WORK PROGRAMME 2012

Improving Information Security Through Collaboration

VERSION 4.1 – 19TH JANUARY 2012

Contents

ACRONYMS

ABAC: Accruals Based Accounting (financial management tool)

AD: Administration Department

ADA: Administration Department Activity

CEN/CENELEC: European Committee for Standardization /European Committee for Electro technical Standardization

CERT: Computer Emergency Response Team

CII: Critical Information Infrastructures

CIIP: Critical Information Infrastructure Protection

COCOM: Communications Committee

D: Deliverable

DG: Directorate-General

ED: Executive Director

EGC: European Government CERTs

EFMS: European Forum for Member States

EISAS: European Information Sharing and Alert System

ENISA: European Network and Information Security Agency

EPCIP: European Programme for Critical Infrastructure Protection

EP3R: European Public Private Partnership for Resilience

ERNCIP: EU Reference Network for Critical Infrastructure Protection

ETSI: European Telecommunications Standards Institute

EuroSCSIE: European SCADA and Control Systems Information Exchange

FI: Future Internet

FIA: Future Internet Assembly

FP (7): Framework Programme (7)

HCIN: Heads of Communications and Information Network

HR: Human Resources

ICT: Information and Communication Technologies

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

ISA: Interoperability solutions for European public administrations

ISAC: Information Sharing & Analysis Centre

ISO: International Organization for Standardization

ISP: Internet Service Providers

ITSU: Information Technology Services Unit

ITU: International Telecommunication Union

KPI: Key Performance Indicator

LE: Law Enforcement

LEA: Law Enforcement Agency

MB: Management Board

MISS: Missions

MS: Member States

NCO: National Contact Officer

NCON: National Contact Officers Network

NIS: Network and Information Security

NIST: National Institute of Standards and Technology

NLO: National Liaison Officer

NRA: National Regulatory Authority

PAU: Public Affairs Unit

PPP: Public Private Partnership

PSG: Permanent Stakeholders Group

Q: Quarter

R&D: Research and Development

RSS: Really Simple Syndication

SCADA: Supervisory Control And Data Acquisition

SDO: Standards Development Organisations

SME: Small and Medium Enterprise

SR: Stakeholder Relations

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

TCD: Technical Competence Department

WP: Work programme

WS: Work Stream

1 Executive Summary

1.1 Introduction

In putting together the work programme for 2012, ENISA has continued its efforts to concentrate on issues that are both strongly aligned with the European policy agenda and also considered as core areas of competency for the Agency. For this reason, the development of the 2012 work programme has been carried out in a different way to the process used in previous years. The procedure followed this year was designed to ensure that the input from the Permanent Stakeholder Group (PSG) and from the Management Board (MB) was taken into account as from the beginning of the work programme development process.

As a result of this process, the work programme for 2012 is structured into four streams of work. These work streams cover the evolution of the global threat environment, the need to continue to improve Critical Information Infrastructure Protection (CIIP) across the EU, supporting the CERT and other operational communities and economic and governance aspects of NIS respectively.

1.2 Background

This work plan was developed taking into account a number of developments related to information security both at the European and at the international level. In particular, the composition of the work programme reflects changes in the global threat environment, the key EU policy statements that have a bearing on Network & Information Security (NIS) and the move towards increased dialogue between different operational communities.

The main drivers for ENISA's work in this area are the Commission Communication on Critical Information Infrastructure Protection (CIIP) of March 2009[1], the conclusions of the Council Presidency of the Tallinn ministerial conference on CIIP[2], the Commission Communication on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security" adopted on 31 March 2011[3] and the Council Conclusion on CIIP of May 2011 The work programme for 2012 builds on the work carried out during 2010 and 2011 and concentrates on assisting the Commission and Member States in their activities under the core instruments foreseen by the initial communication– the European Forum for Member States (EFMS), pan-European Exercises and the European Public Private Partnership for Resilience (EP3R).
The Telecom Ministerial Conference on CIIP organised by the Presidency in Balatonfüred, Hungary, on 14-15 April 2011 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

[1] Commission Communication of March 2009, "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM(2009)149.
[2] Ministerial Conference on Critical Information Infrastructure Protection, 27-28 April 2009, Tallinn, Estonia
[3] "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)

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 a process.

As in previous years, ENISA has carefully followed developments in ICT technology and changes in the threat situation for global networks. Whilst the work programme has been kept highly focused on the key policy objectives, the Agency has remained open for dialogue with other communities involved in improving information security on a pan-European or international basis. In particular, ENISA has responded to Commissioner Malmström's call for cooperation between ENISA and the new Cybercrime centre hosted by EUROPOL and has introduced elements into the work plan reflecting this. ENISA recognises that collaboration between previously distinct communities will continue to develop as a consequence of the Treaty of Lisbon[4] and will actively support the Member States in facilitating this dialogue when called upon to do so.

1.3 Structure

1.3.1 Work Streams

The 2012 Work Programme has been structured as four separate work streams, which have been chosen so as to reflect the input from the exercise carried out with the PSG, the Management Board and ENISA respectively.

These work streams are as follows:

- WS1: Identifying & Responding to the Evolving Threat Environment
- WS2: Improving Pan-European CIIP & Resilience
- WS3: Supporting the CERT and other Operational communities
- WS4: Security Economics & Governance

In addition, supporting work will continue in the form of stakeholder engagement activities and project support activities. Press and Communications will also be planned as a separate activity within the Agency, as in previous years.

The table below provides a visual summary of the work streams and the related work packages (WPKs):

[4] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, entered into force on 1 December 2009, 2007/C 306/01.

WS1 - Identifying & Responding to the Evolving Threat Environment	WS2 - Improving Pan-European CIIP & Resilience
WPK 1.1: Emerging Opportunities & Risks *WPK 1.2: Mitigation & Implementation Strategies* *WPK 1.3: Knowledge Base*	*WPK2.1: Further Securing EU's Critical Information Infrastructures and Services* *WPK 2.2: Cyber Exercises* *WPK 2.3: European Public Private Partnership for Resilience (EP3R)* *WPK 2.4: Implementing Article 13 a*
WS3 - Supporting the CERT and other Operational Communities	**WS4 - Securing the Digital Economy**
WPK3.1: Support and enhance CERTs operational capabilities *WPK3.2: Application of good practice* *WPK3.3: Support and enhance (co)operation between CERTs, and with other communities*	*WPK 4.1: Economics of Security* *WPK 4.2: Security governance* *WPK 4.3: Supporting the development of secure, interoperable services*

PS - Project Support Activities
Awareness Raising Activities, Targeted dissemination, Flash Notes Service

SR - Stakeholder Relations
Management Board & Permanent Stakeholder Group Secretariat, *National Contact Officers (NCO) Networks,* *EU Relations,* *Managing Stakeholder Relations*

PAU - Policy & Public Affairs Activities
Aligning to the Policy Environment, Public Relations, ENISA Digital Communication, ENISA Publications and Brand Materials, Spokesman and Media Relations, ENISA Events, ENISA Internal Communication

A short description of these work streams and supporting activities is presented in the following paragraphs, whilst a more complete description of each work stream is presented in the following sections of the document.

1.3.2 WS1 – Identifying & Responding to the Evolving Threat Environment

Information Security is about managing risks and threats linked to the security of information and information systems)

ENISA's objective in this work stream is to provide stakeholders with information on how risks and threats are evolving. More specifically, the aim is to link particular trends to particular stakeholder communities, thereby helping such communities to recognise and respond to changes in the threat landscape that are particularly relevant to their activities. In addition, we will propose suitable mitigation strategies and identify recommendations

and implementation options for dealing with the identified risks. The emphasis will be on the provision of non-technical information regarding all the components of risks. The principle output of this work stream is a periodic report summarising and prioritising risks by stakeholder community.

1.3.3 WS2 – Improving Pan-European CIIP & Resilience

This work stream seeks to improve the level of resilience and level of protection of Critical Information Infrastructure throughout Europe with the goal of improving the level of preparedness of Member States to cope with large scale incidents affecting their ICT infrastructure.

1.3.4 WS3 – Supporting the CERT and other Operational Communities

The objective of this work stream is to continue to assist Member States in improving their operational response capabilities in the face of an incident. Here, the approach is to build on previous work that ENISA has carried out with the CERT community and related communities and to ensure that the flow of information and the coordination between such communities is optimal. This objective also includes assisting Member States in developing key concepts, such as Early Warning Systems, and ensuring that such systems are capable of operating across national boundaries, thereby improving the pan-European response capability

1.3.5 WS4 – Securing the Digital Economy

The fourth work stream provides a stronger focus on contributing to the development of NIS policy and strategy at the EU level in order to support the objectives of the Digital Agenda and to ensure that the Digital Economy of the future is correctly secured. ENISA will support the Commission and the Member States in this area by looking at three different aspects of the Digital Economy; Economic drivers and barriers for security, governance aspects and priorities for research and development.

In this context, socio-economic aspects of security, as well as privacy and trust related issues will be taken into account. Moreover, existing EU initiatives related to Future Internet (FI) technologies and systems will also be considered as an important input to the work.

1.3.6 Stakeholder Relations Activities

As in 2011, the Executive Director and the Head of the Technical Competence Department (TCD) will continue to take an active role in the development of stakeholder relations. Where discussions with stakeholders are closely related to the work programme, TCD staff will support this activity.

The main stakeholder-related activities foreseen in this work programme are as follows:

- Secretariat activities for the Management Board and the Permanent Stakeholder Group
- National Contact Officer & National Liaison Officer Networks

- EU Relations
- Managing Stakeholder Relations

In carrying out its stakeholder activities, ENISA will ensure that it does not duplicate existing points of contact, either within the Agency itself or with other European bodies.

These activities are described in section 4 of this document.

1.3.7 Project Support Activities

Project support activities are those activities that are best carried out independently of the individual work streams. Such activities are common to the different areas of the work plan and it is more effective to implement them within the work streams but to manage the coherence of the overall approach in terms of project support. In 2012, ENISA plans to use this approach in the following areas:

- Awareness rising.
- Targeted dissemination.
- Flash Notes.
- Work on standardisation.

Where research and innovation is concerned, ENISA will seek to identify gaps between research and innovation, and to identify priorities and open questions for future research as well as the significance of research efforts to address current problems of NIS that cannot be addressed by policy actions alone.

It is important to note that these activities are mainly resourced by the individual work packages and the effort reported under the project support activity itself is limited to that needed to perform the necessary coordination activities.

1.3.8 Public Affairs

In 2012, the Agency will continue strengthening its focus on EU Policy development by analysing and reviewing EU policy documents, , and legal acts, by supporting with its input and expertise as and when required and by participating in high-level events. Moreover, the Agency shall continue to promote its work both towards the general public and towards its stakeholder communities.

By increasing visibility with key actors at political and strategic level and by involving political and industrial decision makers and by reaching out to NIS communities, the Agency shall further promote its work.

1.3.9 Administration and IT support activities

A short summary of the administration and IT support activities that support the operation of the Agency is provided in the final sections of this work programme.

Remark

This work programme (WP2012) defines the tasks of ENISA in 2012. It has no correlation to the Agency's internal organisational structure.

2 Introduction

2.1 Relation to the previous work programme

The work programme for 2012 represents a substantial departure from the 2011 work programme.

There is no direct relation between the proposed Work Stream 1 and previous versions of the work programme, although the activities of the work stream are somewhat similar to the activities of the work carried out by the Agency between 2008 and 2010 entitled 'Emerging and Future Risks (EFR)'. The essential difference between the work carried out in the area of EFR and the work envisaged in 2012 is in the scope and in the method used. In the 2012 work programme, the objective is to identify threats from a global perspective, rather than performing risk analyses with a specific scope. Where method is concerned, the identification of risks will be based primarily on work carried out by other organisations – ENISA will seek to identify, collate and analyse such studies in order to provide an overview and to draw conclusions based on a combination of studies.

Work Streams 2 and 3 are a direct continuation of work initially carried out in the areas of resilience & CIIP and CERT-related activities in the 2010 and 2011 Work Programmes. The activities in these work streams are closely aligned with the CIIP Action Plan defined in the Commission's communication of March 2009[5] and the Commission Communication on Critical Information Infrastructure Protection of 31 March 2011[6]. These areas are considered as a key competence areas of ENISA.

Work Stream 4 contains elements that can be considered as a continuation of work begun in 2011 (e.g. Economics of Security) and work that was started in 2010 (e.g. activities in support of the ePrivacy Directive,). There are also new activities defined as part of this work stream.

2.2 Policy 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 policy context.

The ENISA-Regulation[7]
All activities and tasks fulfilled by the Agency are fulfilled on the basis of the founding ENISA-Regulation.

The Council Resolution of December 2009[8]

[5] Commission Communication of March 2009, "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM(2009)149.
[6] "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)
[7] March 2004 establishing the European Network and Information Security Agency.

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.

The Council conclusion on CIIP of May 2011[9]

The 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.

The Commission proposal on the future of ENISA[10]

This document spells out a proposal from the European Commission for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA). The proposal complements regulatory and non-regulatory policy initiatives on Network and Information Security taken at Union level to enhance the security and resilience of ICTs. The proposal mentions several of the on-going developments in NIS policy (notably those announced in the Digital Agenda for Europe) that would benefit from the support and expertise of ENISA.

The Electronic Communications Regulatory Framework[11]

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.

The CIIP Action Plan[12]

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[13]

---

[8] Council resolution of 18 December, 2009 'On a collaborative approach to network and information security (2009/C 321 01)

[9] Council Conclusion on CIIP of May 2011 (http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf)

[10] The European Commission *Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)* (14358/10)

[11] Telecommunications Regulatory Package (article 13a. amended Directive 2002/21/EC Framework Directive)

[12] Commission Communication of March 2009, "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM(2009)149.

[13] "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)

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.

The Communication on Personal Data Protection in the European Union[14]

The European Commission recognizes that the rapid technological developments and globalisation have profoundly changed the world around us, and brought new challenges for the protection of personal data. The communication published in November 2010 establishes key objectives for a comprehensive approach for data protection.

The Single Market Act[15]

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 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).

The Digital Agenda[16]

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.

The Internal Security Strategy for the European Union[17]

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.

The 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

[14] *A comprehensive approach on personal data protection in the European Union*, Communication COM(2010) 609,

[15] Single Market Act – Twelve levers to boost growth and strengthen confidence "Working Together To Create New Growth", COM(2011)206 Final

[16] *A Digital Agenda for Europe*, COM(2010)245, May, 2010.

[17] An internal security strategy for the European Union (6870/10), http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/113055.pdf

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.

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

2.3 Mobile Assistance Teams (MATs)

The mission of ENISA is to work together with the EU-institutions and the Member States to develop a culture of Network and Information Security for the benefit of citizens, consumers, business and public sector organisations in the European Union. As part of this mission, one of the central tasks of ENISA is to ensure that good practices identified by Member States in implementing information security are made available to the rest of the community through timely exchange of information and good practice. This approach brings many benefits to the EU community.

In a letter to Dr Zsolt Nyitrai, Minister of State for Infocommunication of Hungary[18], which held the EU presidency at the time, Commission Vice President Neelie Kroes stated that 'ENISA should be able to mobilise its full team of security experts to assist Member States, upon request, to provide technical assistance whenever and wherever necessary, even at short notice. It should also act as an agile broker for peer learning between those Member States that seek improvement of their capacity and those with more advanced capacity that are able and willing to help'[19].

In implementing the 2012 work programme, ENISA strongly aligns itself with the vision of Vice President Commissioner Kroes that it would serve Member States better by taking a more active role in assisting and advising national bodies. As such, the Agency aims to improve the effectiveness of its activities by developing the capability to mobilise teams of security experts in order to assist Member States, by providing technical assistance wherever and whenever it is required.

In particular, based on our experience to date, we think that we could assist Member States more effectively by taking a more proactive attitude towards:

- Identifying where the 'offer' and 'demand' for different types of information and best practice are situated throughout the EU.
- Brokering relationships between those Member States with a particular requirement and those willing to share their experience.

[18] Letter dated 24 May, 2011; the letter was discussed at the EU Telecommunications Council on 27 May, 2011
[19] For more detail, see the letter sent by the Executive Director of ENISA to the Management Board members on 29 June, 2011.

- Assisting Member States throughout the period during which the issue under consideration is being resolved.

Selective use of Mobile Assistance Teams will enable ENISA to respond to Member States' needs in an agile manner and to increase the scalability of its activities by leveraging existing experience in the EU community.

3 Work Streams

3.1 WS1- Identifying & Responding to the Evolving Threat Environment

3.1.1 Justification

An essential component of any approach to information security is the assessment of trends and changes, which requires a forward-looking approach. In particular, the assessment of emerging threats is a necessary part of preparing for future challenges. In this work package the objective is to derive "IT-Security readiness statements" for various areas and government initiatives, in particular with regard to Member States and the Commission (e.g. by identifying emerging opportunities and risks of policy initiatives).

This will be achieved by assessing emerging opportunities and risks for areas and initiatives pertinent to various stakeholder communities. Analysing both opportunities and risks, will enable the Agency to draw conclusions that reflect the trade-offs that institutions and businesses will need to make. This approach should help policy makers and business communities to take full advantage of innovative technologies and business models, whilst still maintaining a high degree of security. The work to be conducted will make maximum use of existing cooperation agreements and support relevant stakeholders as appropriate.

3.1.2 Specific Policy Context

Specific policy references for this work stream are as follows:

- ENISA Regulation
- Directive 2009/140/EC, Art. 13a
- The Council Resolution of 18 December 2009
- Internal Security Strategy for the European Union

3.1.3 Overall Objectives

The main priority will be to provide stakeholders – in particular Member States and the Commission - with community specific views on opportunities and risks. In addition, where risks are identified, we will recommend suitable mitigation strategies and provide guidelines on how such strategies can be implemented in operational environments. The outcome of this process approach will be:

- Appropriate processes to identify relevant areas and policy initiatives
- Periodic reports on prioritised risks per stakeholder community (i.e. sector)
- Associated proposals for mitigation strategies and for materialization of opportunities

3.1.4 A knowledge base for storing and managing relevant data over time (initially as an internal tool with horizontal relevance) Work Packages

The following work packages constitute the Work Stream:

- WPK 1.1: Emerging Opportunities & Risks.
- WPK 1.2: Mitigation & Implementation Strategies.
- WPK 1.3: Knowledge Base

3.1.5 WPK 1.1: Emerging Opportunities & Risks

WS Name	
WS1: Identifying & Responding to the Evolving Threat Environment	
WORK PACKAGE NAME:	
WPK 1.1: Emerging Opportunities & Risks	
DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):	
SMART Goal: Produced deliverables are being referenced by others.	#of references to the deliverable by the stakeholder community within 6 months after publication (end of Q4).

DESCRIPTION OF TASKS:

The following activities are envisaged in order to elaborate on opportunities and risks for various areas identified:

- Identification, analysis and summary of opportunities and risks for an agreed set of stakeholder communities. A variety of aspects will be part of the analysis of risks; such as business (i.e. opportunities), social, legal and trust aspects.

- Identification of areas and policy initiatives to be considered by involving corresponding stakeholders in the assessment activities (especially government initiatives of Member States and policy initiatives of the Commission). This will contribute to the development of an "IT-Security Readiness Statement" for these areas and initiatives.

- Collection and aggregation of existing quantitative data will be a long-term objective that will be developed initially within this action and refined in future versions of the work programme. At the same time, interfaces with activities of other work streams such as Incident Reporting Schemes, Information Sharing, EISAS, etc. will be exploited. Existing information from COM (e.g. Eurostat) and Member States (i.e. yearly report on breaches according to Art 13a Telecom Package, Directive 2009/140/EC) will form part of the data to be analysed. The data collected in this activity will be input for the Knowledge base developed in WPK1.3 (see below).

- Production of assessments of emerging threats, opportunities and risks per identified area/initiative with the support of the participating stakeholder(s) either in new areas or building on past ENISA work (Q4) (e.g. Cloud Computing, Internet of Things and Future Internet, mobility issues, e-health, child online protection, supply chain security, browser security, etc.).

- Specifically in the area of cloud computing, ENISA will undertake a study revisiting the 2009 study Cloud Computing: Risks, Benefits and Recommendations for Information Security. Possible new issues to include are:
  - The implications of the conclusions review of the 95/46 data protection review

for cloud computing security
- The implications of extra-European legislation (such as the US Patriot Act) which may be enforced within Europe.
- A detailed study of security considerations for a pan-European community cloud PPP.
- The implications of a major failure scenario of a large cloud provider for European business and services.

In carrying out this work, ENISA will seek to identify, collate and analyse such studies in order to provide an overview and to draw balanced conclusions based on a combination of studies. Particular attention will be paid to the need to avoid duplication of effort, either by replicating what is already done in the Member States or the Commission or by competing with similar private sector initiatives. The approach will elaborate on policy opportunities and focus on emerging issues

OUTCOMES AND DEADLINES:

- D1 (Priority HIGH): Security threat landscape in Europe based on aggregated data collected from stakeholders (report) (Q3 - 2012).
- D2 (Priority HIGH): Identification and analysis of specific areas of interest/policy initiatives. (report) (Q4 - 2012).
- D3 (Priority HIGH): Opportunities and risks per identified area/policy initiative (report), together with associated structured data (periodically performed - once per quarter Q3-Q4).

STAKEHOLDER IMPACT

Various stakeholders (in particular Member States and Commission):	D1: The aggregated data will be made available to stakeholders. D3: The periodical report on emerging opportunities and risks is expected to be used by many stakeholders to improve their prioritisation of issues and adapt their planning accordingly.
Stakeholder participating in the assessment (pro area/ policy initiative)	D2: Stakeholders from the relevant areas/policy initiatives will use the performed analysis.

RESOURCES FOR 2012 (person months and budget)

- 80K Euros
- 18,2 Person Months

LEGAL BASE & POLICY CONTEXT

- ENISA Regulation
- Directive 2009/140/EC, Art. 13a
- The Council Resolution of 18 December 2009
- Internal Security Strategy for the European Union

3.1.6 WPK 1.2: Mitigation & Implementation Strategies

WS Name	
WS1: Identifying & Responding to the Evolving Threat Environment	
WORK PACKAGE NAME:	
WPK 1.2: Mitigation & Implementation Strategies	
DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):	
SMART Goal: By the end of Q4, the deliverables will be endorsed by at least 5 Member States and the Commission.	#of Member States endorsing the deliverable.
SMART Goal: By the end of Q4, the deliverables will be endorsed by at least 5 relevant stakeholders.	#of participants endorsing the deliverable (in particular Member States and Commission).
SMART Goal: Produced deliverables are being referenced by others.	#of references to the deliverable by the stakeholder community within 6 months after publication (end of Q4).

DESCRIPTION OF TASKS:

The objectives of this work package are (a) to recommend suitable mitigation strategies for each of the risks identified in deliverable D3 of WPK 1.1, and (b) to provide guidance on how such strategies can be implemented in relevant environments (mainly Member States government initiatives and Commission).

Although building on the results of WPK 1.1, additional risks will be considered (e.g. those risks identified in other Work Streams, e.g. Art. 13a). Similarly, for the same emerging threat/risk various mitigation and implementation strategies might be generated for different stakeholder communities. The same holds true for identified opportunities, where various materialization options might be relevant, depending on organisational conditions and areas/policy initiatives. Proposed measures will be developed by taking into account stakeholders' viewpoints.

As part of this work, opportunities for improving security will also be identified and measures will be proposed to develop/materialize these at low cost.

Recommendation will be developed that are not too technical and are generic enough to be applied in more than one area (i.e. to be reusable).

OUTCOMES AND DEADLINES:

- D1 (Priority HIGH): Periodic report on recommendations for mitigating the risks considered and materialisation of opportunities (periodically performed, i.e. Q2-Q4 in coordination with deliverable D3 of WPK 1.1). It is expected, that this deliverable will be consolidated with the corresponding periodic report of WPK 1.1. and will contain reference to both emerging risks and mitigation strategies.
- D2 (Priority MEDIUM): Implementation guidance per area/policy initiative (Q4).

STAKEHOLDER IMPACT	
Sector specific stakeholder	D1: The periodical report on emerging opportunities and risks will be used by many stakeholders to adapt current strategies for mitigating risk. D2: Implementation guidelines will be used to inform stakeholders of practical considerations relating to the mitigation approaches outlined.
RESOURCES FOR 2012 (person months and budget)	
• 100K Euros • 15,6 Person Months	
LEGAL BASE & POLICY CONTEXT	
• ENISA Regulation • Directive 2009/140/EC, Art. 13b • The Council Resolution of 18 December 2009 • Internal Security Strategy for the European Union	

3.1.7 WPK 1.3: Knowledge Base

WS Name	
WS1: Identifying & Responding to the Evolving Threat Environment	
WORK PACKAGE NAME:	
WPK 1.3: Knowledge Base	
DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):	
SMART Goal: By the end of Q4, the information maintained in the Knowledge Base will be used within the Work Stream and other ENISA activities.	KPI: Number of entries of ENISA activities in the Knowledge Base.
DESCRIPTION OF TASKS:	
The objective of this work package is to establish and maintain a knowledge base for querying security threat and risk data over time. The Knowledge Base is the main knowledge management tool that will support the work conducted within this Work Stream. The Knowledge Base will also be used to store related information that will be generated/collected within this work stream. Hence, the Knowledge Base is primarily an internal tool that will also hold information generated by other Work Streams, fulfilling thus a role as horizontal knowledge repository. This will be: • A collection of security data, that is, structured qualitative and quantitative security information with corresponding references to other (external) information sources. This data will cover security threats, vulnerabilities, risks, opportunities and trends, mitigation measures, implementation strategies and materialisation measures for identified opportunities. • Particular attention will be given to the ability to derive multiple views (e.g. by sector/technology/other criteria) to be used for other activities within ENISA.	

As part of this work package, procedures to maintain, access and query the Knowledge Base will be developed. These functions will ensure that the stored information is usable within other ENISA activities (i.e. in order to serve as an internal horizontal tool). In addition, the Knowledge Base will provide access functions that will allow for the generation of context dependent, views on the stored information. Within this work, the value of the Knowledge Base on top of available databases will be identified. In the middle term (beyond 2012), the potential of the Knowledge Base to serve as information source on the IT-Security Readiness "big picture" will be identified. Possible use cases will be developed, together with the relevant stakeholders participating in WPK 1.1 and 1.2. For this purpose, the requirements of such stakeholders will be collected in 2012.
OUTCOMES AND DEADLINES:
• D1 (Priority LOW): Knowledge Base and associated procedures(Q4 - 2012) • D2 (Priority LOW): Stakeholder Requirements (Q4 - 2012)

STAKEHOLDER IMPACT	
Various relevant Stakeholders (primarily Member States and Commission)	D2: The requirements for potentially using the Knowledge Base will be collected.
ENISA	D1, D2: The Knowledge Base and associated procedure will help reusing ENISA work and manage relevant documents.

RESOURCES FOR 2012 (person months and budget)
• 70K Euros • 6,0 Person Months
LEGAL BASE & POLICY CONTEXT
• ENISA Regulation • Directive 2009/140/EC, Art. 13b • The Council Resolution of 18 December 2009 • Internal Security Strategy for the European Union

3.2 WS2– Improving Pan-European CIIP & Resilience

3.2.1 Justification

The work packages described in this section are closely aligned with the CIIP Action Plan described in the Commission's communication of March 2009 and of March 2011. Much of this work also directly supports objectives laid down in the Internal Security Strategy document as well as the Digital Agenda.

Work packages in the area of CIIP are, for the most part, a natural continuation of work carried out as part of the work programmes of 2010 and 2011.

3.2.2 Specific Policy Context

The policy context for this work stream is as follows:

- Digital Agenda
- COM Communication on CIIP of March 2009
- European Programme for Critical Infrastructure Protection (EPCIP)
- COM(2004) 702 Critical Infrastructure Protection in the fight against terrorism
- COM(2006) 786 on a European Programme for Critical Infrastructure Protection
- COM(2005) 576 Green Paper on a European Programme for Critical Infrastructure Protection
- 2008/114/EC Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
- COM (2009) 149 on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"
- The Commission Communication on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security" adopted on 31 March 2011[20]
- The Telecom Ministerial Conference on CIIP organised by the Presidency in Balatonfüred and its follow-up[21]
- COM(2009)278 Final on the Internet of Things – An Action Plan for Europe
- COM (2006) 251 A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"

3.2.3 Overall Objectives

The objective is to assist Member States in implementing secure and resilient ICT systems and to increase the level of protection of critical information infrastructures and services in Europe. More specifically, the objectives of this work stream are:

- To enhance the operational capabilities of Member States by helping relevant stakeholders to increase their level of efficiency and effectiveness
- To support and promote exercises on a pan-European level
- To identify and address the information security challenges in critical information infrastructures
- To support and promote the European Public Private Partnership for Resilience (EP3R)
- To identify and address information security issues in Industrial Control Systems and Interconnected Networks

[20] "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)

[21] http://www.eu2011.hu/files/bveu/documents/HU_CIIP_Conference_Presidency_Statement_final.pdf

- To support to the EU-U.S. Working Group on Cyber-security and Cyber-crime established in the context of the EU-U.S. summit of 20 November 2010.[22]

3.2.4 Work Packages

The following work packages constitute the Work Stream:

- WPK 2.1: Further Securing EU's Critical Information Infrastructure and Services
- WPK 2.2: Cyber Exercises
- WPK 2.3: European Public Private Partnership for Resilience (EP3R)
- WPK 2.4: Implementing Article 13a

[22] See: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/597&type=HTML

3.2.5 WPK2.1: Further Securing EU's Critical Information Infrastructure and Services

WS Name	
WS2: Improving Pan-European CIIP & Resilience	
WORK PACKAGE NAME:	
WPK 2.1: Further Securing EU's Critical Information Infrastructure and Services	
DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):	
SMART Goal: By end of Q4 2012, at least 10 operators and 5 Member States take part in the study on Smart Grids	**KPI**: # operators # Member States
SMART Goal: By end of Q4 2012, at least 5 major cloud computing operators and 5 Member States take part in the study on cloud computing	**KPI**: # operators # Member States
SMART Goal: By end of Q4 2012, at least 10 operators and 5 Member States take part in the traffic redirection study	**KPI**: # operators # Member States
SMART Goal: By end of Q4 2014, at least 5 Member States and 5 Operators deploy ENISA's guide on Rerouting and Emergency Communications during Crisis	**KPI**: # operators # Member States
DESCRIPTION OF TASKS:	

The objectives of this work package are to:

- Analyse cyber security aspects of Smart Grids and SCADA
- Analyse the role and impact of cloud computing for CIIP, and
- Analyse traffic redirection and emergency data communications.

Smart Grids and SCADA

The dependency of Smart Grids on ICTs is highlighted in numerous studies, including the ones performed by ENISA in 2010 and 2011. Building on these results ENISA aims to identify and address the information security challenges of Smart Grids.

In co-operation with existing pan European and international initiatives (e.g. EuroSCSIE, Smart Grid Information Security Group, Commission's thematic group of experts, ERNCIP, EU US Working Group, FP7 projects, EPCIP studies, NIST work) ENISA will identify existing, national and/or pan European, pilots and test beds in the area of Smart Grids. The Agency will then analyse risk assessments, reference architectures, standards, certification processes, and cyber security measures taken to enhance the security and resilience of these installations or initiatives.

Based on the knowledge and expertise acquired, ENISA will contribute to existing standardisation efforts (e.g. CEN/CENELC), EP3R and the EU US working group. The Agency will assist Member States in properly developing and/or deploying Smart Grids test beds (e.g. by offering training) and will develop guidelines on incident reporting mechanisms for incidents related to Smart Grids. Finally, ENISA will assist relevant stakeholders in implementing these mechanisms.

ENISA will assess the cyber security challenges and threats associated with

distributed infrastructures and intelligent components and their deployment in critical sectors. The result will be specific R&D recommendations to be used for shaping new FP8 action lines mostly in the area of 'Internet of Things'.

The main outcome of the study will be strategic, high level requirements and good practices guides for relevant stakeholders. The findings of the study will be validated by a dedicated working group established for this purpose (e.g. EP3R, EuroSCSIE and ERNCIP). The members of the groups will be leading experts from Member States' competent authorities and industry (e.g. operators, manufacturers and academia).

Building on the work of 2011 ENISA will continue its co-operation with existing initiatives on Industrial Control Systems' security (EuroSCSIE), standardisation efforts, private sector (primarily operators, ICS manufacturers, security tools providers), regulators, and national PPPs to implement ENISA's recommendations and good practices. Through this participation ENISA will develop better insights on the needs of stakeholders, engage experts from these groups, and collect and analyse information.

Cloud Computing in the context of CIIP

It has been noted that "Cloud computing may indeed become one of the backbones of our digital future"[23]. Given the importance of Cloud Computing as a business model, ENISA aims at improving the resilience of critical cloud services in the face of large-scale cloud incidents.

The objective of this study, which will take account of the work to be carried out in WPK 1.1, is to support Commission and Member States in defining European and national strategies for cloud computing by providing:

- An analysis of interdependencies of cloud computing with existing infrastructures supporting critical services
- An impact assessment of possible cascading failures
- A cost-benefit evaluation of the opportunity to introduce an incident reporting scheme for cloud computing providers, similar to the one already adopted in the telecommunication sector (e.g. articles 4 of the ePrivacy Directive and 13a of the Telecom Framework Directive).

The main outcome of the study(ies) will be recommendations for policy makers and good practice guides for relevant stakeholders on how to address key challenges, risks and vulnerabilities

Traffic Redirection and Emergency Data Communications

Rerouting data communication traffic and prioritising among different options during a crisis is necessary to ensure the highest possible level of resilience. This is usually

[23] Quoting Commissioner Kroes

done in an ad-hoc manner using policies and practices developed through tacit knowledge and experience.

ENISA will investigate this area with the aim of developing a good practice guide on rerouting data communication traffic and emergency communication. This will be done by identifying and analysing existing initiatives at corporate, national, or international level. The Agency will mostly focus on how operators decide to reroute traffic and the impact of their decisions during a crisis. The study will also analyse the role and responsibility of Member States and the private sector in ensuring emergency data communication during a crisis. In this context, ENISA will assess whether Member States and the private sector could work towards developing national or regional plans that achieve this goal.

The study will engage leading experts from both public and private sector in the field. It will also consult with academia and identify emerging R&D topics for further investigation. The study will also issue recommendations for policy and decision makers. The expected output of the activity is a report on Mechanisms and Policies for Treating Traffic During a Cyber Crisis.

ENISA will continue analysing the interdependencies of ICTs to certain critical sectors (e.g. finance, maritime). Building on the work done by Member States, Commission studies (e.g. EPCIP) and the private sector, ENISA will engage experts in a dialogue to assess whether cyber security measures are properly deployed. This will enable ENISA to identify critical services/sectors that more work is needed in the future.

OUTCOMES AND DEADLINES:

- D1 (Priority HIGH): Cyber Security Risks and Challenges of Smart Grids (Report) (Q4 - 2012)
- D2 (Priority HIGH): Cloud computing and Critical Services (Report) -(Q4 - 2012)
- D3 (Priority MEDIUM): Good Practice Guide on Rerouting and Emergency Communications during Crisis (Report) (Q4 - 2012)

STAKEHOLDER IMPACT

Member States' Competent Authorities, NRAs, European Commission	support MS competent authorities and EU institutions in their efforts to develop a consistent strategy on smart grids and cloud computing (D1, D2)
Telecommunication network providers, Internet Exchange Point providers, Tier 1 providers	understand the problems of traffic redirection, contribute to the identification of good practices and deploy the state of the policies (D3)
Communication Network and Service providers Cloud Computing providers NRA for Telecommunications	analyse the criticality of cloud computing for critical services; work with stakeholders to address open issues and reduce the level of risk (D2)
ICS manufacturers and operators	understand the risks of ICS, identify good

	practices, contribute to standards and deploy state of the art policies (D1)
ICS security tools providers	Identify and propose good practices for ICS and cloud computing providers (D1, D2)
ICS operators from energy Smart Grid Providers	developing and adopting the appropriate cyber security policies and practices of Smart Grids
RESOURCES FOR 2012 (person months and budget)	
• 180K Euro • 21.2 Person Months	
LEGAL BASE & POLICY CONTEXT	
• ENISA Regulation • The Council Directive 2008/114/EC of 8 December 2008 • The CIIP Action Plan[4] • The Council Resolution of 18 December 2009 • Internal Security Strategy for the European Union	

3.2.6 WPK 2.2.: Cyber Exercises

WS Name	
WS2: Improving Pan-European CIIP & Resilience	
WORK PACKAGE NAME:	
WPK 2.2: Cyber Exercises	
DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):	
SMART Goal: By end of Q4 2012, at least 15 Member States and 10 private companies take part in the execution of Cyber Europe 2012	**KPI**: # Member States # private companies
SMART Goal: By end of Q4 2012, at least 10 Member States take advantage of ENISA's services for national exercises	**KPI**: # Member States
SMART Goal: By end of Q4 2014, at least 10 Member States adopt the pan European procedures for information sharing and co-ordination among MS during cyber crisis	**KPI: #** Member States
DESCRIPTION OF TASKS:	
Building on the experience on exercises and especially of Cyber Europe 2010, this work package comprises the following activities • Planning and executing the second pan European exercise, CYBER EUROPE 2012 • Promoting national and international cyber security exercises • Promoting good practice guides on National Contingency Plans, developing a roadmap for future exercises and EU wide procedures for co-ordination of activities among Member States during crisis management.	

Planning and Executing CYBER EUROPE 2012

This activity is related to the organisation of the second pan European exercise on large-scale network security incidents. More specifically it includes the following tasks:

- Planning of CYBER EUROPE 2012
- Defining the measures and scenarios to be tested
- Engaging the relevant public and, if appropriate, private stakeholders
- Defining the necessary policies (e.g. media, observers)
- Defining the monitoring and evaluation process
- Executing and evaluating the pan European exercise within 2012
- Investigating the possibility of having a synchronised exercise with US and/or stakeholders

The output of this activity will be the exercise itself. It will be accompanied by the report of the exercise that would include findings and recommendations of the stakeholders that took part in the exercise. In particular, the exercise will be used to clarify decision making processes and support contingency planning.

Promoting National and International Exercises

This activity of the work package is related to CIIP exercises at large. More specifically it includes the following tasks:

- Promoting national exercise to Member States through dedicated seminars, workshops or events
- Assisting Member States in developing national/regional exercises (e.g. providing strategic and technical advice at the planning and execution phases)
- Co-operating with other regional and/or international exercises, possibly and participating as observers (e.g. with EU in the context of EU US working group)
- Taking stock of and analysing non EU national and regional CIIP exercises and organising an international workshop with relevant players about good practices on CIIP exercises
- Contributing to EU US working group efforts on building a co-operation program for cyber exercises between EU Member States and the US.

The output of this activity will be a status report on national and international preparedness exercises on CIIP.

Promoting good practice guides on National Contingency Plans, Developing a roadmap for future exercises and EU wide procedures for co-ordination of activities among Member States during crisis management activities.

In this activity ENISA will:

- Promote the existing good practice guide on national contingency plans to Member States through dedicated seminars, workshops or events
- Assist Member States in developing national contingency plans (e.g. providing strategic and technical advice at the planning and execution phases)
- Contribute to and support the work of Member States on the development of pan European procedures for information sharing and co-ordination of activities among Member States during cyber crises by building on existing mechanisms (e.g. good practice guides on national contingency plans, Euro cyber Standard Operating Procedures (SOPs), IWWN procedures, the CERT community procedures)
- Develop a roadmap for future CIIP exercises beyond 2012 taking under consideration input from EP3R, the EU US working group, and experts from MS and private sector

OUTCOMES AND DEADLINES:

- D1 (Priority HIGH): Report of CYBER EUROPE 2012 (report) (Q4 2012)
- D2 (Priority HIGH) Status Report on National and International CIIP Exercises (report) (Q3 2012)
- D3 (Priority HIGH): Roadmap on Exercising for CIIP beyond 2012 (report) (Q32012)

STAKEHOLDER IMPACT

EU and MS Public Agencies related to CIIP	provide input on current level of preparedness for large-scale events and cooperation capacities (D1); give an overview of "what others are doing" (D2) provide insights and recommendations for future actions in policy as well as deployment and maintenance of preparedness measures for CIIP (D2 and D3).
Internet and Network Operators	provide input on current level of internal preparedness for large-scale events and inter-operator cooperation as well as public-private sector coordination (D2); give an overview of "what others are doing", as it is foreseen to also include intra-sectorial exercises wherever possible (D1) provide insights on which requirements future actions may bring in the area of preparedness measures for CIIP (D1 and D3); provide the opportunity to address Network Operators ideas on "what and how" needs to be exercised when it comes to responding to large scale incidents affecting their infrastructure resilience. (Deliverable 3)

RESOURCES FOR 2012 (person months and budget)

- 120K Euros
- 24.5 Person Months

LEGAL BASE & POLICY CONTEXT

- ENISA Regulation

- The CIIP Action Plan
- The Council Directive 2008/114/EC of 8 December 2008The Council Resolution of 18 December 2009
- Internal Security Strategy for the European Union

3.2.7 WPK 2.3: European Public Private Partnership for Resilience (EP3R)

WS Name	
WS2: Improving Pan-European CIIP & Resilience	
WORK PACKAGE NAME:	
WPK 2.3: European Public Private Partnership for Resilience (EP3R)	
DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):	
SMART Goal: By end of Q4 2012, at least 3 position papers are produced from corresponding WGs	**KPI**: # position papers
SMART Goal: By end of Q4 2012, at least 3 EP3R workshop are organised	**KPI**: # workshops
SMART Goal: By end of Q4 2012, at least 8 national PPPs, 5 pan European associations and 15 key private companies are actively involved in EP3R	**KPI**: # of national PPPs # of pan Eur. associations # of key private companies
SMART Goal: By end of Q4 2012, at least 10 MS and 20 key private stakeholders participate in the study on cyber security strategies	**KPI**: # Member States # of key private companies
SMART Goal: By end of Q4 2012, at least 4 new MS organise a seminar on national PPP	**KPI**: # Member States
SMART Goal: By end of Q4 2014, at least 3 new MS establish a national PPP	**KPI**: # Member States
DESCRIPTION OF TASKS:	
The objective of this work package is to: • Engage national PPPs in the establishment and evolution of EP3R. • Promote the results of EP3R to relevant stakeholders. • Manage EP3R working Groups and support the activities of the Steering Committee. • Exploit synergies with the ENISA work programme. *Engage national PPPs in the establishment and evolution of EP3R* ENISA will establish trusted information sharing relationships with national PPPs and share knowledge and information on the establishment and evolution of EP3R. ENISA will consult with national PPPs on 'how they could support EP3R' and also 'how EP3R could benefit national PPPs'. Also ENISA will take stock of national PPPs experiences with the engagement of private stakeholders, the provided incentives, the results produced, and the challenges faced. ENISA will also identify Member States that have not established national PPPs. Using ENISA's good practice guide on building PPPs as basis the Agency will offer seminars, workshops and targeted events to relevant stakeholders in these Member States. Upon request, ENISA can also assist in developing a national PPP e.g. providing strategic and technical advice at the planning, establishment and execution phases.	

Finally, ENISA will ensure close cooperation and synergy between EP3R's activity and further international activities in particular the ones conducted in the context of the EU US working group on cyber-security and cyber-crime and develop links to other cross country PPPs (e.g. Financial ISAC, the European Government CERTs group (EGC), the EuroSCSIE for ICS and others).

Manage EP3R working groups and support the Steering Committee

ENISA will establish and manage EP3R working groups through an open and inclusive process. In particular the Agency will work with EP3R stakeholders to identify topics of common interest. ENISA will further identify and engage relevant experts, form virtual groups of experts, and develop when appropriate detailed roadmaps with clear milestones and outcomes. The Agency, with support from external rapporteurs, will also arrange for regular teleconferences, organise quarterly EP3R workshops, update the EP3R portal, draft and peer review position papers, and make sure that working groups deliver according to plan.. Finally, ENISA will provide advisory services to the working group sand will report to the EP3R findings and recommendations from its studies. This will help in assessing opportunities for new working groups.

In 2011 EP3R started with 3 Working Groups. In 2012, some of the initial working groups might conclude their activities and others might be adapted or created to reflect new priorities and address new topics including Smart Grids (building on the outcome from the Ad Hoc Expert Group on Security and Resilience of Communications Networks and Information Systems for Smart Grids established by the Commission in 2010), Emergency Data Communications, Security of Supply Chain. Special emphasis will be given to fighting botnets at European and global level and to national cyber security strategies. ENISA will work with experts from public and private stakeholders to take stock of existing cyber security strategies (in EU and non EU countries as well as OECD, NATO and others), assess them, survey experts to identify good practices, form a dedicated virtual working group to discuss and validate findings, and finally develop a good practice guide on cyber security strategies.

ENISA will support the activities of the Steering Committee of EP3R. The Agency, in co-operation with the European Commission, will engage high level public and private experts in strategic discussions on the results, impact and future directions of EP3R.

Exploit synergies with the ENISA work programme

The Agency will consider the EP3R as an expert community, capable of supporting other elements of the work programme and will inform and involve the group in other activities as appropriate. The EP3R will also be used to disseminate information from other ENISA activities to the public and private sector participants.

Promote EP3R results and recommendations to targeted stakeholders

ENISA will promote EP3R results to relevant public and private stakeholders (e.g. key industry players, Members States, and academia) and participate in relevant workshops, conferences and events. The Agency will work with stakeholders to deploy EP3R results and make sure that impact is achieved.

OUTCOMES AND DEADLINES:

• D1 (Priority HIGH) Dissemination Actions (Q1-Q4 2012) • D2 (Priority HIGH) Management of EP3R Working Groups (Q1-Q42012) • D3 (Priority MEDIUM) Good practice guide on cyber security strategies (report) (Q4-2012) • D4 (Priority HIGH) Three Position Papers (one for each Working Group) (report) (Q4-2012)	
STAKEHOLDER IMPACT	
Telecommunication network providers, Internet Exchange Point providers, Tier 1 providers, Vendors / Manufacturers, Security Providers	Contribute to the discussion on policies to be adopted at national and pan European level, exchange information about good practices (D4)
NRAs, competent national authorities, ministries, European Commission	Understand emerging issue, interact with private sector on possible solutions, contribute to the discussion towards a common pan European strategy (D4)
National PPPs	engage them in the process, help them interact with other national PPPs, share their results and good practices, understand new policy priorities (D2, D3, D4)
RESOURCES FOR 2012 (person months and budget)	
• 80K Euros • 23.8 Person Months	
LEGAL BASE & POLICY CONTEXT	
• ENISA Regulation • The Council Directive 2008/114/EC of 8 December 2008 • The CIIP Action Plan • The Council Resolution of 18 December 2009 • Internal Security Strategy for the European Union	

3.2.8 WPK 2.4.: Implementing Article 13a

WS Name	
WS2: Improving Pan-European CIIP & Resilience	
WORK PACKAGE NAME:	
WPK 2.4: Implementing Article 13a	
DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):	
SMART Goal: By end of Q4 2012, at least 10 Member States deploy ENISA's reporting framework and the good practice guide on minimum security requirements	**KPI**: # Member States
SMART Goal: By end of Q4 2012, at least 10 operators and 10 Member States participate in the study on metrics and thresholds for min security requirements	**KPI**: # Member States # Providers
SMART Goal: By end of Q4 2014, at least 20 Member States deploy ENISA's reporting framework and the good practice guide on minimum security requirements	**KPI**: # Member States
DESCRIPTION OF TASKS:	
The objectives of this work package are to: • Support National Regulatory Authorities (NRA) in transposing article 13a in a harmonised manner across the EU • Develop and implement the process for collecting annual national reports of incidents • Develop minimum security requirements and propose associated metrics and thresholds. Support NRA's in implementing the provisions under article 13a Building on the work of 2011, ENISA will continue working with NRAs towards a harmonised implementation of article 13a. The Agency will assist NRAs and the private sector in implementing the reporting framework at national and EU level (ENISA and Commission). This covers the implementation of the reporting scheme, the classification of security breaches, the parameters and thresholds to be used and the template and procedure for reporting such breaches to NRAs. Based on the experience and knowledge gained through the interaction with NRAs, ENISA will organise dedicated workshops to share good practices with NRAs on the harmonised implementation of article 13a. ENISA will regularly interact with the Commission on the harmonised implementation of article 13a, address with the Commission all legal barriers raised by NRAs, participate in the COCOM and debrief Member States on state of progress.	

Develop and implement the process for collecting annual national reports of security breaches

ENISA, in close co-operation with NRAs, currently develops and implements a process for collecting annual reports of incidents, as foreseen in article 13a. ENISA will continue its efforts in 2012, aiming at delivering the final process by Q3 2012. ENISA will analyse all legal and technical barriers (e.g. how reports are submitted, stored and processed) raised by NRAs in co-operation with the Commission. NRAs are expected to provide guidance on how ENISA should analyse the collected reports and extract conclusions at national and EU level (aggregate analysis). The result of this action will be a process that NRAs will use to submit their reports to ENISA in a secure manner.

In the context of this work, ENISA, together with all NRAs, will help define the conditions and the process for reporting cross-border security breaches affecting more than one Member State (according to the article, the affected Member State needs to immediately inform neighbouring Member States, ENISA and the Commission). ENISA will help define the process to follow, i.e. the notification scheme and the response and recovery actions to be taken in such cases.

As from end of 2012, ENISA will analyse the collected annual reports on security breaches with the objective to provide an overview of the status of security and resilience in the telecommunication sector. The Agency will cluster incidents, assess the most common root causes, and identify the measures taken in different cases. The analysis will reveal good incident management practices during a crisis that could be used by all NRAs. Based on the analysis of the annual incident reports and the discussion with NRAs, ENISA will develop strategic insights for further action in this field. These actions will contribute to the strategy and thematic priorities of EP3R and to new scenarios for future pan European exercises.

Develop minimum security requirements and propose associated metrics and thresholds

Building on the results of 2011, ENISA will work with NRAs to deploy the good practice guide on minimum security requirements.

The Agency will organise dedicated workshops to promote the guide and explain the proposed context, concept and frameworks. Through constant interaction with NRAs, ENISA will validate the applicability of the guide and adapt it to better fit the interests and needs of NRAs. Upon request ENISA can also support NRAs in their efforts to implement nationally the guide. ENISA will regularly interact with the Commission on the deployment of the guide.

ENISA will also try to match the minimum security measures with a proper set of metrics. Metrics can be used by NRAs to assess the adherence of providers to the minimum security measures. The Agency, in constant consultation with NRAs and providers, will develop, validate and adopt the appropriate set of metrics as well as suitable thresholds. During this process, ENISA will use results from previous years

on the matter. The metrics can be used at sectorial, national and even at pan European level. ENISA will also assess whether the experiences of this study could also be used by other sectors (e.g. cloud computing providers).	
OUTCOMES AND DEADLINES:	
• D1 (Priority HIGH): Support NRAs in harmonised implementation of article 13a (workshops) (Q1-Q4 2012) • D2 (Priority HIGH): Framework for collecting annual national reports of security breaches (report)– (Q3 2012) • D3 (Priority HIGH): Metrics and Thresholds for Measuring adherence to Minimum Security Requirements (Q4 2012)	
STAKEHOLDER IMPACT	
Telecommunication network providers, Internet Exchange Point providers, Tier 1 providers	Co-operate with operators on the smooth deployment of article 13a, explain how the article 13a could be implemented, engage them in the adoption of minimum security requirements (D1-D3)
NRAs, competent national authorities, ministries, European Commission	Develop a harmonised view of article 13a, deploy nationally the min security requirements (D1-D3)
RESOURCES FOR 2012 (person months and budget)	
• 120K Euros • 20,90 Person Months	
LEGAL BASE & POLICY CONTEXT	
• ENISA Regulation • Directive 2009/140/EC, Art. 13a and b • The Council Resolution of 18 December 2009 •	

3.3 WS3 – Supporting the CERT and other Operational Communities

3.3.1 Justification

The work packages described in this section are closely aligned with the CIIP Action Plan described in the Commission's communication of March 2009. Much of this work also directly supports objectives laid down in the Internal Security Strategy document.

In the area of CERTs, ENISA aims to support the EU Member States to ensure that their respective national / governmental CERTs act as key components of their national capability for preparedness, information sharing, sustainable coordination and response. This is done by defining, together with the relevant stakeholders, baseline capabilities for national / governmental CERTs, and by providing necessary means to achieve that baseline.

3.3.2 Specific Policy Context

The policy context for this work stream is as follows:

- Digital Agenda – specifically Action 38 (pillar Trust and Security) – 'Member States should establish by 2012 a well-functioning network of CERTs at national level covering all of Europe.'
- COM (2009) 149 on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"
- COM (2011) 163 on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security" adopted on 31 March 2011[24]
- COM (2006) 251 A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"

3.3.3 Overall Objectives

The objective is to assist Member States in implementing secure and resilient ICT systems and to increase the level of protection of critical infrastructure and services in Europe. More specifically, the objectives of this work stream are:

- To enhance the operational capabilities of Member States by helping the CERT community to increase its level of efficiency and effectiveness
- To support and enhance (co)operation between CERTs, and with other communities.

3.3.4 Work Packages

The following work packages constitute the Work Stream:

- WPK 3.1: Support and enhance CERTs operational capabilities
- WPK 3.2: Application of good practice
- WPK 3.3: Support and strengthen cooperation between CERTs, and other communities

[24] "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)

3.3.5 WPK3.1: Support and enhance CERTs operational capabilities

WS Name	
WS3: Supporting the CERT and other Operational Communities	
WORK PACKAGE NAME:	
WPK 3.1: Support and enhance CERTs operational capabilities	
DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):	
SMART goal: By Q4, 80% of updates in CERT inventory are confirmed **SMART goal**: In 6 month after publication receive at least 10 references to each report from external websites, official publications, discussions on mailing lists or other means. **SMART goal**: By Q4 2012, 80% of updates in CERT inventory are confirmed.	**KPI:** % confirmed updates **KPI:** # of references
DESCRIPTION OF TASKS:	
This work package aims at enhancing CERTs capabilities in the EU Member States as well as for the CERT for EU institutions, by provision of good operational practice and the development and facilitation of suitable training and exercises. In its Communication **"A Digital Agenda for Europe"** the European Commission affirms the role of national / governmental CERTs as one key player in the area of trust and security. *Further definition and deployment of baseline capabilities for national / governmental CERTs* The European Commission specified the target deadline for establishing well-functioning national / governmental CERTs in all Member States by the end of 2012. Since 2005, ENISA has supported Member States in this regard, and in 2008 the Agency started to specify baseline technical and policy recommendations of national / governmental CERTs. Work in 2012 will focus firstly on assessing the level of compliance with those baseline capabilities in the MS. Secondly the baseline capabilities will be further discussed with the CERTs, adjusted and where appropriate extended. A special emphasis this year will be put on good practice in national and regional cooperation. **Deliverable:** new version of baseline document and status report on deployment *Further development of capabilities to provide training and exercises for CERTs* *"Member States together with ENISA should [...] undertake regular [...]* ***exercises in incident response****."(* COM(2010) 673; 3rd action).	

ENISA will enhance its capability to deploy good practice in the area of CERT operation (and cooperation). Even though parts of the CERT community work on preparing and deploying training (for example via the successful TRANSITS program, which will be supported further) the situation with regards to training and exercising is far from being sufficient, for new teams but especially for established and more developed teams. In 2012, ENISA therefore plans a two-fold approach: firstly we will produce a new and extended version of the CERT exercise material (which is now an integral part of the TRANSITS courses). Secondly, we will assess the way for a more (pro)active provision of training and exercises for both newly established and mature teams. The direct result will be a roadmap of how to prepare ENISA to provide a sufficient level of educational measures, leveraging on the available good practice material produced since 2005.

Deliverable: updated and refreshed CERT exercise material; roadmap for enhanced training and exercising for CERTs

Collect and provide good practice in the field of early warning and incident detection

*"[...] to react in real-time conditions, a **well-functioning and wider network of Computer Emergency Response Teams (CERTs)** should be established in Europe [...]".* (COM(2010) 245; chapter 2.3)

Leveraging on the work of 2011, in 2012 ENISA will work with the CERT community to produce a good practice document on NIS Early Warning, situational awareness and proactive detection of incidents. The goal is that this material will also contribute to the efforts to make available extended training and exercising for CERTs.

Deliverable: a new exercise scenario "Early Warning 2" to be fed into ENISA exercise and training material.

CERT Inventory complete update

CERTs and similar entities cooperate quite well in communities built in Europe and beyond since more than two decades. ENISA has monitored these activities since 2005 and has developed an inventory of CERT activities in Europe which has been regularly updated. This year the ENISA CERT Inventory will be updated as a whole to reflect the developments in the European landscape accordingly and additionally all current information will be rechecked and updated.

Deliverables: updated document 'CERT Inventory'

Providing support to the CERT community

ENISA has supported various CERT communities and initiatives in Europe and beyond (e.g. FIRST, TF-CSIRT, FI-ISAC, EGC, etc.) for example by providing a secretariat and communication support (FI-ISAC) to enhance CERTs (and other communities)

cooperation and to improve the cross-border incident response capability. ENISA will furthermore continue to strengthen its position as independent and experienced contact for the various European and International CERT communities. This will be accomplished by presenting ENISAs work in events organised by these communities, and enable the communities to influence the agencies work by giving feedback.

OUTCOMES AND DEADLINES:

Summary of outputs with timing (Q1, Q2, etc.):
D1 (Priority HIGH): An updated version of the "Baseline capabilities for national / governmental CERTs" (Q4 – 2012).
D2 (Priority HIGH):. A status report on level of deployment of current set of baseline capabilities of national / governmental CERTs in the MS (Q4 – 2012).
D3 (Priority MEDIUM):. An updated and (where appropriate) extended set of CERT exercise material; a new scenario on "Early Warning" (Q4 – 2012).
D4 (Priority HIGH): A roadmap on how to enhance the roll-out of ENISA exercise material to the CERT communities (Q4 – 2012).
D5 (Priority MEDIUM): Updated "ENISA Inventory of CERTs in Europe" (Q2 and Q4 - 2012).
D6 (Priority MEDIUM): Complete update of Inventory document (Q4 – 2012).

STAKEHOLDER IMPACT

CERT community	The deliverables will support the deployment of "Baseline capabilities for national / governmental CERTs" in the Member States and the EU institutions. In addition other CERTs can benefit from the outcome, for example in training and exercises, but also in self-assessment of capabilities. The trainings and exercises developed in this program are also suited to enhance the cooperation with and better (mutual) understanding of other communities, and by this act as a platform for closer cooperation with these communities (i.e. law enforcement, defence, etc.)

RESOURCES FOR 2012 (person months and budget)

- 202 125Euros
- 24.8 Person Months

LEGAL BASE & POLICY CONTEXT

- ENISA regulation article 3
- Communication on Critical Information Infrastructure Protection (esp. chapters 3.4.3, 5.1, 5.2 and 5.3)
- Communication on "A Digital Agenda for Europe" (esp. chapter 2.3)
- Communication on "The EU Internal Strategy in Action: Five steps towards a more secure Europe" (esp. objective 3)

3.3.6 WPK3.2 Application of good practice

WS Name	
WS3: Supporting the CERT and other Operational Communities	
WORK PACKAGE NAME:	
WPK 3.2: Application of good practice	
DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):	
SMART goal: By Q4 at least two TRANSITS training sessions have been organised with support by ENISA[25]	**KPI:** # of training sessions supported

DESCRIPTION OF TASKS:

This work package aims at strengthening CERTs capabilities in the EU MS as well as for the CERT for EU institutions, by applying good practices in the operational environment.

CERT training support

"Member States together with ENISA should [...] undertake regular [...] ***exercises in incident response****."(* COM(2010) 673; 3rd action).

ENISA will continue to support the successful TRANSITS program for CERT staff members taking place at least twice a year in Europe. The TRANSITS program consists of basic and advance (hands on) courses. Additionally, we will also contribute to the training initiatives of related communities (for example LE community). Other trainings that aim at enhancing CERT capabilities in the Member States and on EU level may be supported as appropriate.

Support for the CERT for EU institutions

"Present in 2010 measures aimed at a reinforced and high level Network and Information Security Policy, including […] measures allowing faster reactions in the event of cyber attacks, including a ***CERT for the EU institutions."*** (COM(2010) 245; chapter 2.3)

In relation to the work of 2011, in 2012 ENISA will continue to support the Pre-configuration-Team for the establishment of a "CERT for EU institutions" as proposed by the "Rat der IT Weisen". ENISA will make available necessary resources to adequately support this CERT in a form that allows the agency to deliver best quality support. .'

Besides other things the Agency will contribute to the steering board for the EU pre-configuration team.

[25] Provided that the organiser of the previous regular TRANSITS courses continue this effort.

Providing support to the operational activities

In reference to the CERT for EU Institutions activities ENISA will continue to support this team to establish operation and carry out all services (e.g. alerts and warning, training and exercises, etc.). In particular the Agency will continue contributing to the work of the steering board for the EU pre-configuration team, detaching resources to the day-to-day business of that team and providing other forms of support as appropriate.

OUTCOMES AND DEADLINES:
Summary of outputs with timing (Q1, Q2, etc): D1 (Priority HIGH): support at least two TRANISTS basic courses, and in addition one TRANISTS enhanced (TRANSITS2) course (Q4 – 2012).

STAKEHOLDER IMPACT	
CERT community	The CERT community will benefit from the support of ENISA for activities related to the deployment of "Baseline capabilities for national / governmental CERTs" in the Member States and EU Institutions. In addition other CERTs can benefit from the outcome, for example in training and exercises. The training sessions and exercises developed in this program will also enhance the cooperation with and better (mutual) understanding of other communities, and by this act as a platform for closer cooperation with these communities (e.g. law enforcement, defence, etc.)

RESOURCES FOR 2012 (person months and budget)
• 30 000Euros • 15 Person Months

LEGAL BASE & POLICY CONTEXT
• ENISA regulation article 3 • Communication on Critical Information Infrastructure Protection (esp. chapters 3.4.3, 5.1, 5.2 and 5.3) • Communication on "A Digital Agenda for Europe" (esp. chapter 2.3) • Communication on "The EU Internal Strategy in Action: Five steps towards a more secure Europe" (esp. objective 3)

3.3.7 WPK3.3: Support and enhance cooperation between CERTs, and with other communities

WS Name	
WS3: Supporting the CERT and Other Operational Communities	
WORK PACKAGE NAME:	
WPK 3.3: Support and enhance cooperation between CERTs, and with other communities	
DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):	
SMART goal: In 6 month after publication receive at least 10 references to each report from external websites, official publications, discussions on mailing lists or other means.	**KPIs:** # of references
SMART goal: By the end of 2012 ENISA built good working relationship with other communities (e.g. EUROPOL, INTERPOL, etc.)	**KPIs:** # of communities
SMART goal: At least 50% of the EU population is represented at the workshops	**KPI**: % of EU population represented
SMART goal: Workshop participants score at least as 3 on a scale of 1-5	**KPI**: average feedback on scale of 1-5 per workshop
DESCRIPTION OF TASKS:	
This work package aims at enhancing the cooperation of CERTs at the European level, by identifying and addressing barriers, and by identifying and advocating incentives. In addition, this package aims at "breaking barriers" between different communities (such as law enforcement) in order to further enhance the capabilities of CERTs to fulfil their duty. This work will contribute to the work on baseline capabilities for national / governmental CERTs in the EU MS as well as for the CERT for EU institutions, and may result in enhanced training and exercises for CERTs in the future. *Development and deployment of EISAS* *"Member States should **network together their national / governmental CERTs** [...] to enhance Europe's preparedness. This activity will also be instrumental in developing [...] a European Information Sharing and Alert System (**EISAS**)"* (COM(2010) 673; 2nd action). This activity aims at further developing EISAS, as foreseen in the EISAS roadmap and described in more detail in the Action Plan for EISAS Enhanced, which formed part of WPK 2.4 in WP 2011. The goal of this activity is two-fold. Firstly, EISAS will, once it is deployed, support the Member States in reaching out to citizens and SMEs with relevant security information, thus representing an important component in the EU's CIIP policy. In addition, EISAS intends to be the result and the additional benefit gained from a reinforced cooperation between national capabilities of EU Member States, primarily national / governmental CERTs. Consequently, the end as such (a deployed EISAS)	

should be seen as equally important as the means to reach that goal.

ENISA will facilitate at least one pilot for EISAS deployment in one Member State, with the support of at least one other Member State. This deployment pilot will focus on two main aspects: collaboration among the relevant key players, and sharing and distributing of good practice information.

Deliverable: Report on the EISAS pilot; enhanced roadmap for activities beyond 2012.

Support cooperation between CERTs and law enforcement

*"Every Member State [...] should have [...] a **well-functioning CERT**. It is important that [...] **CERTs and law enforcement** authorities cooperate"" (* COM(2010) 673; 1st action).
In its **Communication** the European Commission highlights that *"**Cooperation between CERTs and law enforcement** agencies is essential [...]"*(COM(2010) 245; chapter 2.3)

ENISA's activities in this area will be in line with the text of the EU Internal Security Strategy document. In particular, ENISA will not be involved in any operational activity. However, the Agency is in a unique position within Europe to break barriers in cooperation between various communities. In 2011, the Agency started to look into barriers and incentives for the cooperation between CERTs and law enforcement to address cybercrime, established and deepened contacts to stakeholders in both communities and produced a first version of a good practice document. In 2012, ENISA will build on this work, and will propose concrete steps to assist CERTs to improve their collaboration and information exchange with law enforcement resources tasked to prevent and fight cybercrime. This activity is two-fold, which is reflecting the situation in "real everyday life":

Address operational barriers:

Leveraging on the work of 2011, ENISA plans to support national / governmental CERTs to help them in their cooperation with law enforcement, in order to contribute to vital and trusted information exchange, and to the establishment of a "well-functioning network of CERTs". ENISA will also provide assistance regarding a system of contact points between CERTs and Law Enforcement Agencies (LEA), in order to help CERTs to play their part in prevention of cybercrime. An enhanced good practice guide for enabling CERTs to address technical NIS aspects of cybercrime in the form of a report is foreseen in this respect. As for other activities these results shall contribute to ENISAs capability to make available sufficient training and exercise material for CERTs and the law enforcement communities.

Deliverables: enhanced good practice guide, including (if appropriate) concrete measures for improved CERT/LE cooperation (promising areas may be structured exchange of information on new cyber attacks, assistance in cases requiring highly sophisticated digital evidence preservation etc.).; if applicable: draft roadmap to

produce training material

Address legal / regulatory barriers:

CERTs face legal challenges when cooperating and sharing information with law enforcement. ENISA intends to support CERT cooperation on European level by further analysing these legal challenges and providing possible solutions in dialogue with key stakeholders. In addition the Agency intends to start exploring legal and procedural obstacles faced by CERTs from Europe when cooperating and sharing information with CERTs and law enforcement from Third Countries. The output of this analysis would be a report which will also review possible solutions. As for other activities these results shall contribute to ENISAs capability to make available sufficient training and exercise material for CERTs and the law enforcement communities.

Deliverables: good practice guides on legal / regulatory aspects of CERT / law enforcement cooperation; if applicable: draft roadmap to produce training material

Workshop:

A workshop is foreseen in the area of this activity that will bring together the relevant stakeholders from CERT and law enforcement, in order to further discuss obstacles and solutions, to establish concrete actions for closer cooperation. One suitable discussion point for this event could be how to collaborate closer with the envisaged future European Cybercrime Centre (to be realised in 2013)

Deliverables: report on the findings of the workshop (to be shared among the participants only; a summary will be made publicly available!)

OUTCOMES AND DEADLINES:	
Summary of outputs with timing (Q1, Q2, etc.): D1 (Priority HIGH): Pilot of the EISAS activity in one Member State, with the help of ENISA and support by at least one other Member State (Q4 - 2012). D2 (Priority MEDIUM): Updated good practice material for addressing NIS aspects of cybercrime (Q4 - 2012). D3 (Priority MEDIUM): Findings / conclusions from the 7th annual CERT workshop (report, to be shared only among workshop participants (Q3 - 2012).	
STAKEHOLDER IMPACT	
CERT community	The deliverables in this WPK will further strengthen cooperation capabilities for cooperation between MS, and especially national / governmental CERTs. To some extent the deliverables will be useful for other CERTs as well, but to a lesser extent than those in WPK2.1
Other communities, especial law enforcement	As the majority of activities in this WPK are carried out together with the CERT community and law enforcement, law enforcement will benefit greatly from experiences made, for example during the workshop, especially when it comes to understanding the different roles and contributions both

	communities can give to fighting cybercrime. By this a better mutual understanding of roles and responsibilities will be achieved and a platform for more in-depth (future) cooperation is established.
RESOURCES FOR 2012 (person months and budget)	
• 192 125 Euros • 25.2 Person Months	
LEGAL BASE & POLICY CONTEXT	
• ENISA regulation article 3 • Communication on Critical Information Infrastructure Protection (esp. chapters 3.4.3, 5.1, 5.2 and 5.3) • Communication on "A Digital Agenda for Europe" (esp. chapter 2.3) • Communication on "The EU Internal Strategy in Action: Five steps towards a more secure Europe" (esp. objective 3)	

3.4 WS4: Securing the Digital Economy

3.4.1 Justification

Any approach to information security that is to be successful in the long-term must take account of economic drivers and barriers. For this reason, economic aspects of security are attracting increased attention in the NIS world. Economic factors become particularly important during recessionary periods, when the optimal use of scarce financial resources (and notably the reduction of operational expenditure) is one of the key market drivers.

It is clear however that successful approaches to information security are not driven by economics alone. Information assurance and information security governance frameworks are important tools for organizations to identify and control information security risks. There are a number of governance frameworks (COBIT, ISO27K, SOX, e.g.) that are well established in the IT industry. The advent of cyber security as a subject in its own right has put information security governance in the spotlight, as international cooperation is key to resolving many of the associated issues.

The uptake of new technologies and network architectures requires a different focus in security governance. Organizations are increasingly using a complex and connected mix of ICT services, each operated by different external service providers. The service providers in turn use a fragmented supply chain of different partners to deliver these services. In such a setting, it may be cumbersome to use existing control frameworks. Customers (businesses, governmental organizations) need to know how well the IT service is protected, but not always the details about how this is done.

An increasing number of users have been able to transfer their use of commercial and/or public services to the online environment. In this context, interoperability of services is an enabler for the EU digital economy. At the same time, the right for personal data protection still needs continuous efforts to be well supported in online environment. Security and trustworthiness of infrastructure and supply chain needs consolidation.

3.4.2 Specific Policy Context

Specific policy references for this work stream are as follows:

- COM(2010) 245: “A Digital Agenda for Europe“ of 26 August 2010
- COM(2010) 609: “A comprehensive approach on personal data protection in the European Union, Communication” of November, 2010
- COM(2008) 865: “An updated strategic framework for European cooperation in education and training“
- 2009 Malmö Ministerial Declaration on eGovernment
- ITU Resolution 179 (Guadalajara, 2010)
- Interoperability solutions for European public administrations (ISA) (OJ L 260, 3.10.2009, p. 20), available at: http://ec.europa.eu/isa/strategy/index_en.htm.

- 'Towards interoperability for European public services' COM(2010) 744, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, available at: http://ec.europa.eu/isa/strategy/doc/annex_i_eis_en.pdf

3.4.3 Overall Objectives

ENISA aims to address the challenges outlined above in order to ensure that Europe is able to manage properly the introduction and deployment of new interoperable services while respecting fundamental rights of individuals and using secure and trustworthy solutions.

This work will closely monitor and contribute to network and information security aspects of the Future Internet Public Private Partnership (FI-PPP)[26] that aims to advance Europe's competitiveness in Future Internet technologies and systems and to support the emergence of Future Internet-enhanced applications of public and social relevance. It addresses the need to make public service infrastructures and business processes significantly smarter (i.e. more intelligent, more efficient, more sustainable) through tighter integration with Internet networking and computing capabilities. The new business opportunities that will be introduced by the FI also bring new challenges in terms of security and privacy that need to be addressed in a timely manner. The Digital Agenda stresses the importance of effective interoperability between IT products and services to build a truly digital society.

3.4.4 Work Packages

The following work packages constitute the Work Stream:

- WPK 4.1: Economics of Security
- WPK 4.2: Security governance
- WPK 4.3: Supporting the development of secure, interoperable services

[26] The future of the Internet http://ec.europa.eu/information_society/activities/foi/index_en.htm

3.4.5 WPK 4.1: Economics of Security

WS Name	
WS4: Securing the Digital Economy	
WORK PACKAGE NAME:	
WPK 4.1: Economics of Security	
DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals[27]):	
SMART GOAL: At least 5 sector actors (i.e. representatives of industry, regulators, academia, etc.) use the results of the study in projects before end of 2013.	**KPI**: # Sector Actors
DESCRIPTION OF TASKS:	
The objective of this work package is to give guidance on how to prioritise and maximise the effectiveness of investments in security measures. In 2011 ENISA consulted key stakeholders to determine key areas of economics of security and recommend a follow-up strategy. Among the most prominent topics that emerged from this open consultation are: *Behavioural economics of Security* Given the ever increasing complexity in the field of information security, it is often the end user that seems to be the weakest link. They are repeatedly found to make poor security decisions that appear to be careless if not irrational. Things may become critical if these end users operate in a business environment, thus placing their employer at significant business and consequently financial risk. *Software liability* Often a piece of software will come with a license agreement that states that the creator is not liable for any damages that may result from the use of their product. However, do the programmer, publisher, designer, etc. of a piece of software have the right to say that they are not at all responsible? If a company was to produce a common household item, and it was found to be of poor quality and unnecessarily endangered the user with normal use, they would be held responsible in a court of law. Should the same law apply to computer products? The ramifications are even more staggering when one considers that hardware and software can have uses in medical fields, where human lives are at stake, and in financial markets where large sums of money are concerned, and in educational institutions, where performance is measured *Return On Security Investment* Executive decision-makers want to know the impact security is having on the bottom line. In order to know how much they should spend on security, they need to know	

[27] Since the reports that will be the outcome of this activity will be published during Q4/2012 assessment of the relevant KPIs should be carried out in the period of Q2-Q3/2013.

how much is the lack of security costing to the business and what are the most cost-effective solutions. This work package will be based on the output of the 2011 work.
OUTCOMES AND DEADLINES:
D1 (Priority LOW): Report analysing in-depth one of the most prominent topics analysed through the open consultation carried out by ENISA in 2011. (Q4 2012).
STAKEHOLDER IMPACT
Large Organisations SMEs — The report is expected to provide concrete guidance to stakeholders for dealing with the issue of the report. The added value is that the topic(s) to be addressed will be the outcome of a thorough examination carried out by a group of experts in the field of Economics of Security
RESOURCES FOR 2012 (person months and budget)
• 35 599 Euros • 6,0 Person Months
LEGAL BASE & POLICY CONTEXT
• ENISA regulation article 3

3.4.6 WPK 4.2 Security governance

WS Name	
WS4: Securing the Digital Economy	
WORK PACKAGE NAME:	
WPK 4.2: Security governance	
DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):	
SMART GOAL: D1, D2: At least 5 large government agencies involved.	**KPI:** Number of government agencies involved
SMART GOAL: D1, D2 80% of participants found workshop useful and of good quality and support next step.	**KPI:** Number of votes on workshop evaluation forms
SMART GOAL: D3 At least 3 government agencies and 3 network operators involved.	**KPI:** Number of government agencies and network operators involved
SMART GOAL: D4 at least 5 MS involved.	**KPI:** Number of MS involved
DESCRIPTION OF TASKS:	
In this work package ENISA will focus on information security governance in settings with multiple service providers, and in particular bringing together IT service providers, businesses, and governmental organisations to address the following issues: *Supply chain governance:*	

In collaboration with the European Commission (DG Information Society and Media) and the European Public-Private Partnership for resilience[28] (EP3R) ENISA will work towards preparing recommendations on managing supply chain integrity risks of ICT equipment in the EU. In this respect a number of issues will be addressed, briefly summarised below:

- clearly defined product and service requirements consistently carried through the whole supply chain from design, through production, delivery, purchase, installation, and maintenance/upgrade of installed products and systems;
- methodologies for evaluation and verification of components for compliance with upstream requirements;
- ability to evaluate provenance (the confirmed origin) and authenticity of the component parts (hardware, software);
- measures to protect and maintain the integrity of systems, their configuration and operating parameters throughout their originally intended usage model

Contributing in extending and implementing the provisions of Article 4 of ePrivacy Directive (Data Breach Notification):

In 2010 ENISA started its work in the area of data breach notifications, mentioned in the Article 4 of the amended ePrivacy Directive. The first outcome demonstrated that its provisions will in medium and long term significantly contribute to the protection of data as well as user's confidence on digital communications networks and offered services. Further investigations have shown that the Agency could play a significant role in supporting the implementation of specific measures at EU MS level contributing to the actual implementation of Art.4 of the ePrivacy directive (via good practices guidelines, EU level co-ordination, etc.) but also contribute in assessing the feasibility of extending its provisions to other sectors (e.g. finance, retail, health, etc.). In 2012, ENISA will continue and extend the collaboration it already established with the relevant stakeholder (i.e. DG INFSO, DG JUST, EDPS, Art29) also exploring the feasibility of developing an information exchange platform of Data Breach Incidents across the EU. Finally the work performed by ENISA in 2011 on 'monetising privacy' can also be extended through investigations on the impact of different types of secondary use of data (related - unrelated, leakage) as well as the impact in terms of consumers /market behaviour data breach notifications.

OUTCOMES AND DEADLINES:
D1 (Priority MEDIUM): Survey on current practices in supply chain integrity (D3) (Q4 – 2012). D2 (Priority HIGH): Contributing in extending and implementing the provisions of Article 4 of ePrivacy Directive (Data Breach Notification) (D4) (Q4 – 2012).

STAKEHOLDER IMPACT	
National competent bodies	D1 provides national competent bodies with an overview of current practices in

[28] http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/ep3r/index_en.htm

	supply chain integrity.
EU MS regulators, citizens, service providers	D2 helps to implement article 4 of the ePrivacy directive.
RESOURCES FOR 2012 (person months and budget)	
• 90K Euros • 24,6 Person Months	
LEGAL BASE & POLICY CONTEXT	
• ENISA regulation article 3 • Data Protection Directive 95/46/EC • Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive) • COM(2010) 609: "A comprehensive approach on personal data protection in the European Union, Communication" of November, 2010	

3.4.7 WPK 4.3 Supporting the development of secure, interoperable services

WS Name	
WS4: Securing the Digital Economy	
WORK PACKAGE NAME:	
WPK 4.3: Supporting the development of secure, interoperable services	
DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals[29]):	
SMART GOAL: At least 5 sector actors (i.e. representatives of industry, regulators, academia, etc.) validating each report through contributions in the review process, participation in relevant WG's, quotations and references in publications, etc.	**KPI:** # Sector Actors
DESCRIPTION OF TASKS:	
In recent years, a continuously increasing number of users have been able to transfer their use of commercial or public services to the online environment. In this context, interoperability of services is an enabler for EU digital economy. However, further effort is required to reach interoperability of eSignatures, identification and eAuthentication. At the same time the right for personal data protection still needs continuous efforts to be well supported in online environment. Security and trust in infrastructure and supply chain needs consolidation. In this work package ENISA addresses these topics in order to ensure that Europe is able to manage properly the introduction and deployment of new interoperable services while respecting fundamental rights of individuals and using secure and trustworthy solutions. The Agency will take into consideration and will support initiatives proposed by different communities such as: • Future Internet Assembly (FIA)[30], • FI Private Public Partnership (FI PPP)[31] • International Standardisation Organisations (SDOs) such as ETSI, ISO, ITU, etc. and will align these activities with relevant policy initiatives at the level of the EU in support of the Digital Agenda. One of the objectives of ENISA, expressed in its Regulation[32], is to track the development of standards for products and services on network and information security. The Agency has performed in previous years studies identifying gaps in available standards and problem statements for Standards Development Organisations (SDOs). In 2012 ENISA intends to build on top of those activities by supporting SDOs in the process of developing new standards related to the fields of	

[29] Since the reports that will be the outcome of this activity will be published during Q4/2012 assessment of the relevant KPIs should be carried out in the period of Q2-Q3/2013.

[30] The Future Internet is a generic term for research activities on new architectures for the Internet (Wikipedia).

[31] *A public-private partnership on the Future Internet*. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, 28 October 2009, available at: http://ec.europa.eu/information_society/activities/foi/library/fi-communication_en.pdf

[32] 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, Official Journal L077 , 13/03/2004 P. 0001 – 0011, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

expertise of the Agency.

ENISA will support the European Interoperability Strategy and the European Interoperability Framework to be drawn up under the ISA programme (Interoperability Solutions for European Public Administrations[33]). The Agency can contribute to the clusters 'Trusted Information Exchange'[34,] by supporting, at EU level, efforts towards the interoperability of key enablers such as eID, eSignature, etc., as well as to the cluster 'Interoperability Architecture' contributing to the development of a joint vision on interoperability architecture by defining needs for common infrastructure services and common standards from information security perspective i.e. cryptographic minimal requirements. At the same in 2012 the Agency will carry out a practical study/assessment of open source eIdentification, eAuthentication schemes (e.g. Open ID) with an emphasis on security and privacy.

The deployment of a certification scheme for data protection[35] is considered as an approach to establish trust on online services. Examining the network and information security aspects of this activity and providing advice and support as appropriate is aligned with the objectives of the Agency[36]. ENISA can support in exploring the feasibility of implementing a pan-European scheme for trustmarks[37] [38]. The Agency recognises the importance of issuing a code of EU online rights, and will contribute to the network and information security aspects of this action, supporting citizen's digital rights in the EU. This work will be conducted in close collaboration with the European Commission and in particular DG Justice and DG Information Society and Media.
Deliverable: Developing recommendations for network and information security aspects of an EU approach on certification schemes. Identifying criteria and levels of certifications for trustmarks.

Privacy by design is promoted by European Commission[39]. Further work is needed to map and apply the principles of privacy by design in engineering systems[40].

[33] Interoperability solutions for European public administrations (ISA) (OJ L 260, 3.10.2009, p. 20)., available at: http://ec.europa.eu/isa/strategy/index_en.htm , ISA replaces the IDABC programme (Interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (OJ L 181, 18.5.2004, p. 25).
[34] *'Towards interoperability for European public services'* COM(2010) 744, Annex 1, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, available at: http://ec.europa.eu/isa/strategy/doc/annex_i_eis_en.pdf
[35] *A comprehensive approach on personal data protection in the European Union*, Communication COM(2010) 609, November, 2010 http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf
[36] COUNCIL RESOLUTION, 18/12/2009, on a collaborative European approach to Network and Information Security, (2009/C 321/01) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF
[37] *A Digital Agenda for Europe*, COM(2010)245, May, 2010, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245%2801%29:EN:NOT
[38] *A comprehensive approach on personal data protection in the European Union*, Communication COM(2010) 609, November, 2010 http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf
[39] *A comprehensive approach on personal data protection in the European Union*, Communication COM(2010) 609, November, 2010 http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf
[40] *Engineering Privacy by Design,* S. F. Gürses, C. Troncoso, and C. Diaz, in *Computers, Privacy & Data Protection,* 2011, https://www.cosic.esat.kuleuven.be/publications/article-1542.pdf

Furthermore, in this area, technologies proposed by research community are only slowly incorporated by industry[41]. To contribute to this area, ENISA will identify gaps between policy approach, research results and practice requirements for new information technologies applying privacy by design principles (e.g. smart metering). **Deliverable**: Study on deployment of privacy by design principles on new information technologies. During 2012 ENISA aims to organise (and establish) an annual (one day) workshop in the area of Privacy and Trust. The main objective of this event will be to become the reference annual event in the EU covering both policy and research developments in the area of Privacy and Trust. ENISA intends to organise the first edition of this event in collaboration with DG INFSO and possibly with one partner from academia. **Deliverable**: Annual workshop on Privacy, Accountability and Trust in the Future Internet. ENISA will track standards initiatives in the areas of eIdentity and eSignature and will support the Commission in implementing key action 3 of the Digital agenda: "The Commission will propose a revision of the eSignature Directive with a view to provide a legal framework for crossborder recognition and interoperability of secure eAuthentication systems". In particular, ENISA will ensure that its stakeholder community is correctly informed of ongoing activities in this area and will support a more active participation (such as a workshop) if required. **Deliverable**: Report – EU Developments in the area of eIdentity and eSignature.	
OUTCOMES AND DEADLINES:	
D1. Developing recommendations for an EU approach on certification schemes. Identifying criteria and levels of certifications for trustmarks (Q4 - 2012). D2 (Priority LOW): Study on deployment of privacy by design principles on new information technologies (Q4 - 2012). D3 (Priority LOW): Annual workshop on Privacy, Accountability and Trust in the Future Internet (Q2 or Q3 - 2012). D4 (Priority MEDIUM): EU Developments in the area of eIdentity and eSignature (Q4 – 2012)	
STAKEHOLDER IMPACT	
Online providers DPAs, EC	Deliverable 1 will help identifying the risks generated by trustmarks; will provide assurance models and definitions of trust models
Industry, online providers, MS, EC	Deliverable 1 & 2 will provide guidelines for industry and also for new best practices to be used in case of privacy

[41] *Study on the economic benefits of privacy-enhancing technologies (PETs),* European Commission, 2010, http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf

	enhancing technologies as well as for labelling sites from trustworthiness perspective.
RESOURCES FOR 2012 (person months and budget)	
• 185K Euros • 28 Person Months	
LEGAL BASE & POLICY CONTEXT	
• ENISA regulation article 3 • Directive 1999/93/EC eSignature • Interoperability solutions for European public administrations (ISA) (OJ L 260, 3.10.2009, p. 20). • Towards interoperability for European public services' COM(2010) 744, Annex 1, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, • A Digital Agenda for Europe, COM(2010)245, May, 2010, • A comprehensive approach on personal data protection in the European Union, Communication COM(2010) 609, November, 2010 • COUNCIL RESOLUTION, 18/12/ 2009, on a collaborative European approach to Network and Information Security, (2009/C 321/01)	

3.5 Summary of Work Streams and Work Packages

WS1	Identifying & Responding to the Evolving Threat Environment	Budget line	Budget	Person months
WPK1.1	Emerging Opportunities & Risks.	3620	80 000	18,2
WPK1.2	Mitigation & Implementation Strategies.	3600	100 000	15,6
WPK1.3	Knowledge base	3600	70 000	6,0
			250 000	**39,8**
WS2	**Improving Pan-European CIIP & Resilience**	**Budget line**	**Budget**	**Person months**
WPK2.1	Further Securing EU's Critical Information Infrastructures and Services	3610	180 000	21,2
WPK2.2	Cyber Exercises	3610	120 000	24,5
WPK2.3	European Public Private Partnership for Resilience (EP3R)	3610	80 000	23,8
WPK2.4	Implementing Article 13a	3610	120 000	20,9
			500 000	**90.4**
WS3	**Supporting the CERT and other Operational Communities**	**Budget line**	**Budget**	**Person months**
WPK3.1	Support and enhance CERTs operational capabilities	3600	202 125	24,8
WPK3.2	Application of good practice	3600	30 000	15,0
WPK3.3	Support and enhance (co)operation between CERTs, and with other communities	3600	192 125	25,2
			424 250	**65**
WS4	**Securing the Digital Economy**	**Budget line**	**Budget**	**Person months**
WPK4.1	Economics of Security	3620	35 599	6,0
WPK4.2	Security governance	3600	90 000	24,6
WPK4.3	Supporting the development of secure, interoperable services	3620	185 000	28,0
			310 599	**58,6**
Total			**1 484 849**	**253,8**

MISS	Missions (related to tabled activities)	3016	350 000	

3.6 Prioritisation of work packages and deliverables

In order to ensure that ENISA continues to focus on the tasks where it adds the most value, three levels of prioritisation have been included in this year's core work programme (i.e. the defined work streams).

- Prioritisation of work packages.
- Prioritisation of deliverables.

In each case, a priority of HIGH, MEDIUM or LOW has been assigned. These priorities should be interpreted as the importance of the WPK or deliverable with respect to the work programme as a whole. Low priority WPK or deliverables may be cut or reduced subject to budget availability.

WS/WPK	Priority	Deliverable	Priority
WS1 : Identifying & Responding to the Evolving Threat Environment			
WPK 1.1 Emerging Opportunities & Risks.	HIGH	D1 : Security threat landscape in Europe based on aggregated data collected from stakeholders .	HIGH
		D2 : Identification and analysis of specific areas of interest/policy initiatives.	HIGH
		D3 : Opportunities and risks per identified area/policy initiative.	HIGH
WPK 1.2 Mitigation & Implementation Strategies.	HIGH	D1 : Periodic report on recommendations for mitigating the risks considered and materialisation of opportunities .	HIGH
		D2 : Implementation guidance per area/policy initiative.	MEDIUM
WPK 1.3 Knowledge base	LOW	D1 : Knowledge Base and associated procedures.	LOW
		D2 : Stakeholder Requirements (Q4 - 2012)	LOW
WS2 : Improving Pan-European CIIP & Resilience			
WPK 2.1 Further Securing EU's Critical Information Infrastructures and Services	HIGH	D1 : Cyber Security Risks and Challenges of Smart Grids.	HIGH
		D2 : Cloud computing and Critical Services.	HIGH
		D3 : Good Practice Guide on Rerouting and Emergency Communications during Crisis.	MEDIUM
WPK 2.2 Cyber Exercises	HIGH	D1 :Report of CYBER EUROPE 2012 (report) (Q4 2012)	HIGH
		D2 : Status Report on National and International CIIP Exercises (report) (Q3 2012)	HIGH
		D3 : Roadmap on Exercising for CIIP beyond 2012 (report) (Q32012)	HIGH
WPK 2.3 European Public Private Partnership for Resilience (EP3R)	HIGH	D1 : Dissemination Actions (Q1-Q4 2012)	HIGH
		D2 : Management of EP3R Working Groups (Q1-Q42012)	HIGH
		D3 : Good practice guide on cyber security strategies (report) (Q4-2012)	MEDIUM
		D4 : Three Position Papers (one for each Working Group) (report) (Q4-2012)	HIGH
WPK 2.4 Implementing Article 13 a	HIGH	D1 : Support NRAs in harmonised implementation of article 13a (workshops) (Q1-Q4 2012)	HIGH
		D2 : Framework for collecting annual national reports of security breaches (report)– (Q3 2012)	HIGH
		D3 : Metrics and Thresholds for Measuring adherence to Minimum Security Requirements (Q4 2012)	HIGH
WS3 : Supporting the CERT and other Operational Communities			
WPK 3.1 Support and enhance CERTs operational capabilities		D1 : An updated version of the "Baseline capabilities for national / governmental CERTs".	HIGH
		D2 : A status report on level of deployment of	HIGH

	HIGH	current set of baseline capabilities of national / governmental CERTs in the MS).	
		D3 : An updated and (where appropriate) extended set of CERT exercise material; a new scenario on "Early Warning".	MEDIUM
		D4 : A roadmap on how to enhance the roll-out of ENISA exercise material to the CERT communities.	HIGH
		D5 : Updated "ENISA Inventory of CERTs in Europe" .	MEDIUM
		D6 : Complete update of Inventory document.	MEDIUM
WPK 3.2 Application of good practice	HIGH	D1 : support at least two TRANISTS basic courses, and in addition one TRANISTS enhanced (TRANSITS2) course.	HIGH
WPK 3.3 Support and enhance (co)operation between CERTs, and with other communities	HIGH	D1 : Pilot of the EISAS activity in one Member State, with the help of ENISA and support by at least one other Member State (Q4 - 2012).	HIGH
		D2 : Updated good practice material for addressing NIS aspects of cybercrime .	MEDIUM
		D3 : Findings / conclusions from the 7th annual CERT workshop (report, to be shared only among workshop participants.	MEDIUM
WS4 : Securing the Digital Economy			
WPK 4.1 Economics of Security	LOW	D1 : Report analysing in-depth one of the most prominent topics analysed through the open consultation carried out by ENISA in 2011.	LOW
WPK 4.2 Security governance	LOW		
		D1 : Survey on current practices in supply chain integrity.	MEDIUM
		D2 : Contributing in extending and implementing the provisions of Article 4 of ePrivacy Directive (Data Breach Notification).	HIGH
WPK 4.3 Supporting the development of secure, interoperable services	LOW	D1 : Developing recommendations for an EU approach on certification schemes. Identifying criteria and levels of certifications for trustmarks .	LOW
		D2 : Study on deployment of privacy by design principles on new information technologies.	LOW
		D3 : Annual workshop on Privacy, Accountability and Trust in the Future Internet.	LOW
		D4 : EU Developments in the area of eIdentity and eSignature	MEDIUM

4 Stakeholder Relations

4.1 Management Board & Permanent Stakeholder Group Secretariat

WORK PACKAGE NAME:
SR1: Management Board & Permanent Stakeholder Group Secretariat
DESCRIPTION OF TASKS:
Management Board The structure of ENISA's Management Board is laid down in the Agency's founding Regulations. As in previous years, two formal meetings will be organised; in 2012, joint informal meetings of sub-groups will be held with the PSG as appropriate. The existing electronic newsletter will be continued throughout 2012. *Permanent Stakeholders Group* Members of the PSG primarily act as advisors to the Executive Director. In addition to their well-established role in advising on the overall content and orientation of the work programme, they will also be asked to promote ENISA WP activities within the NIS Stakeholder network communities and as sources of advice on experts for TCD expert groups. In 2012, as in the past, two formal meetings will be organised and joint informal meetings of sub-groups will be held with the Management Board as and when required. Improved leadership and communication capabilities for identified sub-groups of NIS Stakeholder network communities will continue through the usage of inter-active portal-based communities of interest and face-to-face meetings around specific issue areas (particularly in relation to public-private cooperation) with NCON members.
OUTCOMES AND DEADLINES:
D1. 2 formal meetings of the Management Board (Q1 & Q4, 2012) D2. 4 releases of the Electronic Newsletter for the MB (Q1, Q2, Q3, Q4 – 2012). D3. 2 formal meetings of the Permanent Stakeholder Group (Q1 & Q4, 2012) D4. Informal meetings and sub-group meetings as required.
STAKEHOLDER IMPACT
Management Board: Improved communication between the MB and ENISA. More timely recognition and resolution of issues Permanent Stakeholder Group: More effective use of the PSG. Increased emphasis on getting PSG advice and using this in core activities.
RESOURCES FOR 2012 (person months and budget)
• 170K Euros • 6 Person Months

4.2 National Contact Officers (NCO) Networks

WORK PACKAGE NAME:
SR2: National Contact Officers (NCO) Network

DESCRIPTION OF TASKS:	
The National Contact Officers (NCO) is an extension of the National Liaison Officers (NLO). The NLO is extended with contact points from Governmental CERTs and Regulatory Bodies/Agencies. A single point of contact by NLOs in MS will be maintained for those officials acting in direct support of (or who themselves are) members of the ENISA Management Board. But more structured on going contact will be developed with personnel in national regulatory agencies and the range of government ministries with whom we already either have to or do interact but on a sporadic and piecemeal basis using the National Contact Officers Networks (NCONs), which are being established on a non-permanent, ad hoc basis. We envision organising small meetings of a limited number of NCOs according to the particular interests of different groups of MS. We would expect these meetings to discuss (perhaps even develop themselves) and agree particular work programme activities, and then to validate/approve outcomes.	
OUTCOMES AND DEADLINES:	
D1. Ad Hoc meetings with National Contact Officers on particular issues. D2. Input to the 2013 work programme (Q1 – 2012)	
STAKEHOLDER IMPACT	
National Contact officers	Increased dialogue with NCONs and more effective deployment of NIS policies.
Member States	More effective use of NCONs should result in a more effective dialogue with MS and should enable ENISA to reduce its use of other instruments (such as questionnaires).
RESOURCES FOR 2012 (person months and budget)	
• 3,0 Person Months	

4.3 EU Relations

WORK PACKAGE NAME:
SR3: EU Relations
DESCRIPTION OF TASKS:
The Agency will continuously develop and enhance relations with EU Institutions and Bodies. More precisely, this involves amongst other tasks the analysis and review of EU policy acts by liaising and interacting with EU policy makers, by injecting expertise and by raising ENISAs profile by participating in high-level events. ENISA shall provide advice and assistance, as provided in its founding regulation, to the EU Institutions regarding relevant NIS policy issues. Developing and maintaining a network of key actors, advocacy and regular interaction with ENISA's relevant stakeholders in the EU Institutions is highly

importance in order to raise the Agency's profile as such and, finally, to 'enhance the levels of security in Europe'.
OUTCOMES AND DEADLINES:
D1. Analysis and review of relevant EU policies (as required). D2. ENISA presence in High-Level Events. D3. Input to NIS policy on an as needed basis.
STAKEHOLDER IMPACT

Member States	Close interaction with representatives of the Parliament and the Council will allow ENISA to identify issues that are potentially important for MS and to involve them in the discussions at a sufficiently early stage.
EU institutions	By liaising closely with the EU institutions, ENISA can be instrumental in helping to harmonise the approach to information security within the institutions themselves.

RESOURCES FOR 2012 (person months and budget)
• 7.2 Person Months

4.4 Managing Stakeholder Relations

WORK PACKAGE NAME:
SR4: Managing Stakeholder Relation
DESCRIPTION OF TASKS:
The agency will refine its approach to maintaining and developing its stakeholder community in order to have a clear, updated and appropriate position with respect to each of its stakeholders. This essentially involves ensuring that ENISA is investing in reciprocal, evolving and mutually defined stakeholder's relationships, which will enable the Agency to keep its goals aligned with stakeholder's expectations. *Structured Approach to Stakeholder Management* In order to achieve this, ENISA will establish an on-going process for analysing stakeholder communities and relating these communities to core activities of the work programme. This analysis will help the Agency to better understand the needs of its stakeholders and how best to satisfy their requirements within the scope of the limits established by the latter. In particular, the CRM system will be used to help ensure that ENISA does not duplicate existing points of contact, either within the Agency itself or with other European bodies. *Deployment of the CRM platform* The work on the CRM platform carried out in 2012 as part of this activity builds on the work of 2011. In 2012, ENISA will deploy the interactive platform, which will

further enhance the ability of the Agency to reach and interactively involve appropriate stakeholders in the agency's activities, to build stakeholder communities and to facilitate cooperation and information sharing among them.	
OUTCOMES AND DEADLINES:	
D1. A Structured Approach to Stakeholder Management (Q2 - 2012) D2. A fully deployed CRM system (Q3 – 2012) D3. Accompanying procedures (Q3 – 2012)	
STAKEHOLDER IMPACT	
Management Board	A clear stakeholder strategy will help the Management Board to understand how the Agency interacts with its various stakeholder communities.
All Communities	ENISA expects to liaise more effectively with all communities as a result of the SRM platform.
RESOURCES FOR 2012 (person months and budget)	
• 13.1 Person Months	

4.5 Summary Table

Activity	Stakeholder Relations	Budget line	Budget	Person Months
SR1	Management Board & Permanent Stakeholder Group Secretariat	3001	170 000	6,0
SR2	National Contact Officers Networks		N/A	3,0
SR3	EU Relations		N/A	7,2
SR4	Managing Stakeholder Relations		N/A	13,1
Total			**170 000**	**29.3**

MISS	Missions (related to tabled activities)	3016	38 000	

5 Project Support Activities

5.1 Awareness Raising Activities

WORK PACKAGE NAME:	
PR1: Awareness Raising Activities	
DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):	
SMART goal: By end of Q3 2012, at least one set of supporting and educational material is produced in at least three European official languages	**KPI**: # supporting and educational material
DESCRIPTION OF TASKS:	
Correctly securing systems involves successfully combining people, processes and technology and ill-informed citizens can sometimes be the weakest link in a system's defences. The final work package of this work stream is therefore concerned with ENISA's stakeholders with appropriate and up-to-date information on risks and countermeasures in order to enable them to react appropriately in the electronic world. ENISA considers awareness raising as a 'horizontal activity' in the sense that most awareness raising activities take place within the particular work packages defined by the work plan. It is clear however, that there is a need to coordinate the messages being passed in the different subject areas. The objectives of this project support activity are as follows: • Ensuring the coherence at the Agency level of awareness raising initiatives that take place within individual work packages. • Coordination of activities that are not specific to any subject area. • Promoting the use of technology to achieve a greater impact. *Ensuring coherence of awareness raising activities* This task involves liaising regularly with the teams that implement the different work packages of the work programme and ensuring that the messages that are being passed are coherent from an agency perspective. *Coordination of activities that are not specific to any subject area* Three actions are envisaged for 2012: • Follow-up activities to the work carried out in the 2011 work programme on the feasibility of a European month of network and information security for all • Support for the Awareness Raising area of the EU-U.S. Working Group on Cyber-security and Cyber-crime • Follow-up activities to the work carried out in the 2011 work programme on the	

introduction of NIS into the curricula of schools. *Promoting the use of technology to achieve a greater impact* The aim of this work is to identify technology channels that could be useful for supporting awareness raising activities and to support their use in the various activities that ENISA undertakes. Particular attention will be given to new media technologies (e.g. e-Commerce, social networks, etc.).
OUTCOMES AND DEADLINES:
D1. Implementation of 2011 recommendations on the European Month of Network & Information Security for all (Q4 – 2012). D2. Transfer of experience in implementing NIS within the school curriculum (Q4 – 2012).
STAKEHOLDER IMPACT
Citizens: D1 will increase the level of understanding of information security concepts and enhance fundamental skills. School children: D1 will increase the level of understanding of information security and help mitigate risks for children. This is a considerable benefit for society, as tomorrow's generation will develop an understanding of the risks and possible solutions at a much earlier age.
RESOURCES FOR 2012 (person months and budget)
• 55K Euros • 9,6 Person Months
LEGAL BASIS
• COM(2010) 245: "A Digital Agenda for Europe" of 26 August 2010 • COM(2008) 865: "An updated strategic framework for European cooperation in education and training" • 2009 Malmö Ministerial Declaration on eGovernment • ITU Resolution 179 (Guadalajara, 2010)

5.2 Targeted dissemination

WORK PACKAGE NAME:
PS2: Targeted Dissemination
DESCRIPTION OF TASKS:
ENISA recognises the importance of disseminating its findings and recommendations and will adopt a strategic approach to create impact among its stakeholders within the NIS field. This work package aims at featuring step-by step guidance to ensure that substantiated advice by ENISA is disseminated in a suitable format that is meaningful to targeted stakeholders. The objective is to complement the specific dissemination activities of the content owners within ENISA, by opening up their deliverables to new groups of stakeholders.
OUTCOMES AND DEADLINES:
D1. Dissemination plan associated with each work package (Q1 2012)

D2. General guidelines for future dissemination (Q4 2012)	
STAKEHOLDER IMPACT	
All Communities	More effective dissemination of ENISA's results should lead to direct improvements in information security within the stakeholder communities that ENISA serves.
RESOURCES FOR 2012 (person months and budget)	
• 3,0 Person Months	

5.3 Flash Notes Service

WORK PACKAGE NAME:	
PS3: Flash Notes Service	
DESCRIPTION OF TASKS:	
Flash notes will be issued in order to communicate ENISA's position on high profile NIS topics arising in the public political debate and the media. Flash notes may be disseminated in the form of press releases, RSS feeds, News Items or directly to concerned stakeholders such as the Parent DG, the MB and PSG of ENISA. Such service is considered to be demand driven based on the needs of NIS stakeholders and its scope will be restricted to ENISA's activities. The position of ENISA will be issued on an evidence based, well-reasoned and objective analysis.	
OUTCOMES AND DEADLINES:	
D1. Flash Notes on particular topics as required	
STAKEHOLDER IMPACT	
Commission	The intention is to use this service to 'feed' the corresponding service within the Commission.
Other Communities	Other communities could benefit from this service. This will depend on the subject matter of the Note.
RESOURCES FOR 2012 (person months and budget)	
• 0,0 Person Months (negligible)	

5.4 Work on standardisation

WORK PACKAGE NAME:
PS4: Work on Standardisation
DESCRIPTION OF TASKS:
In 2010 ENISA has established the collaboration with ETSI TISPAN in the area of resilient architectures. This collaboration was continued in 2011 through the participation in meetings of TISPAN WG7 and collaboration in the elaboration of a study on ontology and taxonomies of resilience. At the same time contacts with ISO SC27 were launched (WG5 – Identity management and privacy technologies) and ITU SG17.

In 2012, ENISA will continue its involvement in the International standardisation process and maintain links with standardisation bodies. As part of this work, the Agency will seek out synergies with the work programme and involve standards bodies in the different work packages in as far as this is appropriate. The work in this area will ensure that any activities associated with standards and contained in the different work packages will be correctly coordinated at the Agency level.
OUTCOMES AND DEADLINES:
Alignment with work package objectives.
STAKEHOLDER IMPACT
All Communities — Close collaboration with standards bodies will be of benefit to all communities..
RESOURCES FOR 2012 (person months and budget)
• Accounted for in existing work packages.

5.5 Summary Table

Activity	Project Support Activity	Budget line	Budget	Person Months	Priority
PS1	Awareness Raising Activities	3600	55 000	9,6	Medium
PS2	Targeted Dissemination		N/A	3,0	High
PS3	Flash Notes Service		N/A	0,0	Medium
PS4	Work on Standardisation		N/A	N/A	Medium
Total			**55 000**	**12,6**	

6 Policy & Public Affairs activities

6.1 Public Affairs activities

6.1.1 Introduction

In 2012, the Agency will continue to endeavour its visibility towards key actors and decision-makers in IT Security through its updated Communication Strategy. ENISA will be reaching out to NIS communities to promote its work, underlining the importance of NIS for the economy and security of the critical information infrastructure of Europe, and to facilitate all the stakeholders to make informed decisions on NIS matters. The Agency's external communication channels are complemented by enhancing its internal communication activities.

6.1.2 Aligning to the Policy Environment

The Agency's annual work programme shall be aligned to the given European Union policy framework and environment ensuring coherence and continuity in the Agency's short- and medium-term.

ENISA shall maintain its capability of assessing NIS related technical and political challenges, the general policy environment, threat landscape, market technologies, and needs of its stakeholders in order to be able to adjust its priorities and work accordingly. The Agency's strategic approach shall be developed in close consultation with its stakeholders, including the EU Member States, the European Commission, the Agency's Management Board and Permanent Stakeholders' Group.

ENISA continuously monitors and takes account of all NIS areas with a view to advance ENISA's positioning in relation to the given policy context. This results in media, public affairs, and events activities in line with the advocacy and positioning of the Agency vis-à-vis key stakeholders.

According to Art. 10 of the ENISA Regulation, the Agency shall maintain the capability to reply to requests posed by the European Parliament, the European Commission and by notified bodies of the Member States.

6.1.3 Public Relations

The Agency will continue raising its profile as to achieve an increased impact and to raise Network and Information Security in general on the political agenda. Increasing visibility and awareness with key actors at strategic and decision-making level is key to live up its regulation based mission to 'enhance the levels of security in Europe'. This includes, among other things, developing and maintaining a network of key actors, participating in relevant for organising high-level meetings and participating in high-level events (e.g. EU Presidency related events).

The Agency maintains close cooperation with relevant EU-Agencies, and with the Intra EU-Agencies HCIN network (Heads of Communications and Information Network),. ENISA Digital Communication

The ENISA corporate website is the Agency's primary external communication channel. It also serves as "business card" to key stakeholders, as well as the interested public. The website shall meet the increasing need to communicate effectively with the wider public, stakeholders in general and NIS communities in particular, and to disseminate the Agency's reports and studies. The Agency will enhance the website by providing a number of portals, and move towards an interactive, collaborative communication platform to empower stakeholders to work with ENISA more effectively and efficiently. Web usability surveys of corporate website and community portals shall be conducted to support continuous improvement of the sites' navigation, design and user friendliness. The Agency shall also strive for providing compelling digital content, such as video clips, and to increase website traffic in general.

6.1.4 ENISA Publications and Brand Materials

The Agency has shifted its efforts to reduce printed publications, to both reduce costs and its environmental footprint. In accordance with its founding regulation, ENISA publishes a General Report covering its activities during the previous year. Furthermore, the Agency publishes corporate material, such as fact sheets, corporate brochures and leaflets. Therefore, the Agency intends to review the existing publications, and consider the best possible online publications.
To ensure coherent brand communication through all communication channels, the Agency maintains its corporate brand visibility manual and templates. It uses a databank comprising professional images in addition to own photos of events with a view to a coherent audio visual appearance, across all channels, online, in PPTs, video clips, and its publications.

6.1.5 Spokesman and Media Relations

The Agency communicates to the wider public through press and media channels. ENISA maintains a network of both general and specialised media contacts across Europe, issues press releases in five languages, conducts interviews, organises press conferences, and monitors media uptake. Media impact shall be increased through communication planning through a 'communication calendar', targeting key media at Member State level and update its contact with key communication actors in the Member States bodies. The ENISA Spokesman acts as primary contact for press and media communication.

6.1.6 ENISA Events

The Agency ensures visibility and disseminates its results at conferences and major political events for NIS and ICT stakeholder communities. ENISA presents itself in Brussels and other major cities with several dedicated events, (e.g.) one being a high-level discussion forum and another being the presentation of the annual General Report. The objective is to contribute to an overall positive appearance and presentation of the Agency.

6.1.7 ENISA Internal Communication

Team work and information sharing between all staff has always been key to the success of ENISA's internal communication. In order to guarantee pro-active communication channels, ENISA has established various internal communication means including lasting information sharing platforms such as its intranet. ENISA organises, among other measures, weekly staff meetings providing an opportunity to raise issues directly by means of face-to-face communication. Surveys and team buildings will also be implemented in 2012, in order to guarantee a smooth internal communication in the Agency.

6.2 Summary of Public Affairs Activities

PAU	Public Affairs	Budget line	Budget	Person Months	Priority
PAU 1	Aligning to the Policy Environment	N/A	N/A	3	High
PAU 2	Public Relations	N/A	N/A	7	High
PAU 3	ENISA Digital Communication	3220	81.000	9,5	Medium
PAU 4	Publications and Brand Materials	3240	65.000	4,7	Medium
PAU 5	Spokesman and Media Relations	3210	49.000	9,6	High
PAU 6	ENISA Events	3200	15.000	4,5	High
PAU 7	ENISA Internal Communication	N/A	N/A	4,5	High
Total			**210.000**	**42,8**	

MISS	Missions (related to tabled activities)	3016	35.000		

7 IT Services

7.1 Purpose

The IT Services Unit (ITSU) is an autonomous unit reporting directly to the Executive Director, delivering ICT services across the agency, including server and desktop computing, security, service desk, email, telephony, network storage, printing, Internet and Intranet, etc.

7.2 Activities

During 2012, apart from the regular activities carried out by ITSU, the focus will be on testing of parts of the IT continuity plan, enhancement of user productivity through the introduction of additional e-workflows and mobility tools and improving online meeting and communication functionality.

7.3 Summary of Activities related to IT Services

Activity	Unit	Budget line	Budget	Person Months
ITSU 1	ICT Administration	N/A	N/A	9,5
ITSU 2	ICT Services	2300	30 000	9,5
ITSU 3	ICT Support	2301, 2302	150 000	9,5
ITSU 4	Telecommunications	2202	45 000	9,5
			225 000	**38,0**

MISS	Missions (related to tabled activities)	3016	5.000	

8 Administration activities

8.1 Purpose

The Administration Department contributes to the goals of the Agency with regard to service, compliance and assurance. In 2012 the Administration aims at further expanding electronic workflows in service areas where such workflows are not available yet while maintaining a good service level of existing ones. In 2012, the Administration Department seeks to:

- Mitigate assurance and compliance risks
- Broaden the scope of electronic workflows currently in use at the Agency to allow for remote working

8.2 General Administration

General administration tasks contribute to the management and measurement of performance of the Administration Department, including people management. Major tasks include planning, advising, representing, reporting upon and controlling the activities of the Sections and the Department.

In 2012 the Administration Department will broaden the scope of electronic workflows and implement an electronic procurement system and tool, as well as workflows with financial support orientation. The Agency will build on the experience gained by means of a process redesign project, and ex post controls project and the implementation of the ABAC suite in a coherent manner. Ad hoc operational tasks as it might be needed and agreed with the operational Departments might also be supported, as required. In 2012 the priorities of General Administration include:

- Further mitigate assurance and compliance risks
- Carry out the multi-annual planning of activities
- Maintain a high degree of annual budget execution
- Re-evaluate the scope and delivery method of services offered
- Coordinate internal control activities
- Deploy additional electronic workflows
- Continue ensuring business continuity (subject to resource availability)
- Continue working on the set up of the new ENISA building
- Laying out remote ways of work
- Carry out project management in such areas as building management, process redesign etc.

8.3 Accounting and Finance

Accounting at ENISA is a discreet function that addresses the following tasks in line with the Financial Regulation of ENISA:[42]

- Preparing the annual accounts of the Agency
- Keeping the accounts of the Agency
- Laying down and validation of accounting systems
- Keeping assets inventories
- Execution of Payments and collection of revenue
- Treasury management

Finally, the coordination of audits conducted by the European Court of Auditors falls in the responsibility of the Accounting area.

Finance carries out budget planning, administration and financial control, portions of payroll administration and missions' overview and back up. The goal of Accounting and Finance Section is to ensure the credibility of financial circuits and budget planning. Close monitoring of Budget planning and execution allows the Agency to increase its Budget utilisation rates to the benefit of its operations and counterbalance budget constraints. In 2012 the priorities of Accounting and Finance include:

- Budget planning including activity based budgeting
- Monitoring of budget execution and planning
- Functional support regarding electronic workflows (ABAC, missions' management)
- The revision of finance and accounting procedures
- Contributing to the internal control environment of the Agency
- Supporting the process redesign and the deployment of electronic workflows

8.4 Human Resources

Human resources carry out recruitments, performance evaluations, organisation of trainings, health and safety at work, leave management handling of individual rights and payroll management. In 2012 the priorities of the HR Section include:

- Multi annual resource planning
- Affirmative measurable measures for staff retention (attrition rates, goals, cost of turnover, trainings, promotions etc.)
- Services through electronic workflows
- Staff evaluation
- Additional measures e.g. team building
- Follow up of health and safety measures

[42] Accounting comprises of the tasks of the Accounting Officer, which is an independent function reporting directly to the ED.

8.5 Legal

The Legal Section carries out budget implementation and control activities that include general contract management and public procurement of the Agency. The Legal Section services the Agency with regard to litigation and pre-litigation support. The Legal Section plays a role to ensure compliance with regard to prevailing legal rules and regulations and in order to make available service to management and staff as appropriate in order to meet compliance objectives. The Legal Section makes available to the Agency legal advice, legal services as well as procurement guidance and services. In 2012 the priorities of the Legal Section include:

- Efficient procurement project planning and execution.
- Contract management planning
- Follow up on compliance matters
- Implement electronic workflows in the area of procurement and support process redesign

8.6 Summary of Administration Activities

ADA 1	General Administration	Budget line	Budget	Person months[43]	New Activity
	TOTAL	Title 2 (except for BL 2202 and Chapter 23)	326 000	57.6	
ADA 2	**Accounting and Finance**	**Budget line**	**Budget**	**Man months**	**New Activity**
	TOTAL		0	38.4	
ADA 3	**Human Resources**	**Budget line**	**Budget**	**Man months**	**New Activity**
	TOTAL	Title 1	5 532 044	28.8	
ADA 4	**Legal and procurement**	**Budget line**	**Budget**	**Man months**	**New Activity**
	TOTAL		0	19.2	
	GRAND TOTAL		5 858 044	144	

MISS	Missions related to tabled activities	3016	35 000		
MISS	Missions related to ED activities	3016	35 000		

[43] A full year is calculated on the basis of 9.6 months per staff member on the staff planning chart.

9 APPENDIX A: OPERATIONAL BUDGET LINES (TITLE 3)

Table: Activities and corresponding Budget Lines in Statement of Estimates 2012 (Budget 2012)

Statement of Estimates 2012		Work Programme 2012			
Budget Line	**Heading**	**WP ref.**	**Title**	**Amount**	**Totals**
3001	Meetings of official Bodies	**SR1**	Management Board & Permanent Stakeholder Group Secretariat	170.000	170.000
3005	Executive Director Office Meetings	**n/a**	NB: Meetings managed by AD	5.000	5.000
3011	Entertainment and Representation expenses	**n/a**	NB: Meetings managed by AD	5.000	5.000
3016	Missions	**MISS**	Missions of all staff	498.000	498.000
3021	Other Operational meetings	**n/a**	NB: Meetings managed by AD	10.000	10.000
3200	Conferences and Joint Events	**PAU 6**	ENISA Brand events	15.000	15.000
3210	Communication activities	**PAU 5**	Spokesman & Media relations	49.000	49.000
3220	Web Site Development	**PAU 3**	ENISA Digital Communication	81.000	81.000
3230	Translations	**n/a**	NB: Translations managed by AD	29.256	29.256
3240	Publications	**PAU 4**	Publications and Brand Materials	65.000	65.000
3600	Stakeholders' collaboration	**WPK1.2**	Mitigation & Implementation Strategies	100.000	739.250
		WPK1.3	Knowledge base	70.000	
		WPK3.1	Support & Enhance CERTs Operational Capabilities	202.125	
		WPK3.2	Application of good practice	30.000	
		WPK3.3	Support & Enhance Cooperation Between CERTs and Other Communities	192.125	
		WPK4.2	Security governance	90.000	
		PS1	Awareness Raising Activities	55.000	
3610	NIS Policy	**WPK2.1**	Further Securing EU's Critical Infrastructures and Services	180.000	500.000
		WPK2.2	Cyber Exercises	120.000	
		WPK2.3	Pan-European Public Private Partnership for Resilience (EP3R)	80.000	
		WPK2.4	Implementing Article 13 a	120.000	
3620	NIS Technology	**WPK1.1**	Technology Opportunities & Risks	80.000	310.599
		WPK4.1	Economics of Security	35.599	
		WPK4.3	R&D in support of the Digital Agenda	185.000	
	Grand total - Title 3			**2.467.105**	**2.467.105**

10 APPENDIX B: OPERATIONAL ACTIVITIES 2012 (Activity Based Budgeting)

Table: Total Budget expenditure split by Operational Activity (Activity Based Budgeting)

OPERATIONAL ACTIVITIES 2011	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 - Identifying & Responding to the Evolving Threat Environment	**4,1**	**337.920**	**250.000**	**246.375**	**834.294**
WS2 - Improving Pan-European CIIP & Resilience	**9,4**	**794.056**	**500.000**	**559.605**	**1.853.660**
WS3 - Supporting the CERT & Other Operational Communities	**6,8**	**559.592**	**424.250**	**402.371**	**1.386.213**
WS4 - Security Economics & Governance	**6,1**	**503.040**	**310.599**	**362.753**	**1.176.392**
Stakeholder Relations	**3,1**	**219.105**	**170.000**	**181.376**	**570.481**
Project Support Activities	**1,3**	**116.309**	**55.000**	**77.998**	**249.307**
Policy & Public Affairs Activities	**4,5**	**395.081**	**210.000**	**264.946**	**870.026**
Missions & Representation	**0,0**	**0**	**508.000**	**0**	**508.000**
Management & Support activities (Note 5)	**7,2**	**636.006**	**39.256**	**426.513**	**1.101.775**
Total (Note 6)	**42,4**	**3.561.108**	**2.467.105**	**2.521.936**	**8.550.149**

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 activity, provided for in WP and the Statement of Expenditure 2012.
Note 4 - Overheads include all costs which are indirectly involved in the implementation of WP 2012, such as salary costs of non-operational staff, rent, and running costs (e.g. Office supplies).
Note 5 - Management & Support activities include the budget allocated to Other operational meetings (Budget Line 3021) and Translations (Budget Line 3230) of the Agency.
Note 6 - The total human resources in person/years figure (42,4) differs from the actual man power for the year 2012 (44 posts) due to recruitment planning, which affects new staff availability, as well as part time working schemes of existing staff.