COM to to develop the security dimension in the use of ICTs in Member States:

- Establish partnerships with academic institutions and provide information and expertise in its core areas in order to feed the academic curricula and reading recommendations with ENISA reports
- Cooperate with educational bodies to successfully organize a cyber security championship where university students will compete in proposing NIS solutions
- Step up national efforts for the creation of a voluntary certification programme to promote enhanced skills and competence of IT professionals

The European Cyber Security Month (ECSM) will be further consolidated taking into account four basic principles:

- Guide content and priorities based on the analysis of ENISA subject matter experts.
- Support the multi-stakeholder governance approach
- Encourage common public-private activities
- Assess the impact and adapt to the challenges

[42] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667
[43] Special Eurobarometer 390 / Wave EB77.2 EU citizens' experience and perceptions of cyber security issues http://ec.europa.eu/public_opinion/archives/eb_special_399_380_en.htm

Outcomes & deadlines

- WPK 2.3-D1 - Provide technical guidance and support for European Cyber-Security Month (dissemination material, Q4 2014);

Stakeholder impact

The direct beneficiaries of the results of this work package 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 more targeted information on the security dimension in the use of ICTs;
- Develop an increased knowledge and corresponding ICT skills by being part of a best practice sharing community;
- Increase their level of contact with stakeholders of similar profiles

Resources

- 20 kEuro
- 13,1 person months

Legal base & policy context

- ENISA Regulation (New mandate September 2013)
- ENISA Stakeholder Strategy
- Cybersecurity Strategy for the EU
- Council Resolution of 18 December 2009
- Internal Security Strategy for the European Union

3.4 WS3 – Support cooperation

3.4.1 Overview

Justification

Various key policy documents identify the cooperation among stakeholder and stakeholder groups as among the most important activities to enhance and strengthen NIS in the European single market, and to ensure that Europe is placed among the key players in this field on an international scale.

Cooperation is a necessary prerequisite for strengthening the capacities of Member States, EU institutions and third countries. In particular:

- The exchange of ideas, good practice and a common exploration of areas of NIS (generating of new good practices in fields of upcoming technologies, respond to new threats, etc.) will enable EU Member States, the EU institutions and other players to improve services, workflows, communication, etc in order to prepare properly for emergency cases.
- In times of large scale crises, previous collaboration and planning will help to ensure the right mitigation mechanisms, enabling a response with a much lower cost both in time and resources than would be possible without previous cooperation.

One very important element of this work is to build upon existing collaboration in already existing communities, and to further enhance community building in Europe and beyond. Since the creation of ENISA, the Agency has been building trust amongst these communities, bridging the gap between the products and services offered in the market and their needs, continuously updating the information provided to those implementing NIS policy. The secondary aim of this work stream is to ensure that ENISA's supporting role for these communities is maintained. One important means of achieving this is the development of tools to facilitate and improve the international communication and interchange of security relevant information within communities sharing the same interest in different Member States.

Specific Policy Context

Specific policy references for this work stream are as follows:

- ENISA Regulation article 3
- Directive 2009/140/EC, Art. 13a
- CIIP Action Plan 2009 and 2011
- Digital Agenda 2010
- Cybersecurity Strategy for the European Union
- Council Resolution of 18 December 2009
- Internal Security Strategy for the European Union

Overall Objectives

- Support and enhance co-operation between CERTs, and with other communities.
- Organise and manage the next Cyber Europe 2014
- Support Member States and the Commission on the development of a sound European Cyber Crisis Cooperation Framework, national contingency plans and national exercises
- Continue ENISA's work on article 13a (security breach notification) and article 4 (personal data breach notification) and develop synergies between the two initiatives
- Strengthen the cooperation with the newly established European Cybercrime Centre (EC3) in the areas where ENISA and EC3 are jointly involved
- Support the implementation of the new Regulation on electronic identification and trusted services

- Analyse the requirements for incident reporting schemes in the areas of cloud computing and smart grids. Identify and approach new communities and other groups who can contribute to enhance NIS
- Identify characteristics, needs, etc. of specific communities and other groups, and propose good practice for common problems
- Determine (scalable, accepted) methods for trust building among communities and other groups
- Facilitate the bringing together of communities and other groups face-to-face (mitigate obstacles, finding ways to collaborate within constraints and contribute to trust building)
- Identify actionable, complementary information for various communities
- Identify obstacles (technical, legal, etc.) preventing the effective exchange of information information
- Identify suitable mechanisms for information gathering, processing and exchange (format, channels, etc.)
- Identify what types of information should be exchanged and who would be the beneficiaries.

3.4.2 Work Packages

The following work packages constitute the Work Stream:

- WPK 3.1: Crisis cooperation – exercises. The objective of this work package is to prepare and carry out the next Cyber Europe Exercise in 2014, in close collaboration with all relevant stakeholders.
- WPK 3.2: Implementation of EU legislation. The objectives of this work package are on the one hand the continuation of work in the area of Incident Reporting (Article 13a) by analysing the received data. On the other hand it aims at preparing the reporting for Articles 4 of the ePrivacy Directive and Article 15 of the COM proposal for the Regulation on eID and trusted services.
- WPK 3.3: Regular cooperation among NIS communities. The objective of this work package is to further enhance the cooperation between operational communities, mainly CERTs and Law Enforcement Agencies. New potential target groups for ENISA deliverables (esp. training but also other means) might be identified during that work with the initial communities.

3.4.3 WPK 3.1: Crisis cooperation – exercises

Desired Impact

- At least 24 EU Member States and EFTA countries confirm their support for Cyber Europe 2014 (CE2014)
- At least 80% of Member States that are in the process of establishing National Contingency Plans by 2016 are supported by ENISA.
- At least 24 Member States are familiar with the operational procedures during cyber crisis by 2016

Description of tasks

This work package focuses on the following topics:

- Continuation of the work in the area of pan-European cyber exercises (Cyber Europe 2014)
- Enhancement of the capacity to support and organise cyber exercises
- Identification of good practices and improvement of operational procedures for cyber crisis cooperation in Europe

Pan-European Cyber Exercises: Cyber Europe 2014

In 2014, ENISA will organise the third pan-European cyber exercise, Cyber Europe 2014 (CE2014). This exercise will build on the experience gained in previous exercises and will take account of previous recommendations. The exercise will be more ambitious than previous efforts, e.g., technical depth, scenarios, stakeholders involved, objectives, procedures to be tested, complexity etc.

The exact setup and exercise plan will be agreed with the EU Member States and EFTA countries, in line with the EU Cybersecurity Strategy. Each country will be represented in the Exercise Planners group. This group will be responsible for the approval of the exercise setup and plan. The approach that will be followed will be an "opt-in scheme" for the identification of stakeholders in the countries which are interested to play in the exercise (e.g. policy level), allowing for the countries who wish and have the appropriate resources to extend their national play. ENISA will not invite additional third countries or stakeholder communities to participate in future EU cyber security exercises without having first obtained the approval of ENISA's Management Board.

Enhancing 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, such as the one with DG JRC. For example, more structural links will be established with the European Cybercrime Centre and the European Defence Agency.

EU-US Cybersecurity Exercise

ENISA will support COM and the Member States in planning, organising and executing a second EU-US cybersecurity exercise. The effort will be driven by the requirements set by the involved parties: COM, EU MS and US. The exact planning, the timelines and the actual execution of the exercise will be decided by a group of exercise planners composed by representatives from the involved parties. The exercise report summarising the key results and learning points will be verified with all involved parties before publication.

Cyber Crisis Cooperation and Exercises activities overview

ENISA will continue to support MS in the maintainance and training of operational procedures for cyber crisis cooperation. This and the activities described above including key findings in the area of

Cyber Crisis Cooperation and Exercises (C3E) will be summarised in an report at the end of 2014. This report will help ENISA to reach out to other communities/sectors with lessons learnt from supporting exercises (achieving broader impact).

Outcomes & deadlines

- WPK 3.1-D1: Cyber Europe 2014: Exercise Plan and Exercise (exercise, Q4 2014)
- WPK 3.1-D2: Report on Cyber Crisis Cooperation and Exercise Activities and Findings (report, Q4 2014)
- WPK 3.1-D3: EU-US Cybersecurity Exercise Plan

Stakeholder impact

The direct beneficiaries of the results of this work programme will be:

- EU and Member States' 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

- 201,5 kEuro
- 55,7 person months

Legal base & policy context

- ENISA Regulation article 3
- 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

3.4.4 WPK 3.2: Implementation of EU legislation

Desired Impact

- 23 Member States contribute to ENISA's work on the implementation of Article 13a and 12 Member states directly use the outcomes of this work by explicit references or by adopting the same approach nationally.
- 10 Member States contribute to the work facilitated by ENISA on implementing and enforcing article 4 and 6 Member States make direct use of the outcomes of this work by explicit references or by adopting the same approach nationally.
- 10 Member States contribute to ENISA's work on implementing article 15

Description of tasks

This work package focuses on:

- Support for the implementation of Article 13a (security breach notification) and Article 4 (personal data breach notification) and the development of synergies among the two
- Support for the implementation of the new Regulation on electronic identification and trusted services
- Analysis of the requirements for incident reporting schemes in the areas of cloud computing and smart grids

Security & Data Breach Reporting Schemes

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, 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.

ENISA will continue its efforts to bring NRAs and DPAs together to agree on a harmonised implementation of the security and data breach articles (art. 13 a and art. 4). In that respect the Agency will assess the two incident reporting schemes (article 13 a 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.

Support the implementation of the new regulation on electronic identification and trusted services

The European Commission adopted on June 4th 2012 a proposal for a Regulation[44] on electronic identification and trusted services for electronic transactions in the internal market that will replace the existing Directive 1999/93/EC[45] on a community framework for electronic signatures.

ENISA has already contributed to this area by providing recommendations on the reporting of security breaches by the trust service providers to the competent bodies started to address the implementation of security risk assessment by trust service providers and related security measures.

[44] Proposal for a Regulation "on electronic identification and trusted services for electronic transactions in the internal market": http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:EN:HTML

[45] Directive 1999/93/EC on a community framework for electronic signatures was the legal recognition of electronic signatures: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

In 2014, ENISA will continue its efforts on this incident reporting scheme as well as on the implementation of relavant security measures. More specifically, the Agency will identify and bring together the competent regulatory bodies of the Member States and debate with them on the proper implementation scheme of article 15. ENISA will use this group to properly define the scope of incident reporting, the parameters and thresholds as well as the affected services. The Agency will exploit all possible implementation and conceptual synergies with article 13a and article 4.

Support for the implementation of the NIS Directive

Subject to the approval of the NIS Directive, ENISA will assist the Commission and Member States in its implementation. The Agency could provide technical assistance on the requirements of the trusted information platform and the rules for sharing information on threats and vulnerabilities. In addition the Agency could assist the Commission in defining the affected sectors and the relevant stakeholders in each one of them. Finally the Agency, building on its experience with article 13 a and 4, can work with public stakeholders to define the incident reporting modalities for each sector, (the affected services, the parameters and thresholds, the reporting scheme and template, the rooting causes, and the scope of the analysis).

Outcomes & deadlines

- WPK 3.2-D1 - Analysis of Annual 2013 Incident Reports and Recommendations on addressing significant incidents (report, Q2/3 2014)
- WPK 3.2-D2 – Guidelines on Incident Reporting Scheme for Article 15 (report, Q4 2014)
- WPK 3.2–D3 - Support the implementation of the NIS Directive (workshops, Q2-Q4)

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.

Resources

- 130 kEuro
- 33,8 Person Months

Legal base & policy context

- ENISA regulation article 3
- Cybersecurity Strategy of the European Union
- Article 13a of the revised Framework Directive on electronic communications (Directive 2009/140 EC)
- Commission Communication on CIIP (2009 and 2011)
- Article 4 of ePrivacy Directive
- Reform of Data Protection legislative framework
- Directive 1999/93/EC on a community framework for electronic signatures was the legal recognition of electronic signatures.
- Proposal for a Regulation "on electronic identification and trusted services for electronic transactions in the internal market" adopted by the Commission on 4th June 2012.

3.4.5 WPK 3.3: Regular cooperation among NIS communities

Desired Impact

- At least 10 Member States and 2 national / international LEA support the conclusions of the 9th ENISA CERT workshop.
- At least 10 Member States support the Good Practice Guide and / or (where applicable) training and exercise material for the exchange and processing of actionable information by CERTs
- 10 operational CERTs agree to adopt the recommendations of stocktaking on channels and formats for exchange of operational information
- 2 CERTs agree to pilot the good practice material for first responders (material developed in cooperation and accordance with the EC3) (Q4)

Description of tasks

Threats to cybersecurity and cyber-attacks respect no organisational and territorial boundaries. For that reason, effective cooperation between communities at all levels is required to facilitate the exchange of the information and knowledge needed to reduce vulnerability and provide effective responses to cyber incidents. This includes CERTs within particular business sectors which might be affected by large-scale incidents, other incident responders within a country serving other communities, national / governmental CERTs, law enforcement agents and internationally recognised research and development organisations.

Specific tasks to be included under this area are given below:

- Actively support or (when appropriate) organise common trainings including communities such as CERTs and LEA (for example support exercises organised by the Financial ISAC (FI-ISAC) initiative)
- Engage with the European Cyber Crime Centre (EC3), where appropriate, through formal and informal cooperation channels, to leverage synergies while respecting the respective mandates.
- Take stock of existing communities up to date to cyber security challenges that could be beneficial for the work of CERTs (like for example in the area of ICS)
- Facilitate the outreach (when appropriate) to those other bodies and/or communities with similar tasks (and broaden the focus more, to reach out to new communities as well), including taking stock of scalable and accepted methods for trustbuilding within and among communities
- Continue collecting good practice useful for CERTs and LEAs, and further enhance the ENISA exercise and training material.

Outcomes & deadlines

- WPK3.3-D1 : 9th ENISA CERT workshop to prepare a roadmap for future work of ENISA in the area of CERT training and CERT cooperation with LEA (in collaboration with EC3) (Q4)
- WPK3.3-D2 : Good practice guide and / or (where applicable) training and exercise material for the exchange and processing of actionable information by CERTs (Q4 2014)
- WPK3.3-D3 : Draft report "Stocktaking on channels and formats for exchange of operational information"
- WPK3.3-D4 : Draft report "Scalable and accepted methods for trustbuilding within and among communities"
- WPK3.3-D5 : Good practice material for first responders in cooperation with the EC3 (Q4)

Stakeholder impact

- n/g CERTs and Member States' policy makers

- LEA units
- IT managers

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

Resources

- 127,5 kEuro
- 46,4 person months

Legal base & policy context

- ENISA Regulation, in particular art. 3 (Tasks)
- 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)
- 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

3.5 Summary of core operational activities

Core Operational Activities: Workstream 1-3				
WS1	**Support EU Policy Building**	**Budget**	**Person months (R&A)***	**FTE**
WPK 1.1	Identifying evolving threats, risks and challenges	100.000	20,9	2,2
			(12,9)	
WPK 1.2	Contributing to EU policy initiatives	140.000	46,4	4,8
WPK 1.3	Supporting the EU in education, research & standardisation	40.000	21,9	2,3
			(9,6)	
Total WS 1		**280.000**	**89,2 (22,5)**	**9,3**
WS2	**Support Capacity Building**	**Budget**	**Person months (R&A)***	**FTE**
WPK 2.1	Support Member States' capacity building	290.000	66,0	6,9
			(0,5)	
WPK 2.2	Support private sector capacity building	185.000	41,5	4,3
WPK 2.3	Support the EU citizens' capacity building	20.000	13,1	1,4
Total WS2		**495.000**	**120,6 (0,5)**	**12,6**
WS3	**Support Cooperation**	**Budget**	**Person months (R&A)***	**FTE**
WPK 3.1	Crisis cooperation - exercises	201.500	55,7	5,8
WPK 3.2	Implementation of regulations	130.000	33,8	3,5
WPK 3.3	Law enforcement & NIS cooperation	127.500	46,4	4,8
			(0,5)	
Total WS 3		**459.000**	**135,9 (0,5)**	**14,2**
Total WS 1-3		**1.234.000**	**345,6 (23,5)**	**36,0**

** figures in brackets represent person months of Research & Analyses team, included in total figure of particular WPK*

Missions	Budget	Person months	FTE
Missions of all staff	**500.000**	**0,0**	**0,0**

3.6 Summary of Core Operational Activities with deliverables

WS1	**Support EU Policy Building**
WPK1.1	**Identifying technological evolution, risks and challenges**
D1	Annual EU CyberSecurity Threats Landscape.
D2	Identification of trends, security challenges, associated risks and required countermeasures, for emerging technologies (with special attention to selected areas/sectors).
WPK1.2	**Contributing to EU policy initiatives**
D1	Engaging Cloud Computing Stakeholders in the EU's Cloud Computing Strategy and Partnership (workshops, contributions to Commission's SIG and ECP work, Q2-Q4 2014)
D2	Engaging with stakeholders for the secure implementation of EU's Smart Grids policies (workshops, contributions to COM' EG 2 and MS actions, Q2-Q4 2014)
D3	Algorithms and parameters for secure services (study, Q4)
D4	Best practice guide for Privacy and Security by Design and Default for the prevention of data leakage and appropriate controls for the access of data (report, Q4)
D5	Auditing framework for trust services: Technical guidelines for independent auditing bodies and supervisory authorities on the implementation of audit schemes for trust service providers in MS. (Report, Q3 2014)
D6	Annual Privacy forum 2014 (APF'2014) (Workshop, report, Q2-Q4 2014)
WPK1.3	**Supporting the EU in education, research & standardisation**
D1	Inventory of standardisation activities in NIS and Privacy (Workshops, report, Q1-Q4, 2014)
D2	Roadmap for the implementation of the "NIS Driving license"
WS2	**Support Capacity Building**
WPK2.1	**Support Member States' capacity building**
D1	Assisting MS in building capabilities on NCSS (workshops, Q1-Q4)
D2	White Paper – How to Evaluate a National Cyber Security Strategy (report, Q3 2014)
D3	Good practice guide on training methodologies, etc. for operational teams and communities like CERTs ("Train the trainers handbook") derived from experiences from delivering suitable CERT training (Q4 2014)
D4	Regular update of "Baseline capabilities" definition and status and conclusions for new training material (Q4, 2014)
D5	New set of CERT exercise material with at least five new scenarios from the four areas of the "Baseline capabilities", including the topic of processing of actionable operational information (Q4 2014)
D6	Stocktaking of achievements in the area of CERTs and a draft roadmap to plan future work in this area (Q4 2014)

D7	Assisting MS in building capabilities on national PPPs (workshops, Q1-Q4)
WPK2.2	**Support private sector capacity building**
D1	Support the Working Groups of the NIS Platform (workshops, contributions, technical support, Q1 – Q4, 2014)
D2	White Paper on the Certification of Smart Grids (report, Q3, 2014)
D3	White Paper on the Certification of Cyber Security Skills of ICS SCADA experts (report, Q3 2014)
D4	Harmonised Minimum Security Measures for ISPs (report, Q4 2014)
D5	Minimum Security Measures for Cloud Computing (report, Q4, 2014)
D6	White Paper - Procurement Guidelines for Secure Cloud Computing Deployment (report, Q4, 2014)
D7	Guidelines for the identification of critical services, assets and links in Electronic Communication Networks (report, Q4, 2014)
D8	Guidelines for Secure Inter-Banking Communications and Transactions (report, Q4, 2014)
WPK2.3	**Raising the level of preparedness of EU citizens**
D1	Provide technical guidance and support for European Cyber-Security Month (dissemination material, Q4 2014);
WS3	**Support Cooperation**
WPK3.1	**Crisis cooperation - exercises**
D1	Cyber Europe 2014: Exercise Plan and Exercise (exercise, Q4 2014)
D2	Report on Cyber Crisis Cooperation and Exercise Activities and Findings (report, Q4 2014)
D3	EU-US Cybersecurity Exercise Plan
WPK3.2	**Implementation of EU legislation**
D1	Analysis of Annual 2013 Incident Reports and Recommendations on addressing significant incidents (report, Q2/3 2014)
D2	Guidelines on Incident Reporting Scheme for Article 15 (report, Q4 2014)
D3	Support the implementation of the NIS Directive (workshops, Q2-Q4)
WPK3.3	**Regular cooperation among NIS communities**
D1	9th ENISA CERT workshop to prepare a roadmap for future work of ENISA in the area of CERT training and CERT cooperation with LEA (in cooperation with EC3)(Q4)
D2	Good practice guide and / or (where applicable) training and exercise material for the exchange and processing of actionable information by CERTs (Q4 2014)

D3	Draft report "Stocktaking on channels and formats for exchange of operational information"
D4	Draft report "Scalable and accepted methods for trustbuilding within and among communities"
D5	Good practice material for first responders in cooperation with the EC3 (Q4)

4 Horizontal Operational Activities

This chapter describes the stakeholder operational activities and project support activities.

4.1 Management Board, Executive Board & 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 2014 and informal meetings will be held, one with the PSG, if appropriate. The existing electronic newsletter will be continued throughout 2014, 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 2014.

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.

In order to make the most of its stakeholder community and also to ensure that it server the latter as effectively as possible, ENISA will aim to involve stakeholders in concrete activities wherever possible.

4.2 National Liaison Officer Network

In 2014, the Agency shall continue to strengthen its relations with the National Liaison Officers' (NLO) Network. The NLO-Network is an informal network of all Member States, including Iceland, Liechtenstein and Norway, as well as the Commission and Council. They are key actors for the Agency's daily work and interaction, in terms of outreach, effective liaison in the Member States and dissemination.

The National Contact Officers (NCO) is an extension of the National Liaison Officers (NLO), which means that the NLO-Network is extended with contact points from governmental CERTs and Regulatory Bodies/Agencies.

ENISA envisages ad hoc meetings with National Contact Officers on particular topics of interest and is planning to host a minimum of 1 meeting with representatives of this network in 2014.

As a result of the NLO meeting in February 2013 and in effort to optimise resources

- ENISA will regularly send information to the members of the NLO network containing information on upcoming ENISA project related tenders, vacancy notices, and events organised by ENISA or where the Agency contributes to (for example co-organiser, etc.).
- In particular, we will continue the practice of sending, emails with relevant announcements (time - critical) and information such as upcoming vacancy notices, new launch for tenders, etc.An assessment of the NLO section page under the ENISA home page is being carried out in a an effort to revise this tool of communication between the Agency and the NLOs. In this respect the Agency is assessing possible improvements as well as gaps that can be filled either by the ENISA home page or other tools such as the newsletter, social networks, etc.
- Following the relevant discussions made in the context of the NLO meeting of February 2013 ENISA has actively collaborated with the NLOs in the implementation of its WP activites for 2013 (for example in the area of trust marks). Such collaborations will be extended in 2014 starting with the NLO meeting of Q1 2014.

4.3 EU Relations

The Agency will continue to develop and enhance relations with EU Institutions and Bodies. In particular, ENISA will seek to ensure that other European institutions and bodies are aware of the

work that the Agency is carrying out and are liaising with the Agency in the most effective way. To this end, ENISA will establish an office in Brussels in order to support its stakeholder activities with the EU institutions and industry representation groups that are based in Brussels.

ENISA will undertake the analysis and review of EU policy acts when requested to do so and on its own initiative when this is in the interest of its stakeholders.

Developing and maintaining a network of key actors, advocacy and regular interaction with ENISA's relevant stakeholders in the EU Institutions is highly important in order to raise the Agency's profile as such and, finally, to 'enhance the levels of security in Europe'. ENISA will therefore continue to maintain visibility in debates relating to NIS by participating in high-level events.

Finally, ENISA shall provide advice and assistance, as stated in its founding regulation, to the EU Institutions regarding relevant NIS policy issues.

4.4 Corporate Communication

A major element of ENISA's mission is about communicating its work to the wide range of individuals and groups who play a role in network and information security across Europe. In its widest sense, ENISA's corporate communication activity is about how the Agency creates understanding of and support for the Agency's work among these audiences. In 2014, the focus will be on working at all levels 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.

ENISA's media relations programme continues to create opportunities for the agency to extend its reach to communicate with wider audiences than it could reach independently. A programme of targeted press conferences is also planned for 2014, focusing on media in particular geographical locations, or with a particular interest in specific NIS areas.

The Agency will continue to develop dynamic infographics for its web site, and use in presentations. Along with YouTube, other Social Media, such as Twitter, LinkedIn and Facebook will continue to play a prominent role in how ENISA engages with its audiences. Experience from 2012 (when ENISA launch its Social Media presence) and 2013 has shown that the Agency's typical "followers" are NIS opinion formers and professional, making them a highly valuable and influential audience. Finally, the Agency will again produce a number of "Flash Notes" during the year, highlighting key NIS issues in a fast and effective medium.

4.5 Dissemination activities

ENISA continues to regard dissemination activities as a key part of its efforts to communicate effectively with its stakeholder communities. As part of this effort, ENISA will, throughout 2014 be producing informative, tightly focused video clips, plus podcasts and interviews, all available through the Agency's web site, and other media, such as YouTube. These will be produced in addition to the more classic corporate video productions, on wider themes.

4.6 Quality Control

In 2011, the Executive Director, launched the quality management system of the Agency. In 2014, the Agency plans to continue documenting, implementing and maintaining a quality management system in order to improve its effectiveness.

In 2014 the Agency will re-engineer selected operational processes, align organisational requirements with actual implementation in information management and seek process improvements across the board. Efforts will be made to measure the performance of recently designed processes for the purpose of proposing suitable adjustments. A set of tools such as electronic signatures, electronic workflows and enterprise management tools will be gradually integrated as necessary to further improve productivity.

4.7 Summary of Horizontal Operational Activities

Horizontal Operational Activities				
SR	**Stakeholder Relations**	**Budget**	**Person months**	**FTE**
SR1	MB & PSG Secretariat	220.000	9,6	1,0
SR2	National Liaison Officers Network	40.000	4,8	0,5
SR3	EU Relations	0	4,8	0,5
Total SR		**260.000**	**19,2**	**2,0**

CC	**Corporate Communication**	**Budget**	**Person months**	**FTE**
CC1	Corporate Communication	50.000	19,2	2,0
Total CC		**50.000**	**19,2**	**2,0**

PS	**Project Support Activities**	**Budget**	**Person months**	**FTE**
PS1	Dissemination Activities	40.000	9,6	1,0
PS2	Quality control	0	9,6	1,0
Total PS		**40.000**	**19,2**	**2,0**
Total Horizontal Operational Activities		**350.000**	**57,6**	**6,0**

5 Administration and Support Department, Directorate and General Management activities

5.1 Overview

The Directorate consists of the Executive Director and his personal assistant. The Executive Director is responsible for the overall management of the Agency.

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

The Administration and Support Department takes all the necessary actions in order to ensure that the management of the Agency is in line with EU institutions' established finance regulation, staff regulation n and related implementing rules. ENISA keep monitoring the Agency risk framework and upgrading the exiting control and operating standards.

5.2 Activities

5.2.1 ASA 0 Directorate and General management

The activities of Directorate and General Management consist of determination and implementation of strategy, planning, decision making, and overall management activities.

5.2.2 ASA 1 General Administration

The main activities of General administration include, support Directorate, Agency management, meetings, support to overall agency activity, translations, legal officer activities/services, Internal Control Coordination (ICC) and internal communication to contribute to continuously improve the working environment (include Publications & Brand material).

In 2014, the ICC function will monitor the agency activity in administrative transactions, analyse the control risk framework contributing monitoring and map the key risk areas, control follow-up of the implementation of the audits recommendations (European Court of Auditors - CoA and Internal Audit Service - IAS) and issue exception management reports.. In this respect, MATRIX (project management tool to support the agency management and operational activities) shall be used in operations in order to enforce a common project management and performance monitoring culture across the Agency at the same time the horizontal functions will start a integration management process with other tolls that are used (ABAC, SharePoint, Business Objects, etc.). It will also provide the management with operational orientations as to how various organisational units of the Agency perform their tasks in light of the budgetary and regulatory constraints that can be used for strategic review.

During the period under consideration the ICC will also ensure that procedures defined are actually and effectively implemented and carry out spot checks (ex-post controls) at the request of the Executive Director or on its own initiative subject to authorisation of the latter.

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

- Legal Officer activities/services
- Internal Control Coordination (ICC) - Management of Audits replies
- Strategic support and review of the internal support IT systems (Management of ABB tool MATRIX, etc.)
- Liaison with Staff Committee
- Relations with Hellenic Authorities
- Publications and Brand Material
- Purchase of books, newspapers and periodicals
- Purchase of stationery

- Management of postage and delivery charges
- Management of Internal meetings expenditures
- Management of translation services' requests
- Any other task of general administrative nature

5.2.3 ASA 2 Finance, Accounting and Procurement

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

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 and to provide quality annual accounts, in compliance with the applicable financial rules.

The activities of the Section are listed below:

- Financial Transactions' Initiation
- Operational and Financial Verifications
- Budget Preparation and Management
- Missions Management & Helpdesk, including system maintenance
- Financial Helpdesk and Reporting
- Accounting activities
- Statutory reporting activities
- Procurement procedures' overall management, including procurement planning
- Contracts' management
- Support to Audits (European Court of Auditors and Internal Audit Service)
- Internal Trainings related to FAP activities
- Electronic workflows development
- Central correspondent to DG BUDG for systems, rules and framework contracts
- Drafting Financial Internal Policies
- Coordination meetings

5.2.4 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 Rights and Obligations of Staff
- Recruitment
- Entitlements and leave management
- Medical Services and Health in work environment
- Trainings
- Education expenditures
- Management of Interim services
- Work environment and welfare

5.2.5 ASA 4 Information and Communication Technology

The activities of IT include help desk, operations and monitoring, services management and infrastructure management, solutions and development.

- Service Strategy and Development
- Service Transition
- Service Security
- Service Operations
- Services External
- Service Support
- Operational Systems

5.2.6 ASA 5 Facilities Management (FM)

Facilities Management activities include the following:

- Transport and Delivery Services
- Buildings Management
- Inventory Management
- Meeting Services
- Internal Moving Services
- Physical Security
- Personal Security
- Information Security
- Policies and Procedures
- Contingency Plans
- Incident Handlings

5.3 Summary of Administration Support and General Management Activities

Administration and Support Department Activities				
ASA	**Administration and Support Department Activities**	**Budget**	**Person months**	**FTE**
ASA 0	Directorate and General Management activities	5.000	33,6	3,5
ASA 1	General Administration activities	136.728	36,5	3,8
ASA 2	Finance, Accounting & Procurement activities	0	72,0	7,5
ASA 3	HR Activities (including salaries)	5.947.226	25,9	2,7
ASA 4	IT Activities	517.500	52,8	5,5
ASA 5	Facility Management Activities	395.900	24,0	2,5
Total ASA	**Administration**	**7.002.354**	**244,8**	**25,5**

Total Administration, IT and Facility managements	**7.002.354**	**244,8**	**25,5**

6 APPENDIX A: OPERATIONAL ACTIVITIES 2014 (Activity Based Budgeting)

OPERATIONAL ACTIVITIES 2014	Operational HR in person/years (Note 1)	Salary Costs Operational HR in EUR (Note 2)	Operational Expenditure in EUR (Note 3)	Overheads in EUR (Note 4)	Total Activity Cost in EUR
WS1 - Support EU Policy Building	9,3	708.981	280.000	844.376	1.833.357
WS2 - Support Capacity Building	12,6	958.293	495.000	1.141.300	2.594.593
WS3 - Support Cooperation	14,0	1.071.054	459.000	1.275.594	2.805.648
SR - Stakeholder Relations	2,0	152.559	260.000	181.693	594.252
CC - Corporate Communication	2,0	152.559	50.000	181.693	384.252
PS - Project Support Activities	2,0	152.559	40.000	181.693	374.252
Missions	0,0	0	500.000	0	500.000
Total	41,9	3.196.005	2.084.000	3.806.349	9.086.354

Note 1 - The Operational Human Resources consist of the number of ENISA Staff and Seconded National Experts (SNE) directly involved in the implementation of the relevant activities.

Note 2 - The salary costs of Operational Human Resources consists of the cost of ENISA Staff and SNE directly involved in the implementation of the activities.

Note 3 - The Operational expenditure is the direct cost attributed to each Core Operational and Horizontal Operational activity, provided for in WP2014.

Note 4 - Overheads include all costs which are indirectly involved in the implementation of WP 2014, such as salary costs of non-operational staff, rent, and running costs (e.g. Office supplies).