

# WORK

## Programme 2009

Build on Synergies - Achieve Impact



## Table of contents

<b>1</b>	<b>INTRODUCTION</b>	<b>1</b>
1.1	Policy context	1
1.2	Key challenges	2
1.3	ENISA's role	2
1.4	New Work Programme approach and beyond	3
<b>2</b>	<b>MULTI-ANNUAL THEMATIC PROGRAMMES</b>	<b>6</b>
<b>2.1</b>	<b>MTP 1: Improving resilience in European eCommunication networks</b>	<b>6</b>
2.1.1	WPK 1.1: Good practices of regulatory and policy issues	8
2.1.2	WPK 1.2: Gap analysis of measures deployed by operators and good practice guidelines	10
2.1.3	WPK 1.3: Investigation of innovative actions	12
<b>2.2</b>	<b>MTP 2: Developing and maintaining co-operation models</b>	<b>14</b>
2.2.1	WPK 2.1: Co-operation platform for Awareness Raising Community	15
2.2.2	WPK 2.2: Security competence circle and good practice sharing for CERT communities	17
2.2.3	WPK 2.3: European NIS good practice Brokerage	19
2.2.4	WPK 4.1: Building information confidence in the area of micro enterprises through capacity building and enhanced co-operation with multipliers	21
<b>2.3</b>	<b>MTP 3: Identifying emerging risks for creating trust and confidence</b>	<b>23</b>
2.3.1	WPK 3.1: Framework for assessing and discussing emerging risks – Analysis of specific scenarios	25
2.3.2	WPK 3.2: Framework for assessing and discussing emerging risks – Documentation & maintenance	27
<b>3</b>	<b>HORIZONTAL ACTIVITIES</b>	<b>29</b>
3.1	Communicating and reaching out to ENISA stakeholders	29
3.2	Managing ENISA bodies and groups	29
3.3	Managing relations with external stakeholders	29
3.4	Managing internal capabilities	29
3.5	Managing ENISA internal communication	30
3.6	Work Programme development	30
<b>4</b>	<b>PROVIDING ADVICE AND ASSISTANCE</b>	<b>32</b>
<b>5</b>	<b>ADMINISTRATION ACTIVITIES</b>	<b>33</b>
5.1	General Administration	33
5.2	Finance	34
5.3	Human Resources	35
5.4	ICT	36
5.5	Legal and Procurement	37
<b>6</b>	<b>DIRECTORATE ACTIVITIES</b>	<b>39</b>
6.1	Accounting	39
6.2	Internal control co-ordination	39

# 1 INTRODUCTION

This Work Programme defines and describes the Multi-annual Thematic Programmes (MTPs), horizontal activities, provision of advice and assistance and administrative activities of the European Network and Information Security Agency (hereafter also referred to as the Agency). As such the Work Programme provides the main tasks and the budget for 2009 activities of the Agency. In case no budget is allocated to a particular activity, the activity is carried out by the Agency's experts only.

## 1.1 Policy context

The Commission Communication "i2010 – A European Information Society for growth and employment"<sup>1</sup>, highlighted the importance of network and information security for the creation of a single European information space. The availability, reliability and security of networks and information systems are increasingly central to our economies and society.

More and more Europeans live in an information-centred society where the use of ICTs has rapidly accelerated as essential tools in human social and economic interaction. Reliable communications networks and services are now critical to public welfare, economic stability and other critical sectors are exposed.

The Communication "A strategy for a Secure Information Society"<sup>2</sup> recognises that a secure Information Society must be based on enhanced Network Information Security (NIS) and a widespread culture of security. This can only be achieved through a dynamic and integrated approach that involves all stakeholders and is based on dialogue, partnership and empowerment. The Agency underpins that NIS is pivotal to establishing trust and confidence in using eCommunication networks and services.

Network and information security is a challenge for everybody:

**Public administrations** need to make informed policy decisions and to address the security of their own systems, not just to protect public sector information, but also to serve as an example of best practice for other players.

**Enterprises** increasingly see NIS as a critical element in their success or failure, but also as an element of competitive advantage rather than as a "negative cost".

**Individual users** suffer real economic and emotional damage, for example as a result of poor NIS practices and are critical elements in the epidemiology of Malware and extortion through Botnets.

A recent Council resolution<sup>3</sup> recognises that "the establishment of ENISA has been a major step forward in the EU's efforts to respond to the challenges relating to network and information security" and calls the Agency to support the strategy of the European Commission within its mandate as it is set out in the founding Regulation of the Agency.

ENISA fully recognises the importance of its role and supports the strategy of the European Commission. In an effort to maximise the impact of its activities, the Agency will leverage existing synergies and initiatives at national and European level and will follow a more focused and impact oriented approach.

---

<sup>1</sup> COM(2005) 229, 01.06.2005

<sup>2</sup> COM(2006) 251, 31.05.2006

<sup>3</sup> 15768, 01.12.2006

## 1.2 Key challenges

New services, such as Social Networking and VoIP heavily depend on complex, interdependent networks. The availability, scalability and reliability of such services dramatically decrease with the complexity of networks. As interdependencies increase, a disruption in one infrastructure can easily propagate into other infrastructures and have a European-wide domino-effect and impact. Global interconnectivity implies disappearance of national-network boundaries.

The increasing deployment of mobile devices and mobile-based network services poses new challenges. These could eventually prove to be a more common route for attacks than personal computers due to increased complexity and interoperability to more open networks.

The liberalisation of the telecommunications markets has increased competitive pressures on service providers and led them towards more cost-effective infrastructure investments with a direct impact on the quality of software and hardware components. This sometimes means that security of network components is not always given the highest priority throughout the entire product lifecycle (e.g., design, development, deployment, support).

Several service providers have outsourced the management of their network infrastructures without the appropriate quality and security measures being fully provided.

The interoperability between network operators, service providers, equipment suppliers, and networks operating across Member States' boundaries using immature technologies creates vulnerabilities and increases risks.

Attacks on information systems are increasingly motivated by profit, rather than by the desire to create disruption for its own sake. Data are illegally mined, increasingly without the user's knowledge. On the other hand, with the explosion of Web 2.0 technologies, and multiple interlinked data-sources, many people are unwittingly exposing highly sensitive personal information without appropriate privacy protection. Strong interoperable authentication mechanisms often come with a price tag, which makes users opt for less secure solutions for controlling access to data and services. Strengthening trust in the use of networks, software and services for governments, businesses and consumers remains a major task.

A breach in NIS can generate an impact that transcends the economic dimension. Indeed, there is a general concern that security problems may lead to user discouragement and lower take-up of ICT, whereas availability, reliability and security are a prerequisite for guaranteeing fundamental rights on-line.

## 1.3 ENISA's role

Addressing these challenges requires a systematic, coherent and integrated strategy that involves all concerned stakeholders and decision makers and is based on dialogue, partnership and empowerment.

ENISA, as an independent European-wide platform, is uniquely positioned to provide advice and assistance to Member States in enhancing their network and information security capabilities. The Agency has already performed valuable work in several important areas like awareness raising, risk assessment, CSIRTs and spam protection. Due to its independent position, the Agency can provide well-informed, objective advice and play a co-ordinating role within the EU to facilitate the exchange of good practices and information between all stakeholders at European level and thus maximize results and impact.

The Agency supports an open multi-stakeholder dialogue and, for that reason, maintains close relations with industry, the academic sector and users. It also sets and develops contacts with a network of national representatives (National Liaison Officers – NLO), and with major individual experts through ad-hoc Working Groups. Less formal but equally efficient interactions are in progress through virtual expert groups and platforms to gather and disseminate expert recommendations and to facilitate information exchange with and between public and private sector parties.

The capacity to provide prompt, independent and high quality responses to Requests received from EU Institutions and MSs' competent bodies gives the Agency a bridging role between EU and national institutions. This role is specific to ENISA and currently it is unique in the world.

A closer participation in the worldwide dialogue is also being developed through continuously expanding contacts with Third Countries as well as with international institutions (e.g., ITU, IETF, OASIS, OECD). The expected impact is a better integration of important foreign player views and a promotion of European approaches.

#### **1.4 New Work Programme approach and beyond**

Due to its mandate and limited resources, the Agency has been directed by the Management Board to focus its efforts on a realistic set of strategic priorities. By concentrating its efforts, the Agency aims to achieve increased impact in key areas and deliver on its promises. The Agency intends to leverage existing national and EU activities, and to avoid duplication of effort and maximize results. Examples of such European activities are the IST-FP6 Research for Critical Information Infrastructure Protection (CIIP), the Competitiveness and Innovation Programme (CIP), the ICT priority in the 7<sup>th</sup> Research Framework Programme and the IDABC programme. To work closely with these initiatives, capitalise on their results, interact with their constituencies and engage them in ENISA's work is one of the key elements of this Work Programme.

To achieve the desired impact and build on synergies, the Agency introduced a new Work Programme approach for 2008. One of the key objectives of this approach is to implement high-level goals provided by the ENISA Management Board<sup>4</sup>, while concentrating efforts on a limited set of strategic priorities, called Multi-annual Thematic Programmes (MTP). These programmes define the work of the Agency for the coming years. A set of SMART<sup>5</sup> goals are defined for each programme. These goals are related to the desired outcomes and impacts and can be assessed and monitored during the duration of the programme via Key Performance Indicators.

Each thematic programme consists of several Work Packages (WPK) that implement the SMART goals of the MTP. Each Work Package defines the tasks, the stakeholders concerned, the desired impact and the resources needed.

---

<sup>4</sup> These high-level goals are:

- Building confidence in the information society through increasing the level of NIS in the EU;
- Facilitating the Internal Market for eCommunication by assisting the institutions to decide the appropriate mix of regulation and other measures (noting in particular, the important contribution the Agency can make to the Framework Directive);
- Increasing the dialogue between the various stakeholders in the EU on NIS;
- Increasing co-operation between MS in order to reduce the difference in the capability of MS in this area;
- Assisting and responding to requests for assistance from the Member States.

<sup>5</sup> SMART is an acronym for Specific, Measurable, Agreed, Realistic and Time bound.

Work Packages may be multi-annual. However, since MTPs are implemented through the Agency's annual Work Programme, the indicated resources and budget could only refer to action, outcomes and operations of one year. The specified budget refers to external activities e.g. workshops, conferences or consultancy. The human resources refer to the effort put by the Agency's experts.

The Work Programme 2008 includes three MTPs and one Preparatory Action (PA). A PA is an activity that will last one year and will investigate under what conditions a new MTP could be initiated. A so-called go/no-go decision can only be taken once the results become available at the end of 2008. However, for the purpose of resource planning the Agency at this stage anticipates a follow-up for 2009 by proposing an MTP in the same area i.e., building information confidence with micro enterprises.

Hence, in 2009 the Agency will focus on three MTPs that are briefly described here. A full description of the MTPs, as well as the individual WPKs, is given in the next chapter. The WPKs proposed for 2009 include their own SMART goals and KPIs that are considered as a first step toward achieving the SMART goals of the MTP.

### **MTP 1: Improving resilience in European eCommunication networks**

In 2008, this MTP focused on stocktaking, best practices identification and analysis of gaps of measures deployed by both National Regulatory Authorities (NRAs) and network operators and service providers. MTP 1 also analysed the suitability of currently deployed backbone internet technologies regarding integrity and stability of network. In 2009, MTP 1 will compare the findings against similar international experiences and results, issue guidelines, and finally formulate consensus-based recommendations after broad consultation with concerned stakeholders. The recommendations will be widely promoted to the concerned policy and decision makers. This MTP will follow and support, as appropriate, the reviewing and updating of the EU Electronic Communication Directives.

### **MTP 2: Developing and maintaining co-operation between Member States**

In 2008 the MTP aimed at

- a) the identification of Europe-wide security competence circles on topics like Awareness Raising and Incident Response,
- b) the European NIS good practice Brokerage<sup>6</sup> and
- c) NIS capacity building for micro enterprises.

From 2009 to 2010, co-operation among Member States will be developed further with the aim to improve the capabilities of all Member States and increase the overall coherence and interoperability levels.

### **MTP 3: Identifying emerging risks for creating trust and confidence**

The Agency will establish a framework that will enable decision makers to better understand and assess emerging risks arising from new technologies and new applications. This will contribute to stakeholders' trust and confidence. To this end, the Agency developed a proof of concept in 2008 of a European capacity for the evaluation of risks that may emerge in 2 to 3 years ahead, linked to a Stakeholder Forum for multi-stakeholder dialogue with public and private sector decision makers. In 2009, this proof of concept will be tested and developed further. In addition, the Agency will continue preparing position papers to express the Agency's view on emerging risks arising from new technologies and new applications. As such, this MTP should provide an antenna function for decision makers in Europe and possibly beyond.

---

<sup>6</sup> This platform is a follow-up of the work conducted in 2007 to define a roadmap on the establishment of European NIS good practice Brokerage.

The table below provides an overview of the MTPs for 2009, including their SMART goals and respective KPIs.

MTP name	SMART goal	KPI
Improving resilience in European eCommunication networks	By 2010, the Commission and at least 50% of the Member States have made use of ENISA recommendations in their policy making process	Commission (yes/no) % of Member States
	By 2010, service providers covering at least 50 million users use ENISA recommendations to improve resilience	# users covered by service providers
Developing and maintaining co-operation models	By 2010, at least 10 Member States have participated in at least 3 different co-operation models.	# Member States involved # Co-operation models
Identifying emerging risks for creating trust and confidence	By 2010, at least 30 stakeholders or stakeholder organisations from at least 15 Member States refer to ENISA as a point of reference for discussing the nature and impact of emerging security challenges in the Information Society.	# stakeholders # Member States

In addition to the above, the Agency will continue performing a number of horizontal activities, such as communication and outreach, secretariat of ENISA bodies, relations with external stakeholders (EU Bodies, Member States, industry, academia, consumers, International Institutions and Third Countries), measuring the uptake of ENISA deliverables, the Agency's internal capabilities, internal communication and Work Programme development.

Also, the Agency will continue providing advice and assistance when called upon. Finally, the Agency's Administrative Department implements general administration, finance, human resources, ICT and legal and procurement. With regard to career development, the Agency has at its disposal a finite number of instruments that includes grading, promotions, trainings and career opportunities within the Agency.

## 2 MULTI-ANNUAL THEMATIC PROGRAMMES

### 2.1 MTP 1: Improving resilience in European eCommunication networks

#### THEME NAME:

**MTP 1: Improving resilience in European eCommunication Networks**

#### DESCRIPTION OF THE PROBLEM TO SOLVE:

Availability, integrity and continuity of public communication networks is of major importance in a converging (connected or integrated) environment of fixed, mobile in particular in the context of all IP infrastructures.

At the same time, a totally interconnected and networked everyday life promises significant opportunities while also creating additional security and privacy-related risks. As interdependencies become complex, a disruption in one infrastructure can easily propagate into other infrastructures and have a European-wide impact.

The international nature of telecommunication business requires a common approach to deal with issues like resilience of networks. Several Member States have already developed or are in the process of developing strategies, policies and regulatory initiatives to cope with the problem. Most of these strategies are based on co-operation with providers, sharing of information on incidents and threats and development of good practices. Despite these efforts, the situation across Europe as regards the obligations and requirements to ensure and enhance the security and resilience of such networks is highly fragmented. The smooth functioning of the Internal Market and the demand of global players call for common requirements, rules and practices across the EU.

#### DESCRIPTION OF THE APPROACH TAKEN SOLVING THE PROBLEM:

The goal of this MTP is to "collectively evaluate and improve security and resilience in mobile and fixed public eCommunications networks and Services in Europe", in short: "Improve Resilience in European eCommunications Networks and Services".

In 2008 ENISA performed a series of stocktakings. More precisely, the Agency analysed the regulatory and policy environments, assessed how providers ensure availability and integrity of networks and services, and evaluated whether existing technologies and standards satisfy the needs and requirements of eCommunications network providers.

In 2009 ENISA will continue its efforts in this direction by performing:

- 1) Analysis of Gaps – ENISA, based on the findings of the stock analysis, will analyse gaps in the policy and regulatory environment, in the measures and practices deployed by providers and in technologies and standards currently in use by them. The gap analysis will take under consideration trends, best practices and recommendations proposed by other organisations or constituencies in Europe or elsewhere.
- 2) Development of good practices and guidelines – as a result of the stocktaking and gap analysis, ENISA will develop in co-operation with stakeholders through workshops, working groups of experts and online consultations good practices and guidelines to bridge the identified gaps. The Agency will consult with all relevant stakeholders with the aim to propose affordable and realistic good practices.

Such holistic approach will be implemented through three (3) Work Packages (WPK), namely:

- WPK 1.1 – Gap Analysis and Good practices on policy and regulatory measures
- WPK 1.2 – Gap analysis and Guidelines on providers' measures
- WPK 1.3 – Investigation of innovative actions

In 2010 ENISA intends to validate the proposed good practices in real working environments through a series of pilots. Additionally, the Agency will promote its findings to national and EU policy and decision makers, regulators, pan-European and international constituencies, standardisation bodies and targeted stakeholders. Finally, the Agency intends to further extend its scope going beyond the availability of networking infrastructure by concentrating its efforts on the availability of services.

#### **DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals)**

**SMART goal:** By 2010, the Commission and at least 50% of the Member States have made use of ENISA recommendations in their policy making process

**KPIs:** Commission (yes/no), % of Member States

**SMART goal:** By 2010, service providers covering at least 50 million users use ENISA recommendations to improve resilience

**KPI:** # users covered by service providers

#### **WHICH HIGH-LEVEL GOALS THE PROGRAMME SUPPORTS:**

- Building confidence in the information society through increasing the level of NIS in the EU
- Facilitating the Internal Market for eCommunication by assisting the institutions to decide the appropriate mix of regulation and other measures (noting in particular, the important contribution the Agency can make to the Framework Directive).
- Increasing the dialogue between the various stakeholders in the EU on NIS
- Increasing co-operation between MS in order to reduce the difference in the capability of MS in this area

#### **STAKEHOLDERS AND BENEFICIARIES**

National Regulatory Authorities, Member States' Governments and EU Policy and Decision Makers, Public eCommunications networks and services providers (fixed, mobile and IP-based), Internet Service Providers (ISPs), Associations of Providers (ECTA, ETNO, GSM Europe), Internet Exchange (Euro IXs), Audit Associations (ISACA), Suppliers of Network Components, Systems and Software (EICTA)

#### **WHY ENISA?**

ENISA is well positioned to help stimulate a European presence to ensure and enhance the security and resilience of public communications network.

Massive cyber-attacks can only be effectively dealt with on a multilateral basis. They require integration of legislation, planning, organizations, infrastructure, and technical efforts. By its designation, ENISA is well-positioned to promote and facilitate European Union joint policies, activities, and procedures in this area.

#### **PROGRAMME PROPOSED BY:**

ENISA, Management Board, Permanent Stakeholders' Group

#### **LEGAL BASE**

ENISA Regulation, articles 3a), c), d), f), i) and k)

## WPK 2.1.1: Good practices of regulatory and policy issues

### MTP Name

Improving resilience in European eCommunication networks

### WORK PACKAGE NAME:

WPK 1.1: Good practices of regulatory and policy issues

### DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

**SMART goal:** in depth analysis of each topic covers at least 50% of Member States

**KPI:** # Member States

**SMART goal:** at least 50% of Member States participate in the open consultation process for each good practice

**KPI:** # Member States

**SMART goal:** at least 3 Member States express interest in piloting good practices for each area

**KPI:** # Member States

### DESCRIPTION OF TASKS:

In 2008 ENISA performed a pan-European stocktaking of the regulatory and policy environment related to the resilience of public eCommunications networks. The stocktaking identified relevant authorities in Member States and analysed their tasks and policy and regulatory initiatives. The analysis revealed significant differences in Member States' policy and regulatory strategies, measures and activities.

ENISA will organise at the end of 2008 a workshop to present the findings of its stocktaking to relevant stakeholders. The Agency together with stakeholders will assess the identified gaps, prioritise them and select three promising areas that require further in depth analysis at pan-European level. Possible topics for further analysis include co-operation models (e.g. public private partnerships on improving redundancy, development of guidelines on security policy plans), national preparedness and recovery measures (e.g. restoring priority communications, national roaming), reporting and analysis of incidents through information exchanges (e.g. security breaches, network failures, service interruptions), monitoring and auditing mechanisms, development of best practices and incentives for their deployment, and guidelines affecting the procurement of public eCommunications networks.

For each selected topic, ENISA will initially organise a thematic workshop to consult with relevant public and industry stakeholders on the concrete aspects to be analysed. The Agency will then form a group of experts, organise thematic discussions with identified experts using electronic means, perform targeted interviews of stakeholders, and assess similar cases of non-EU countries (e.g. OECD countries). The collected input from experts and the analysis done on similar cases will result in realistic and affordable good practices for each area.

The three proposed good practices will be put for open consultation with relevant stakeholders. During the consultation period ENISA will organise a workshop inviting all relevant stakeholders to debate about the proposed good practices. Synergies will be sought, whenever relevant and feasible, by organising joint workshops as with those indicated in other work packages of MTP 1. Stakeholders' suggestions and proposed improvements could significantly enhance the appropriateness, affordability and acceptance of the proposed good practices. Possible stakeholders, in addition to the relevant national and European public authorities, include European policy and regulatory groups (e.g. IRG WG on security), sector associations (e.g. ETNO, EUROISPA, EICTA, GSM Europe, ISACA, Euro-IXs), and trans-border providers (e.g. Telcos and large ISP).

In 2010 ENISA intends to validate the proposed good practices in real working environments. The Agency intends to select a limited number of relevant stakeholders and perform for each area a pilot assessing the usability, effectiveness and affordability of its recommendations. The experience from the pilot phases will be taken under consideration in refining the good practices.

#### **OUTCOMES AND DEADLINES:**

- Three Thematic Workshops (Q2-Q3 2009)
- Consultation Workshop with Stakeholders (Q4 2009)
- Good Practices for three identified areas (Q4 2009)

#### **STAKEHOLDERS**

NRAs, national policy authorities dealing with resilience of public communication networks and services, sector associations (EICTA, ETNO, EUROISPA, GSM Europe, ISACA, Euro-IX), telecom operators (fixed, mobile and IP-based), Internet Service Providers (ISPs)

#### **RESOURCES FOR 2009 (person months and budget)**

- €200.000 (organisation of 3 thematic workshops and one consultation workshop, consultancy for development of the good practices of the three selected thematic areas)
- 15 person months

#### **WORK PACKAGE PROPOSED BY:**

ENISA

#### **LEGAL BASE**

ENISA Regulation, articles 3a), c), d), and k)

## 2.1.2 WPK 1.2: Gap analysis of measures deployed by operators and good practice guidelines

### MTP Name

Improving resilience in European eCommunication networks

### WORK PACKAGE NAME:

WPK1.2: Gap analysis of measures deployed by operators and good practice guidelines

### DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

**SMART goal:** The gap analysis covers at least 50% of Member States.

**KPI:** # Member States

**SMART goal:** At least 50% of Member States participate in the open consultation process.

**KPI:** # Member States

### DESCRIPTION OF TASKS:

In 2008, ENISA conducted a stocktaking to assess technical and organisational measures implemented by operators to enhance resilience of public eCommunications networks. The topics addressed by the stocktaking were physical security, continuity of services, emergency preparedness, co-operation among operators and risk management. They are based on the ARECI recommendations. The stocktaking covered operators from different Member States having a wide range of activities and sizes.

The stocktaking revealed gaps in the measures operators deploy to enhance resilience of their networks. In 2009 ENISA will analyse these gaps and identify measures and appropriate implementation strategies that could potentially fill these gaps. To achieve this, ENISA will analyse existing practices (e.g. use of standards, of recommendations, of good practices, etc.) and organise a workshop inviting all relevant stakeholders to debate about possible measures that could be used to improve the situation (see list below).

The input received by the experts and stakeholders in conjunction with the internal analysis will contribute to the drafting of the proposed Guidelines that address the identified gaps. The Guidelines will be communicated to the relevant stakeholders (e.g. operators, operators' associations, internet exchange points, Commission, standardisation bodies, etc.) and through an open consultation process will be further improved. Synergies will be sought, whenever relevant and feasible, by organising joint workshops as with those indicated in other work packages of MTP 1. The produced guidelines will help operators and other relevant stakeholders in implementing resilience measures but will also contribute to the identification of topics that are worth further in depth analysis.

During the above mentioned ENISA activities, identified issues will be presented to relevant stakeholders (e.g. via workshops, virtual groups etc.) to get feedback from relevant constituencies. This will allow the active involvement of relevant stakeholders during the generation of ENISA's guidelines.

### OUTCOMES AND DEADLINES:

- Draft Guidelines (Q3 2009)
- Consultation Workshop on ENISA's Guidelines (Q4 2009)
- Final Guidelines (Q4 2009)

### **STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE**

ISPs, Internet Exchange Points, cc-TLDs Outsourced Service Providers, Telecom operators (fixed, mobile and IP-based), Associations of ISPs, Internet suppliers of systems, components and services.

### **RESOURCES FOR 2009 (person months and budget)**

- €100.000 (consultancy, publication/printing and workshop)
- 16.5 person months

### **WORK PACKAGE PROPOSED BY:**

ENISA

### **LEGAL BASE**

ENISA Regulation, articles 3a), c), d), f), and k)

### 2.1.3 WPK 1.3: Investigation of innovative actions

#### MTP Name

Improving resilience in European eCommunication networks

#### WORK PACKAGE NAME:

WPK 1.3: Investigation of innovative actions

#### DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

**SMART goal:** ENISA's recommendations of innovative actions are applied in at least ten (10) Member States by 2010.

**KPI:** # Member States.

**SMART goal:** To make contributions to at least one research priority for the next revision of the ICT WP of the FP7 of EU funded R&D.

**KPI:** # Number of contributions on research priorities made.

#### DESCRIPTION OF THE WORK PACKAGE

In 2008, ENISA has analysed a number of technologies, protocols and architectures. These findings have been reported in the deliverable "Analysis of existing resilient technologies".

In 2009, ENISA will continue investigating possible ways for enhancing the resilience of public eCommunication networks, not limiting itself to technologies, architectures and protocols such as IPv6, MPLS, DNSSec). In this context, incentives (on market and/or policy related aspects will also be considered with a view on their impact on business practices and identifying incentives and/or developing recommendations mainly addressed to EU and national policy makers.

The result of these investigations will lead to the definition of guidelines about innovative actions to enhance the resilience of public eCommunication networks. The guidelines will be subject to a wider consultation with relevant stakeholders, as well as relevant WPKs of MTP 1 (namely WPK 1.1. and 1.2), in an effort to build consensus and develop concrete recommendations by the second quarter of 2010. ENISA intends to widely promote such recommendations in an effort to support the fastest take-up of most promising innovative actions.

At the same time, this activity will be combined with a pilot action entitled "Open Doors to Technologies Enhancing Network Resilience" comprising of a workshop dedicated to the work carried out in the context of WPK 1.3. The aim of this pilot action is to provide to Scientific Officers of the European Commission (DG INFSO, JLS, MARKET and Research) an insight on the subject of communication networks resilience and the activities of ENISA in this area. This activity could be perceived as the first step in preparing a training scheme covering all aspects of MTP 1. Such a training scheme, in the future could be held at regular intervals at the premises of ENISA and be offered in the long term to representatives of policy making bodies and NRAs of EU Member States.

During 2009 the Agency will also assess the impact of the evolution of networking technologies in terms of security and e-resilience. In this context, some technological and networking trends such as edge networking, machine-to-machine communications, RFID, Personal and Body Area Networks (PAN, BAN), P2P, adhoc networking, femtocells, etc. will be assessed including their impact in terms of security and availability of networking resources. The results of this activity are expected in the form of contributions to the preparation of the Framework Programs of EU funded R&D through the identification of research priorities in the areas of networking resilience as well as network and information security.

The technical approach described in the context of WPK 1.3 for 2009, is fully in line with the 6<sup>th</sup> recommendation made in the context of the study on the "Availability and robustness of electronic communication networks. The ARECI Study" (Final Report, March 2007).

#### **OUTCOMES AND DEADLINES:**

- Report on innovative actions investigated (Q2 2009).
- Workshop with the aim to prepare Guidelines and recommendations about innovative actions to enhance eResilience (Q2 2009).
- Guidelines for policy makers and MS NRAs about innovative actions that enhance the resilience of public communication networks (Q4 2009).
- "Open Doors to Technologies Enhancing Network Resilience" workshop (Q2 2009).
- Workshop on identifying the latest networking trends and their impact in terms of networking resilience as well as network and information security (Q3 2009).
- Report on research priorities in the areas of networking and information security (Q4 2009).

#### **STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE**

Networking equipment vendors, National Regulatory Agencies (NRAs), Network operators, Virtual network operators, Experts in resilient backbone and internet technologies, Industrial R&D institutions, Universities and Research centres, European Technology Platforms (e.g. eMobility, NEM, NESSI, etc.).

#### **RESOURCES FOR 2009 (person months and budget)**

- €150.000 (workshops, consultancies, electronic and printed publications).
- 14 person months

#### **WORK PACKAGE PROPOSED BY:**

ENISA

#### **LEGAL BASE**

ENISA Regulation, articles 3a), b), c), f), and k)

## 2.2 MTP 2: Developing and maintaining co-operation models

### THEME NAME:

MTP 2: Developing and maintaining co-operation models

### DESCRIPTION OF THE PROBLEM TO SOLVE:

Many Member States have the need to increase their capabilities in various fields of network and information security (NIS). Several Member States already co-operate by sharing information on best practices, but this does not happen on a structural basis. This implies missed opportunities to create synergies and improve efficiency and effectiveness at European level.

### DESCRIPTION OF THE APPROACH TAKEN SOLVING THE PROBLEM:

With this horizontal MTP, ENISA will address these needs by fostering its role as facilitator, centre of expertise and advice broker. ENISA will develop various co-operation models in pre-defined areas (awareness raising, incident response and NIS capacity building for micro enterprises), while building on previous work. In addition, the Agency will further develop the European NIS Good Practice Brokerage, including supporting tools such as the Online platform to support the dialogue, Who-is-Who Directory, Country Pages and Country Reports of the activities in the Member States. A highlight will be the various thematic workshops that will foster the relation to existing NIS communities (e.g., CERTs) or build up new communities that share common interests in specific NIS topics (e.g., Awareness Raising). The Agency will leverage on its existing contacts and networks, including the National Liaison Officers network and identified National Competent Bodies.

### DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals)

**SMART goal:** By 2010, at least 10 Member States have participated in at least 3 different co-operation models.

**KPIs:** # Member States involved, # Co-operation models

### WHICH HIGH-LEVEL GOALS THE PROGRAMME SUPPORTS:

- Building confidence in the information age by increasing the capabilities of the MS in the field of NIS.
- Increasing co-operation between MS in order to reduce the difference in the capability of MS in this area.
- Increasing the dialogue between the various stakeholders in Europe on NIS.

### STAKEHOLDERS AND BENEFICIARIES

MS governments (and NRAs); Commission; industry; academia; other stakeholder groups.

### WHY ENISA?

ENISA is uniquely positioned to provide advice and assistance to MS and the Commission in enhancing their network and information security capabilities. ENISA provides an independent European-wide platform to facilitate co-operation between Member States, acting as trusted third party. ENISA has already performed valuable work in awareness raising, CSIRTs, feasibility study on an EU-wide information sharing and alert system, brokering between Member States and micro enterprises.

### PROGRAMME PROPOSED BY:

ENISA, Management Board, Permanent Stakeholders' Group

### LEGAL BASE

ENISA Regulation, articles 3c), d), and e)

## 2.2.1 WPK 2.1: Co-operation platform for Awareness Raising Community

### MTP Name

Developing and maintaining co-operation models

### WORK PACKAGE NAME:

WPK2.1: Co-operation platform for Awareness Raising (AR) Community

### DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

**SMART goal:** By 4Q 2009, have all EU Member States represented in the AR Community with at least 1 representative from the following sectors: industry, academia and government.

**KPIs:** # EU Member States represented; # experts signed up through AR portal and receiving the welcome pack

**SMART goal:** By 2009, have 50 downloads of good practice material shared within the AR Community from the AR portal, 1.500 visits per month to the AR portal and 10 explicit requests for not-downloadable deliverables

**KPIs:** # downloads, # AR portal visits per month, # requests for deliverables

**SMART goal:** By Q2 2009, organise a conference with at least 80 participants from 10 different EU Member States.

**KPIs:** # participants, # EU Member States represented

### DESCRIPTION OF THE WORK PACKAGE

This work package intends to enhance the co-operation platform for the awareness raising Community and offer a perspective on what public institutions and private companies could do to enhance information security awareness. To this end, three main components have been identified as enabler to achieve these goals: AR Community, AR portal and AR Conference.

#### AR Community

ENISA will continue to identify information security AR experts throughout Europe willing to participate in the ENISA AR Community. This task will be carried out building up to the present AR Community trying to have all EU Member States represented with at least one representative from the following sectors: industry, academia and government. The Agency will facilitate discussions, exchange of good practices and knowledge sharing by different means of communications during which cutting-edge topics, key issues and emerging awareness good practices will be discussed and presented. The members of the AR Community will be requested to engage with ENISA in its mission to foster a culture of information security. Members will be a point of contact for matters related to information security awareness in general or related to their countries, industries, or areas of activity. Topics and target groups will be identified as a result of surveys, discussions, and interaction with the AR Community. They will also contribute e.g., by participating in discussions and drafting White Papers on specific security topics and target groups, taking part to virtual working groups building up to the present work. Relevant material will be made available on the AR Community portal (e.g., reports, training material and factsheets).

#### AR portal

The AR portal consists of a number of web pages dedicated to the awareness raising field. Part of them follows in a protected area dedicated to the AR Community members only, such as monthly conference calls material, *ARNews* etc. Relevant material (including excerpts of ENISA reports) will be made available both on the public and protected areas of the AR portal. This activity builds on the similar activity the Agency carried out in 2008. Further technical features could be made available on the AR portal, both public and protected areas (e.g. mailing lists; discussion forum; event calendar etc.). In order to enhance better information security awareness the main pages of the portal may be translated in different languages, such as FR and DE.

### **AR Conference**

In 2Q 2009, ENISA will organise a conference where the AR Community members will meet up to discuss and share experience and good practices. Topics will be selected on the basis of the ENISA and AR Community 2008-2009 findings in the field of information security awareness.

### **OUTCOMES AND DEADLINES:**

- Internal contact list of awareness raising experts part of the ENISA AR Community (ongoing task; 4Q 2009)
- Enhanced AR portal on the ENISA web site (2Q 2008)
- Translation of the public area of the AR portal in 2 languages: FR and DE (1Q 2009)
- Publication of good practices material shared within the AR Community (3Q 2009)
- AR conference aimed at reporting on good practices material and recommendations to enhance co-operation among Member States (2Q 2009)

### **STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE**

Member States, PSG

### **RESOURCES FOR 2009 (person months and budget)**

- €50.000 (AR Conference and printing of ENISA findings)
- 14 person months

### **WORK PACKAGE PROPOSED BY:**

ENISA

### **LEGAL BASE**

ENISA Regulation, articles 3c), d) and e)

## 2.2.2. WPK 2.2: Security competence circle and good practice sharing for CERT communities

### MTP Name

Developing and maintaining co-operation models

### WORK PACKAGE NAME:

WPK 2.2: Security competence circle and good practice sharing for CERT communities

### DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

**SMART goal:** By Q4 2009, at least 3 presentations given about ENISA's work in the CERT field at the CERT/CSIRT community events.

**KPI:** # of presentations

**SMART goal:** By Q4 2009, 80% of updates in CERT inventory are confirmed

**KPI:** % confirmed updates

**SMART goal:** By Q4 at least two TRANSITS trainings have been organised with support by ENISA<sup>7</sup>

**KPI:** # of trainings supported

**SMART goal:** By Q4 2009, at least 50 downloads of ENISA CSIRT good practice collection materials that have been produced or updated in 2009

**KPI:** # of downloads

**SMART goal:** "ENISA CSIRT exercise collection" piloted at least between 2 CSIRT teams

**KPI:** # of exercise pilots

### DESCRIPTION OF TASKS:

CERTs community in Europe has been growing and co-operating in Europe for more than a decade. However, there are still gaps of various kinds in the CERT landscape that ENISA can and should address. Those gaps have been identified by previous works of ENISA like the "gap analysis" by the CERT ad-hoc working group, the "ENISA Inventory of CERT activities in Europe" and the study about "CERT co-operation and its further facilitation by relevant stakeholders". ENISA will furthermore continue to strengthen its position as independent and experienced contact for the various European and International CERT communities like TF-CSIRT and FIRST. This will be accomplished by presenting ENISA's work in events organised by these communities, and enable the communities to influence the Agency's work by giving feedback.

### Continue facilitation of the setting up of CERTs/CSIRTs and stay in close relation to the various CERT/CSIRT communities

The number of EU Member States with their own governmental/national CERTs is growing (among other things, due to the changing threat environment and continuous facilitation by ENISA), but the coverage can still be improved. ENISA has developed and will continue to develop tools (such as CSIRT setting-up and running guides, co-operation guide and CSIRT exercise collection) for strengthening the CERT community and their co-operation and focuses on helping to set-up new governmental/national CERTs in the Member States. To this end the support of the very successful TRANSITS trainings for CSIRT staff members taking place at least twice a year in Europe will be continued. MS requests for special CERT staff trainings may be accommodated, as it has been done in the past, to close the gaps of CERT services in Europe, especially in Government/National CERT coverage. The ENISA CERT Inventory will be updated to reflect the developments in the European landscape accordingly.

<sup>7</sup> Provided that the organiser of the previous regular TRANSITS courses continues this effort.

### **Prepare CERT good practice collection: the role of national/governmental CSIRTs**

ENISA's role as good practice knowledgebase and contact broker is supported by the high quality material ENISA already has prepared in the past (like the "Step-by-step guide on how to set up a CSIRT", available in various languages). ENISA will continue enhancing its library of CERT good practice guides. Following the consultation process with CERTs in the Member States, which started with the findings of the 4<sup>th</sup> CERT workshop *CERTs in Europe* (May 2008 in Athens) the good practice collection for 2009 will cover the special role that national and/or governmental CSIRTs play in their countries' national incident response capability. ENISA will start with identifying best practice and formulate guidance regarding minimal (baseline) services and functions for national/governmental CERTs in co-operation with the relevant stakeholders.

### **CERT Exercises: the next step to achieve impact**

Exercises help CERTs to prepare their response in the case of security incidents, in all aspects of their operation. In 2008, ENISA together with the CERT communities, produced a CSIRT Exercise Book, together with working material that should enable a CERT to train situations where the team might be confronted with new, unknown events. Less critical situations like the incorporation of a new team member or highly critical events like massive cyber attacks against the infrastructure of their clients can be better coped with by the teams if they are trained to show the appropriate reaction.

In 2009 ENISA will facilitate a pilot using this "CSIRT exercises collection" deliverable from 2008. This aims to promote the usage of the collection and to demonstrate real-life applicability. At least two exercises shall be facilitated by ENISA based on the CSIRT Exercise Book. The exercises shall be monitored and the outcome shall be compiled into a report that can potentially be included in the NIS Brokerage document section. The Agency plans organising in the course of 2010 a workshop for members of CERT/CSIRT communities to discuss results of exercises.

### **OUTCOMES AND DEADLINES:**

- Updated "ENISA Inventory of CERTs in Europe" in Q2 and Q4 2009
- First version of the ENISA CSIRT good practice collection in Q4 2009
- CSIRT exercises collection pilot between at least 2 CSIRT teams and a resulting report in Q3/Q4
- At least 2 TRANSITS courses supported by Q4
- Workshop for members of CERT/CSIRT communities to discuss exercise results planned for 2010 Q2

### **STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE**

EU Member States (in particular national CSIRTs), CERT community

### **RESOURCES FOR 2009 (person months and budget)**

- €95.000 (meetings, consultancy, facilitation of exercise, support of TRANSITS courses)
- 15 person months

### **WORK PACKAGE PROPOSED BY:**

ENISA

### **LEGAL BASE**

ENISA Regulation, articles 3c), d), and e)

## 2.2.3 WPK 2.3: European NIS good practice Brokerage

### MTP

Developing and maintaining co-operation models

### WORK PACKAGE NAME:

WPK 2.3: European NIS good practice Brokerage

### DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

**SMART goal:** By Q4 2009, at least 4 Member States are engaged in at least 2 new co-operations, facilitated through the European NIS good practice Brokerage.

**KPI:** # Member States, # co-operations

**SMART goal:** By Q4 2009, the Online Platform is visited by all Member States

**KPI:** # Member States stating to have visited the Online Platform

**SMART goal:** By Q4 2009, all Member States are covered by the Who-is-Who Directory

**KPI:** # Member States

**SMART goal:** By Q4 2009, all updates in Who-is-Who Directory are confirmed

**KPI:** % confirmed updates

**SMART goal:** By Q4 2009, the Country Reports will be updated for all the Member States and they will contain at least 1 thematic section on a specific NIS related topic.

**KPI:** # Member States, # thematic sections

### DESCRIPTION OF TASKS:

On several occasions Member States expressed their desire to improve their co-operation, in particular at governmental level. Some Member States already work together exchanging experiences in order to develop and improve their NIS capabilities, but the number of co-operations, the number of Member States involved and the level of co-operation can be increased. To enhance the level of NIS on a European scale, all Member States shall be encouraged to share information on good practices in NIS in a structured way.

ENISA started to facilitate a European 'NIS Market Place' in 2007, and in 2008 several Member States engaged in co-operation initiatives facilitated through the European NIS good practice Brokerage. ENISA intends to continue facilitating **co-operations** by performing its role of broker between those Member States that have developed good practices in specific NIS areas and are equally willing to share them and those Member States that want to learn about particular experiences and are willing to articulate their needs. Where appropriate, ENISA expertise as well as other stakeholders' expertise will be injected into the co-operations.

For instance, in 2007 and 2008, ENISA facilitated the co-operation between Hungary and Bulgaria in the field of governmental CERT. Hungary had expertise in setting up a Gov-CERT (expertise gathered from previous co-operation with Germany) and was willing to offer its expertise to Bulgaria. ENISA had knowledge and material on how to establish a CERT. Bulgaria requested ENISA support to transfer Agency expertise and Hungarian hands-on experience in setting up a Gov-CERT. Agreement was reached to organise a training that saw the involvement of Bulgarian, Hungarian, supported by ENISA representatives. The training was organised by CERT-Hungary and ENISA according to Bulgaria's needs.

ENISA considers this as a long term and continuous task as Member States have to be pointed to various possibilities of co-operation and have to be convinced that co-operation will be fruitful and beneficial for all partners involved.

In the context of the European NIS good practice Brokerage, co-operations will be facilitated, for instance, in the field CERTs policies, awareness raising, resilience, risk management or other NIS-related areas.

The European NIS good practice Brokerage will be supported by a set of tools:

- **The Online Platform** will be a tool directly linked to this widespread activity. The platform provides general information about various co-operation models, the activities that have been carried out ('success stories'), and a source for information/guidance in order to find the right partners. Thus, the platform may serve Member States to feel encouraged to co-operate. The Online Platform will be kept constantly updated with the aim to expand it with key data.
- **The Who-is-Who Directory** is a compilation of generic addresses of relevant actors in NIS. The directory will be kept constantly updated with the aim to expand it with key data and new sections.
- **The Country Reports** are an assessment of the ongoing and planned activities of NIS in Member States. They also include comprehensive information about relevant actors and their mutual relations. The Country Reports provide information about activities in relation to ENISA. The Country Reports compiled in 2008 will be updated in 2009. In 2009, each Country Report will also contain at least one thematic section that will provide more detailed information on a specific NIS related topic, such as, for instance, resilience of eCommunication, CERTs, or other NIS related topic. The topic of this thematic section will be selected also by taking into account specific studies and/or activities carried out by ENISA.

An annual review will be conducted in order to obtain feedback on the functioning of the European NIS good practice Brokerage. At the end of each year, the result of this review will be presented in an **Annual Evaluation Report on the functioning of the European NIS good practice Brokerage**. This Annual Evaluation Report will focus on co-operations and NIS good practice supporting tools (on-line platform, Who-is-Who Directory, and Country Reports).

#### OUTCOMES AND DEADLINES

- Co-operations (ongoing)
- Online Platform (ongoing)
- Online and printed versions of the Who-is-Who directory (Q4 2009)
- Online updated Country Reports (Q4 2009)
- Annual Evaluation Report on the functioning of European NIS good practice Brokerage (Q4 2009)

#### STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

Member States: Management Board, National Liaison Officers; Networks of the various 'topical communities' (i.e., in industry, academia and consumers, risk assessment etc.)

#### RESOURCES FOR 2009 (person months and budget)

- €115.000 (meetings, consultancy, printing costs)
- 15 person months

#### WORK PACKAGE PROPOSED BY:

ENISA

#### LEGAL BASE

ENISA Regulation, articles 3c) and d)

## 2.2.4 WPK 2.4: Building information confidence in the area of micro enterprises through capacity building and enhanced co-operation with multipliers

### MTP NAME

Developing and maintaining co-operation models

### WORK PACKAGE NAME:

WPK 2.4: Building information confidence in the area of micro enterprises through capacity building and enhanced co-operation with multipliers

### DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

**SMART goal:** By end of 2009, at least 3 multiplier organisations from at least 3 different Member States have been trained to use the customised ENISA security toolkit to build information confidence with micro enterprises.

**KPIs:** # multiplier organisations, # Member States

### DESCRIPTION OF TASKS:

The digital information age continues to provide many opportunities for businesses, especially for micro enterprises. However, the further development and user adoption of ICT still comes with vulnerabilities. In fact, micro enterprises have been identified as one of the weakest links in information security despite the increasing demand for their services as a supplier and sub-contractor in value chains of larger companies. Thus small and micro enterprises may find themselves losing business opportunities. Being the backbone of economy and chief provider of jobs in many EU Member States, this may create severe damage to the innovativeness and competitiveness of European economy. Therefore, changing information security behaviour of micro enterprises must be one of the main objectives of information security policy. Several Member States have already implemented programmes aimed at changing information security behaviour of micro enterprises. However, others still have a need for knowledge, information and support in the field.

During the year 2008 ENISA organised an Ad Hoc Working Group analysing micro enterprises' and their multipliers' needs and expectations in the area of information security. The Working Group implemented validation of the PA 2008 rationale which resulted in confirmation of the fact that associations and Member States are increasingly interested to foster a culture of NIS amongst micro enterprises. However, co-ordinated exchange of information and good practice is lacking. ENISA is well positioned to provide an incentive to establish a platform bringing together relevant organisations from different Member States with the aim to increase knowledge and information on how to build capacity among their constituency and thus support the establishment of concrete peer-to-peer learning practices in the area. To this end, the following steps are considered:

- 1 Call for expression of interest to establish a consortium of multiplier organisations
- 2 Customisation and validation of ENISA security toolkit for micro enterprises by consortium
- 3 Report on lessons learned
- 4 Dissemination of results to existing European programmes/platforms

### Call for expression of interest:

In order to enhance capacity building amongst this constituency, ENISA will establish through Call for expression of Interest a dedicated consortium for business multiplier organisations and industry associations interested in cross-border co-operation aiming at exchange of information on how to build NIS capacity building for micro enterprises. This will bring together relevant organisations from different Member States with the aim to increase knowledge and competence on how to build capacity among their constituency and will be supported by ENISA deliverables.

### Customisation and validation of security toolkit:

- In its previous work on Risk Management, including work in this area as part of the 2008 Preparatory Action on micro enterprises, ENISA has directly identified the need for simplified approaches for micro enterprises that help in the achievement of an acceptable

level of security on low introduction and maintenance costs. Given this situation, the customisation of "ENISA SME security tool kit" for micro enterprises seems to be an appropriate step to help multipliers to have access to content needed to be disseminated to their constituencies in order to achieve good impact in Europe. A customized tool kit can be established consisting of:

- Risk Management approach consolidated from ENISA material and material developed in Member States as core content to be delivered to the micro enterprises by their multiplier organizations. In this context results of the ENISA ad-hoc Working Group on Risk Management can be integrated. Combined with valuable results from the pilot activities of the 2008 Preparatory Action on micro enterprises, this information can be rounded up with training material and demonstrations to play a significant role within the deployment actions by European multipliers for micro enterprises. In 2009, the applicability of the approach in specific sectors of micro business activity should be tested. For this, two significant market sectors should be chosen and agreement with the appropriate multipliers should be reached regarding usability and deployment.
- Good practice on awareness raising, as identified in 2005 by ENISA for various target groups (including SMEs). In addition, ENISA has developed its "User guide on how to raise awareness" that was updated in 2008.

The toolkit will be delivered as capacity building material amongst multiplier organisations through peer-to-peer learning or as training module provided by a dedicated trainer, thereby validating the usefulness of the toolkit for the use of multiplier organisations.

#### **Report on lessons learned:**

The consortium will draft a report on the customisation and validation of the toolkit. This includes lessons learned, enabling other multiplier organisations in the Member States to draw upon previous experience when adapting the toolkit free of charge to their specific needs.

#### **Dissemination of results to existing European programmes/platforms:**

The validated format for NIS Capacity building package for multiplier organisations of micro enterprises will be distributed further to the Member State organisations and availed in the next open take-up. Furthermore, ENISA can support the platform by reaching out to the European Regional Development Programmes (e.g. INTERREG) and to investigate their adaptability as possible national delivery platforms in Member States.

#### **OUTCOMES AND DEADLINES:**

- Call for expression of interest to establish a consortium of multiplier organisations (Q1 2009)
- Selected consortium of multiplier organizations to customise the material and deployment of the package amongst their constituency (Q1 2009)
- Customisation and validation of ENISA security toolkit for micro enterprises by consortium (Q3 2009)
- Report on lessons learned (Q4 2009)
- Dissemination of results to existing European programmes/platforms (Q4 2009)

#### **STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE**

Management Board, Permanent Stakeholders' Group, NLO, industry organisations, industry multipliers, SME associations, incubators

#### **RESOURCES FOR 2009 (person months and budget)**

- €80.000 (platform and meetings)
- 6.5 person months

#### **WORK PACKAGE PROPOSED BY:**

ENISA

#### **LEGAL BASE**

ENISA Regulation, articles 3c), d), e) and i)

## 2.3 MTP 3: Identifying emerging risks for creating trust and confidence

### PROGRAMME NAME:

Identifying emerging risks for creating trust and confidence

### DESCRIPTION OF THE PROBLEM TO SOLVE:

Decision makers in both the public and private sector need a clear insight into the nature and impact of emerging network and information security challenges in the Information Society. Such challenges are connected to emerging applications and technologies entering the European market. Such information security risks are referred to as emerging risks (ER). A better insight in ER allows public and private sector stakeholders to make better-informed decisions.

### DESCRIPTION OF THE APPROACH TAKEN SOLVING THE PROBLEM:

The Agency will establish an ER framework that will enable decision makers to better understand and assess emerging risks arising from new technologies and new applications, thereby creating stakeholders' trust and confidence. In doing so, the Agency aims at providing an antenna function for decision makers in Europe and possibly beyond.

The ER framework consists of ENISA, a Stakeholder Forum and Virtual Expert Groups. The Agency will prepare risk assessment reports to express the Agency's view on risks that may emerge in 2 to 3 years ahead arising from new technologies and applications, while performing a proof of concept of the ER lifecycle method as developed by the Agency in the course of 2006 and 2007.

The Stakeholder Forum consists of ten stakeholder partners and experts from the industry, EU organisations and Member States. It will provide feedback and support to ENISA e.g. by suggesting which new application/technology areas could be assessed and provide feedback on the functioning of the ER framework as a whole. The Stakeholder Forum ensures a multi-stakeholder dialogue with public and private sector decision makers as beneficiaries of the Agency's work in this area.

Virtual Groups of Experts will provide the Agency with their specialised know-how relevant to performing the actual risk assessment of a particular new application/technology area.

Existing/ongoing activities in the area of emerging risks/threats will be taken into account. Interfaces to corresponding research programs and activities of the European Commission have been established. ENISA will aggregate and consolidate various ongoing efforts. Results from this MTP may be used by other stakeholders for research planning activities.

It is foreseen that in the future, once the ER framework is tested and validated, request can be submitted to ENISA to analyse specific emerging and/or future application scenarios, in line with Article 6 of the Internal Rules of operation for the handling of requests. The results will then be given back to the requestor and also be made available to other interested parties, depending on the analysed scenario.

### WHICH HIGH-LEVEL GOALS THE PROGRAMME SUPPORTS:

- Facilitating the Internal Market for eCommunication by assisting European stakeholders to decide the appropriate mix of measures, i.e. technical vs. organisational and legal (noting in particular, the important contribution the Agency can make to the Framework Directive)
- Increasing the dialogue between the various stakeholders in the EU on NIS
- Building confidence in the information age through increasing the level of NIS in the EU

### **DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals)**

**SMART goal:** By 2010, at least 30 stakeholders or stakeholder organisations from at least 15 Member States refer to ENISA as point of reference for discussing the nature and impact of emerging security challenges in the Information Society.

**KPIs:** # stakeholders, # Member States

### **STAKEHOLDERS AND BENEFICIARIES**

Decision makers in both public and private sector, such as Member States governments, industry, R&D organisations, software developers, system integrators and standardisation bodies.

### **WHY ENISA?**

ENISA has the capacity to bring the relevant stakeholders together to facilitate discussion and information exchange at European level.

In 2006 and 2007 ENISA made an assessment of information security risks of emerging applications, developed a roadmap and performed studies on mechanisms to collect, process and disseminate information on emerging risks. At the same time, a number of written position papers on technology trends and risks for emerging areas have been issued.

### **PROGRAMME PROPOSED BY:**

ENISA, Management Board, Permanent Stakeholders' Group

### **LEGAL BASE**

ENISA Regulation, articles 3a), c), d), e), f), g), i) and k)

### 2.3.1 WPK 3.1: Framework for assessing and discussing emerging risks – Analysis of specific scenarios

#### MTP Name

Identifying emerging risks for creating trust and confidence

#### WORK PACKAGE NAME:

WPK 3.1: Framework for assessing and discussing emerging risks – Analysis of specific scenarios

#### DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

**SMART goal:** By Q4 2009, at least 3 risk assessment reports published

**KPI:** # risk assessment reports

**SMART goal:** By Q2 2010, at least 6 references to published risk assessment papers e.g., in policy documents or peer reviewed journals

**KPI:** # references

#### DESCRIPTION OF TASKS:

The main objective of this WPK is to produce and publish risk assessment reports on new application/technology areas. The Agency considers the following indicative list of topics, resulting from discussion with various stakeholders e.g., as emerged during the informal MB/PSG workshop of 5 June 2008 in Hersonnissos, discussion with the Commission services and the established dialogue with the Stakeholder Forum who may submit suggestions for the Agency to consider:

- eID – Following-up on the 2008 activities on pan-European eID interoperability, now focussed on security and privacy risks. For example, the Agency could assess use cases related to cross-border scenarios taking into account relevant Large Scale Projects;
- RFID – Supporting the EU policy initiatives on RFID;
- IPv6 – Supporting the EU policy development e.g., with a view to the co-existence of IPv6 with IPv4;
- Semantic Web – Supporting public and private sector policy makers in general by exploring Web 3.0 scenarios.

Apart from the above, other topics like Internet gambling, Intelligent cars, metadata, reasoning engines ontologies, real-time control systems security, virtualisation and banking and electronic payment security could be considered. It should be noted that the topics mentioned are by no means exhaustive and the Agency expects it to be updated by the end of 2008 upon recommendation of the Stakeholder Forum.

A second objective of this WPK is to test the ER Framework that has been developed during 2006 and 2007. Eventually the application of the ER Framework provides a method to deliver risk assessments in a standardised way with appropriate quality assurance. The ER Framework complements existing RA/RM methods towards identifying emerging risks. Thus, the Agency will not apply or develop any NEW RA/RM methods. At least 1 of the risk assessment reports will be developed through the ER Framework. The test includes interaction with the Stakeholder Forum and relevant Virtual Expert Group. Testing will neither affect the delivery, nor the required quality of any report.

In addition to the above, the Agency may consider targeted presentations of risks assessment reports, including those already produced in 2007, to policy makers at relevant organisations, such as EU institutions.

ENISA will liaise with relevant activities taking place at European level, to avoid any duplication of effort. Specifically, a representative from DG INFSO European Commission is a member of the Stakeholder Forum with an observer status that may act as a liaison between ENISA and DG INFSO on this particular topic and will have the opportunity to provide input. Also, ENISA has already established and will maintain close contact with similar activities and co-ordination actions funded by the European Commission FP7 framework programme, such as FORWARD and WOMBAT and other projects in the area of electronic identity. Apart from EC activities, other relevant initiatives may be communicated by external experts and/or PSG members, as well as NLOs (specifically informing the Agency of similar activities in their respective MS) throughout the roll-out of our work-programme. For this purpose, a permanent communication channel with experts will be established

#### **OUTCOMES AND DEADLINES:**

- At least three risk assessment reports of selected application scenarios (Q3 and Q4 2009)
- Report on testing the ER Framework
- Possible targeted presentations of risk assessment reports to relevant policy makers e.g., in EU Institutions

#### **STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE**

ENISA ER Stakeholder Forum, industry, academia, standardisation bodies, PSG members, NLOs

#### **RESOURCES FOR 2009 (person months and budget)**

- €230.000 (involved external experts, consultancy and data-collection)
- 18 person months

#### **WORK PACKAGE PROPOSED BY:**

ENISA

#### **LEGAL BASE**

ENISA Regulation, articles 3a), c), d), e), f), g), i) and k)

## 2.3.2 WPK 3.2: Framework for assessing and discussing emerging risks – Documentation & maintenance

### MTP Name

Identifying emerging risks for creating trust and confidence

### WORK PACKAGE NAME:

WPK 3.2: Adaptation and maintenance of the ER Framework

### DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

**SMART goal:** By Q4 2009, the EFR Framework should be complete and fully operational

**KPI:** At least one Member State or stakeholder will have used the ER Framework successfully (e.g. by means of a request to ENISA for a particular application scenario)

### DESCRIPTION OF TASKS:

As mentioned in the WPK 3.1, the pilots performed in 2009 will contribute to the improvement of the ER Framework. Identified improvements/adaptations will be implemented by means of a new version of the ER infrastructure. To this extent the ER framework will be updated accordingly. This will involve an update of the ER analysis process, a new version of the ER infrastructure, an update of the involved role definitions and finally an update of the ER handbook. The Agency expects that the version generated in 2009 will be stable/mature for future deployments/usage by involved stakeholders.

In the context of this WP, all necessary actions will be taken to appropriately document and maintain the EFR Framework, but also to improve it according to the experiences from the pilot assessments. Thus, this WPK is processing the feedback from WPK 3.1 to enhance the capabilities of the ER Framework towards the efficiency and effectiveness of its use. Within this WPK, cost/benefit aspects for the use of the ER Framework will be derived.

The ER Stakeholder Forum will contribute to this WPK by means of consultations/reviews. The input of the forum will be used to perform the updates of the ER Framework.

The decision to separate the improvement/adaptation work from WPK 3.1 serves purely project management purposes and allows the Agency to better concentrate on the adaptation of the ER Framework. To some extent, this work package may be executed in parallel to WPK 3.1.

### OUTCOMES AND DEADLINES:

The EFR Framework appropriately documented, maintained and updated.

### STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

EFR Stakeholder Forum, Industry, academia, standardisation bodies (e.g., PSG members)

### RESOURCES FOR 2009 (person months and budget)

- €80.000 (consultancy, development, data-collection, maintenance.)
- 6 person months

### WORK PACKAGE PROPOSED BY:

ENISA

### LEGAL BASE

ENISA Regulation, articles 3a), e), f), g), and k)

## Summary of Multi-annual Thematic Programmes and Work Packages

<b>MTP 1</b>	<b>Improving resilience in European eCommunication networks</b>	<b>Budget line</b>	<b>Budget €</b>	<b>Person months</b>	<b>New activity</b>
WPK 1.1	Good practices of regulatory and policy issues	3510	200.000	15	NO
WPK 1.2	Gap analysis of measures deployed by operators and good practice guidelines	3510	100.000	16,5	NO
WPK 1.3	Investigation of innovative actions	3520	150.000	14	NO
	<b>TOTAL</b>		<b>450.000</b>	<b>45,5</b>	
<b>MTP 2</b>	<b>Developing and maintaining co-operation models</b>	<b>Budget line</b>	<b>Budget €</b>	<b>Person months</b>	<b>New activity</b>
WPK 2.1	Co-operation platform for awareness raising community	3310	50.000	14	NO
WPK 2.2	Security competence circle and good practice sharing for CERT community	3300	95.000	15	NO
WPK 2.3	European NIS good practice Brokerage	3320	115.000	15	NO
WPK 2.4	Building information confidence in the area of micro enterprises through capacity building and enhanced co-operation with multipliers	3330	80.000	6,5	NO
	<b>TOTAL</b>		<b>340.000</b>	<b>50,5</b>	
<b>MTP 3</b>	<b>Identifying emerging risks to create trust and confidence</b>	<b>Budget line</b>	<b>Budget €</b>	<b>Person months</b>	<b>New activity</b>
WPK 3.1	Framework for assessing and discussing emerging risks – Analysis of specific scenarios	3500	230.000	18	NO
WPK 3.2	Framework for assessing and discussing emerging risks – Documentation & maintenance	3500	80.000	6	NO
	<b>TOTAL</b>		<b>310.000</b>	<b>24</b>	

### 3 HORIZONTAL ACTIVITIES

The Agency will perform a number of activities required for its functioning in addition to the thematic Multi-annual Thematic Programmes. This includes communication and outreach activities, managing ENISA bodies and groups, managing relations with external stakeholders, measuring the uptake of ENISA deliverables, managing the Agency's internal capabilities, internal communication and Work Programme development.

#### 3.1 Communicating and reaching out to ENISA stakeholders

The communication and outreach activities of ENISA are pivotal in increasing the impact of the Agency's work. In 2008, the Agency will manage its corporate communication channels and reach out to NIS experts. Corporate communication channels include press and media (EUR35.000), ENISA corporate website (EUR30.000), General Report on ENISA activities (EUR29.000), while producing communication material (EUR40.000). Outreach to NIS experts will be achieved through the ENISA Quarterly Review (EUR40.000), co-organised events (EUR60.000) and speaking engagements of ENISA experts at conferences and events (which does not require any additional budget).

*Legal base: ENISA Regulation, articles 2.3 and 3a), e), f) and k) and 7.5a)*

#### 3.2 Managing ENISA bodies and groups

The Agency will organise meetings of the Management Board (EUR120.000) and the Permanent Stakeholders' Group (EUR100.000, including informal MB/PSG meeting), co-ordination of Working Groups' activities (EUR25.000) and management of the network of National Liaison Officers (EUR25.000).

*Legal base: ENISA Regulation, articles 5, 6, 7.4g), h), and i), and 7.8*

#### 3.3 Managing relations with external stakeholders

The Agency will maintain and continue to develop relationships with EU Bodies, industry, academic and consumer representatives, Third Countries and International Institutions (e.g., ITU, IETF and OECD), identify common areas of interest and assess to what extent collaboration with such actors in specific activities of the Agency is feasible (e.g., facilitating dialogue on secure software development between industry and Commission as legislator). These activities require EUR455.000 for staff missions, EUR10.000 for representation costs, EUR10.000 for meetings of the Executive Director and EUR20.000 for other meetings.

*Legal base: ENISA Regulation, articles 3c) and j) and 7.4g and h)*

#### 3.4 Managing internal capabilities

"The Agency will continue to maintain and expand its Who-is-Who database with public and private sector contacts (EUR0). Building on the internal capacity of the Technology Cabinet installed in 2006 and managed in 2007, the Agency will train its experts on security tools (EUR15.000). The Agency will continue its activities on internal risk management and information security by mainly focussing on Security Policy, Awareness, and Business Continuity (EUR10.000). In addition, the Agency will maintain its ability to make translations (EUR20.000) of official financial documents."

*Legal base: ENISA Regulation, article 7.4d)*

### 3.5 Managing ENISA internal communication

The Agency highly values information sharing and co-operation between its staff and management and among all staff in general. For this purpose, the Agency has established various internal communication channels and as such will frequently issue its ENISA Inside flyer, organise weekly internal staff meetings and information sharing through its own intranet.

*Legal base: ENISA Regulation, article 7.4d) and f)*

### 3.6 Work Programme development

Each year, the Agency draws up its annual Work Programme. The programme is subject to consultation with the Permanent Stakeholders' Group and decision by the Management Board. In principle, this activity does not require any budget.

*Legal base: ENISA Regulation, article 7.5b), 7.6 and 9*

## Summary of Horizontal Activities

HA 1	Providing advice and assistance	Budget line	Budget €	Person months	New activity
HA 1.1	Co-ordination of request handling	3320	0	0,5	NO
HA 1.2	Response to request	t.b.d.	t.b.d.	t.b.d.	NO
	<b>TOTAL</b>		<b>0</b>	<b>0,5</b>	
HA 2	Communicating and reaching out to NIS stakeholders	Budget line	Budget €	Person months	New activity
HA 2.1	Press and media	3210	35.000	3,5	NO
HA 2.2	ENISA corporate website	3220	30.000	10	NO
HA 2.3	ENISA General Report	3211	29.000	4	NO
HA 2.4	Communication material	3210	40.000	2	NO
HA 2.5	ENISA Quarterly Review	3211	40.000	4	NO
HA 2.6	Co-organised events	3200	60.000	3,5	NO
HA 2.7	Speaking engagements	n.a.	0	9,5	NO
	<b>TOTAL</b>		<b>234.000</b>	<b>36,5</b>	
HA 3	Managing ENISA bodies and groups	Budget line	Budget €	Person months	New activity
HA 3.1	Management Board	3003	120.000	4	NO
HA 3.2	Permanent Stakeholders' Group	3000	100.000	4	NO
HA 3.3	Co-ordination of Working Groups	3001	25.000	2	NO
HA 3.4	National Liaison Officers Network	3320	25.000	2	NO
	<b>TOTAL</b>		<b>270.000</b>	<b>12</b>	
HA 4	Managing relations with external stakeholders	Budget line	Budget €	Person months	New activity
HA 4.1	Developing relations with industry, academia, consumer representatives and International Institutions and Third Countries	3330	0	4,5	NO
HA 4.2	Managing relations with EU Bodies	3320	0	3,5	NO
HA 4.3	Missions Executive Director	3015	45.000	0	NO
HA 4.4	Missions Co-operation and Support Department	3012	240.000	0	NO
HA 4.5	Missions Technical Department	3013	130.000	0	NO
HA 4.6	Missions Administration Department	3014	40.000	0	NO
HA 4.7	Representation costs	3011	10.000	0	NO
HA 4.8	Meetings of Executive Director	3005	10.000	0	NO
HA 4.9	Other meetings	3002	20.000	0	NO
	<b>TOTAL</b>		<b>495.000</b>	<b>8</b>	
HA 5	Managing ENISA internal capabilities	Budget line	Budget €	Person months	New activity
HA 5.1	Who-is-Who database	3320	0	0	NO
HA 5.2	Technology Cabinet	3530	15.000	17	NO
HA 5.3	ENISA IT security policy implementation	3500	10.000	1	NO
HA 5.4	Translations	3230	20.000	0	NO
	<b>TOTAL</b>		<b>45.000</b>	<b>22</b>	
HA 6	Managing ENISA internal communication	Budget line	Budget €	Person months	New activity
HA 6.1	ENISA internal newsletter, staff meetings, information sharing through intranet	n.a.	0	4	NO
	<b>TOTAL</b>		<b>0</b>	<b>4</b>	
HA 7	Work Programme development	Budget line	Budget €	Person months	New activity
HA 7.1	Development of 2010 Work Programme	n.a.	0	6,5	NO
	<b>TOTAL</b>		<b>0</b>	<b>6,5</b>	

## 4 PROVIDING ADVICE AND ASSISTANCE

A major evolution since 2006 has been the receipt by ENISA of Requests coming from the Member States (8), from the EC (6) and other European bodies (2) at an average pace of about one a month (see table below). Such requests are also expected to emerge in 2009. This confirms the role foreseen for ENISA in articles 2, 3 and 10 of the Regulation.

Article 6 of the Internal Rules of operation for the handling of requests specifies the procedure for handling incoming request. For eligible requests, the Agency will set priorities on the basis of criteria, such as availability of resources, continuity of long-term actions, existing commitments and expected added value and impact at EU level of the response to the request.

In principle, incoming requests will be handled on a first-come-first-serve basis. In case of need, the Executive Director will consult without delay the Management Board before taking a decision on priorities.

**Table: Requests handled between December 2005 and September 2008**

Requestor	Subject	Budget €	ENISA staff [Person months]
1) EDPS	Facilitating audit of EURODAC System	3.400	1,6
2) Commission	Assessment of security measures taken by electronic communication providers	0	2,2
3) NRA Lithuania	Assistance in setting-up of CERTs through organising a CERT training in Lithuania	6.745	0,8
4) Commission	Providing feedback on Impact Assessment on planned Communication	0	1,3
5) Commission	Advice on mid-term review of Directive on Electronic Signatures	850	0,5
6) Commission	Advice on eID management in Commission services	850	1,1
7) Czech Republic	Assessment of security requirements for Public Administration Information Systems	0	0,6
8a) Commission	Examining the feasibility of a data collection framework	50.000	6,0
8b) Commission	Examining the feasibility of an EU-wide information sharing and alert system	25.000	4,0
9) Greece	Advice on telephony encryption	0	0,1
10) Austria	SBA-ENISA co-operation	0	0,1
11) Austria	Risk management and analysis questionnaire	0	1,0
12) Bulgaria	Facilitating Hungarian-Bulgarian co-operation to set up Bulgarian Government CERT	0	1,0
13) Greece	Creation of CSIRT at FORTH-ICS	0	0,1
14) Austria	Assistance in setting-up of CERTs through organising a CERT training	6.745	0,8
15) Eur. Parliament	Advice on Internet security matters	0	0,5
16) Cyprus	Assistance in setting-up a governmental CERT	t.b.d.	in progress

## 5 ADMINISTRATION ACTIVITIES

The Administration Department seeks to ensure compliance and further enhance the functionality of the administrative procedures of the Agency in order to deliver dependable services. In 2009 the general goals of the Administration Department are to further extend electronic workflows previously introduced and ensure further mitigation of risks. In specific in 2009, the Administration Department seeks to:

- Continue ensuring compliance with the prevailing regulatory framework
- Introduce more electronic workflows to reduce paper based transactions
- Take further steps towards business continuity planning
- Define service levels for administrative services

The Administration Department seeks to further improve its interaction with sections and functions of the Agency that have a horizontal service orientation such as Accounting and Internal Control. The Work Programme 2009 also includes highlights of the activities of these two functions next to the planning of the activities of the Administration department.

### 5.1 General Administration

General administration tasks contribute to the management and measurement of performance of the Administration Department. Major tasks include planning, advising, representing, reporting upon and controlling the activities of the Sections and the Department. In 2009 the priorities of General Administration include:

- Multi-annual planning of activities
- Monitoring of annual budget execution
- Planning the deployment of electronic workflows
- Risk management follow up in terms of business continuity planning

The main activities planned for 2009 are the following:

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget €
1.1	Administration activities' planning. Representation of AD	Planning of activities, guidance and management. Setting goals and priorities. Co-ordinating with Agency's Departments & Sections. Collaborating with key staff to meet service goals. People management.	Planning of activities per Section. Guidance to meet goals. Annual work plan. AD staff objectives. Co-ordination. Communication.	Ongoing	0
1.2	Advise and support the ED and Heads of Departments as appropriate on AD related issues, including governance, sound financial management, activity based management, contingency planning, business continuity, legal services, safeguard of assets	Reports to ED and collaborates with the Heads of Departments and key staff as appropriate	Reports to ED and collaborates with the Heads of Departments and key staff as appropriate. Continuous support to ED and Heads of Department. Timely responses to requests for support. Support the implementation of internal controls and systems to control resources and property.	Weekly	0
1.3	Ensure that appropriate reporting levels on the use of the Agency's resources are available at all times. Leverage on financial data and AD report lines	As appropriate	Periodic evaluation of the Department's internal and external reporting needs. Reporting, and follow up.	Quarterly	0
1.4	Follow up on audit results regarding Administration practices and procedures as they are implemented in line with FR, IR and SR. Collaborate with Internal Control Co-ordination and Accounting. Business continuity planning.	Update of documents and activities reporting  Co-ordination with internal (Internal Control Co-ordination, Accounting, Risk Management Section) and external actors (ECA, IAS etc.)	Implement audit recommendations Continuous improvement of performance.  Risk management	Quarterly	0

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget €
1.5	General organisational tasks – Administration Secretariat	Filing, reporting, initiation as appropriate	Volume of activities Timely execution	Ongoing	0
1.6	Horizontal task support	Administration of horizontal tasks (e.g. translations)	Volume of activities Timely execution	Ongoing	0
1.7	Office Services	Maintenance. Supplies' delivery. Postal services. Vehicle administration	Number and duration of service outages. Volume of activities. Timely execution of activities.	Ongoing	0

## 5.2 Finance

The Finance Section comprises of budget planning, administration and financial control as well as parts of payroll administration and missions' co-ordination. The Finance Section plays a significant role with regard to the overall management of the annual budget and general budget reporting. In 2009 budget available is slightly lower than in previous years. Yet closer monitoring of planning and execution of the Budget is likely to alleviate some of the adverse effects of budget constraints. In 2009 the priorities of the Finance Section include:

- Monitoring of budget execution and planning. Notional activity based management planning
- Functional support regarding electronic workflows (ABAC, missions management).

The main activities planned for 2009 are the following:

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget €
2.1	Opening and Closing of the Annual Budget and preparation of Budgetary Statements.	Approved budget tree opened, appropriations posted properly.	Annual budget lines open and available by the end of the third week of the fiscal year, economic outturn account and supporting operations done on time.	By the end of January and by the end of the third week of December. Preparation by 10 December.	0
2.2	Implementation and Consolidation of Internal Procedures and Internal Controls.	Annual review of internal Procedures and Internal Controls	Guidelines and check-lists reviewed. Annual risk assessment. Controls updated accordingly. Training sessions to create awareness of procedures and controls.	Quarterly	0
2.3	Annual budget reports	Monthly	Budget status reporting for all areas, Titles and Department, as necessary, including analysis of main relevant aspects.	Monthly (for the previous month)	0
2.4	Organising carryovers	Support the Departments in dealing with carryovers	Communication Time and control	Annually by end of second week of the year	0
2.5	Payroll administration	Financial aspects of payroll management in co-operation with HR Payroll planning and control	Timely payment of salaries and liaising with PMO as appropriate	Monthly	0
2.6	Missions' Co-ordination	Support on the preparation and planning of missions and reimbursements	Number of missions, commitments, payments, claims received Average reimbursement terms	Ongoing	0

### 5.3 Human Resources

HR activities at ENISA include recurrent tasks, and general activities particularly related to recruitments, performance evaluations, training, health and safety at work, leave management handling of individual rights and payroll management. In 2009 the emphasis previously introduced with regard to horizontal team management continues in order to serve operational goals at the MTP level. In 2009 the priorities of the HR Section include:

- Resource planning (Staff Policy Plan)
- Training planning and execution, affirmative measurable measures for staff retention (attrition rates, cost of turnover, etc.)
- Implementing electronic workflows

The main activities planned for 2009 are the following:

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget €
3.1	Staff Policy Plan and implementing rules	Draft, update and follow-up of changes to the SR and its IR as well as to other staff guidelines as necessary. Draft, update and follow up the Staff Policy Plan	Updated implementing rules Communicate with Staff. Liaise with Staff Committee and Commission on Implementing Rules and Staff Policy Plan	Ongoing	0
3.2	Administer Title 1 Payroll and individual rights Grading Committee	Monthly Payroll and employer duties carried out on time. Individual rights. Grading Committee.	Flawlessly administer Title 1 and payroll. Control HB Postings. Co-ordinate with ACC and PMO on accuracy of postings Ex post control of payments.	Monthly. Grading Committee (2-4 sessions p.a.)	4.463.000
3.3	Staff Performance Evaluation	Annual performance and probationary period evaluations. Timetables and communication. Appeals' support. Monitor job descriptions and job performance.	Number of evaluations. Planning. Timely conclusion of procedures	Once per year. For probation period, as appropriate	0
3.4	Annual Training Programme	Training Program (in-house, external, upon individual initiative). Preparation, handling and assessment of individual trainings and training requests.	Training planning Document presentation and acceptance. Training programmes to cover key performance areas.	Yearly	100.000
3.5	Recruitment plan	Execute the Agency recruitment plan in line with the Establishment Plan. Publish vacancy notices. Organise Selection Committees. Communicate with candidates. Induction for new recruits.	Number of Staff hired to cover new posts or make up for resignations. Speed of hiring. Planning Staff resettlement guidance.	Ongoing	425.000
3.6	Health and Safety at Work	Annual Staff Health and Safety Programme	Administer Health and Safety Programme (Medical inspections, pre-recruitment medical visits, working conditions, first aid, medical adviser, medical centre).	Yearly	40.000

## 5.4 ICT

The ICT Section administers the internal ICT systems and networks of the Agency. The ICT Section ensures the planning and good operation of all major systems at all times, including servers, databases, client devices (desktops, laptops, cell phones etc.), area networks, communications etc. Part of the ICT work is entrusted to third parties, especially with regard to IP connections, financial management systems etc. Additionally the ICT Section provides guidance and interacts with IT resources available within the operational Departments of the Agency with regard to user requirements, contingency planning and business continuity. In 2009 the priorities of the ICT Section include:

- Deployment of electronic workflows including:
  - Missions' management
  - Internal procurement procedures
- Authentication
- Risk management follow up in terms of:
  - Contingency planning implementation
  - Business continuity follow up

In 2009 the main activities planned for the ICT Section are the following:

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget €
4.1	Planning of ICT systems in terms of hardware, software and networks	ICT Networks and Systems in place managed by ENISA or a third party Software license administration User requirements	Systems' availability and integrity. Downtime. Outage Planning	Ongoing	78.000
4.2	ICT Services	Determine and maintain level of services available	Service delivered according to pre-defined levels	Ongoing	0
4.3	Internal ICT Support	ABAC administration and support. General Systems and Networks support and Help Desk. Maintenance. Testing.	Calls for assistance. Results of a Test Plan Maintenance plan	Ongoing	0
4.4	Risk Management and Security plan for Agency resources Business Continuity	Management of systems' confidentiality and integrity. Co-ordinate with ITMAC, the Risk Management Section and the Technology Cabinet	Planning and implementation of risk mitigation measures  Handling security incidents	Quarterly	71.000

## 5.5 Legal and Procurement

The Legal Section carries out budget implementation and control activities that include general contract management and public procurement of the Agency. The Legal Section makes available to the Agency legal advice, legal services as well as procurement guidance and services. The Legal Section may also carry out *ad hoc* operational tasks as it might be needed and agreed with the operational Departments. In 2009 the priorities of the Legal Section include:

- Back office organisation in terms of an electronic workflow for procurement administration
- Efficient procurement project planning
- Contract management planning

The main activities planned for 2009 are the following:

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget €
5.1	Legal Advice, as requested by the ED and Departments. Data Protection Co-ordination	Legal opinion as requested. Representation of the Agency in all appropriate instances. Participation in internal and external events and work. Data Protection officers' tasks and reporting to EDPS	Number of internal cases handled (legal opinions, complaints, legal cases, reports summarizing key elements and sharing relevant information) Data protection co-ordination	Ongoing	0
5.2	Public Procurement	Regular carrying out of public procurement procedures and appropriate assistance provided to all Departments. Procurement planning.	Procurement Plans, routing slips and forms available, number and type of procurement processes handled, files organized. Purchase Order files. Suppliers' data base. Enquiries handled. Procurement planning and consolidation of procurement activities.	Ongoing	0
5.3	Contract Management	General support on contract management	Number of contracts prepared and signed by the Agency, number of requests for support received from Departments, number of claims received regarding this matter. Routing slips.	Ongoing	0
5.4	Operational support	Provide legal input to ENISA Operational Activities as requested and agreed	Time spent on administering of and providing feedback to Operations.	<i>Ad hoc</i> , as requested and agreed	0
5.5	Representation	Representation in terms of formal events, and representation before Administrative and Budget Authorities and Courts in co-ordination with the Head of Department and approval by ED.	Number of cases handled	Ongoing	0

## Summary of Administration Activities

ADA 1	General Administration	Budget line	Budget €	Man months	New Activity
ADA 1.1	Planning of administration activities	N/A	N/A	1	NO
ADA 1.2	Advice and support	N/A	N/A	2	NO
ADA 1.3	Reporting levels on Agency's resources	N/A	N/A	2	NO
ADA 1.4	Audit follow up	N/A	N/A	3	NO
ADA 1.5	Administration Secretariat	N/A	N/A	12	NO
ADA 1.6	Support on horizontal tasks	N/A	N/A	4	NO
ADA 1.7	Office Services	N/A	N/A	8	NO
	<b>TOTAL</b>		<b>0</b>	<b>32</b>	
ADA 2	Finance	Budget line	Budget €	Man months	New Activity
ADA 2.1	Opening and closing of annual budget	N/A	N/A	3	NO
ADA 2.2	Implementation and consolidation of internal controls	N/A	N/A	18	NO
ADA 2.3	Reporting on annual budget	N/A	N/A	1	NO
ADA 2.4	Organising carryovers	N/A	N/A	1	NO
ADA 2.5	Payroll administration	N/A	N/A	1	NO
ADA 2.6	Missions' co-ordination	N/A	N/A	8	NO
	<b>TOTAL</b>			<b>32</b>	
ADA 3	Human Resources	Budget line	Budget €	Man months	New Activity
ADA 3.1	Staff policy plan	N/A	N/A	2	NO
ADA 3.2	Payroll administration & Grading	Chapter 11	4.463.000	6	NO
ADA 3.3	Performance evaluation	N/A	N/A	6	NO
ADA 3.4	Annual training programme	1320	100.000	4	NO
ADA 3.5	Recruitment plan	1200	425.000	13	NO
ADA 3.6	Health and safety at work	1310	40.000	1	NO
	<b>TOTAL</b>		<b>5.028.000</b>	<b>32</b>	
ADA 4	ICT	Budget line	Budget €	Man months	New Activity
ADA 4.1	ICT systems planning	2300	78.000	6	NO
ADA 4.2	ICT services	2301	0	6	NO
ADA 4.3	Internal ICT Support	2302	0	12	NO
ADA 4.4	IT risk management and Business continuity	N/A	71.000	4	YES
	<b>TOTAL</b>		<b>149.000</b>	<b>28</b>	
ADA 5	Legal and procurement	Budget line	Budget €	Man months	New Activity
ADA 5.1	Legal advice and representation	N/A	N/A	6	NO
ADA 5.2	Public procurement	N/A	N/A	8	NO
ADA 5.3	Contract management	N/A	N/A	0,5	NO
ADA 5.4	Operational support	N/A	N/A	0,5	NO
ADA 5.5	Representation	N/A	N/A	1	NO
	<b>TOTAL</b>		<b>0</b>	<b>16</b>	
	<b>GRAND TOTAL</b>		<b>5.177.000</b>	<b>140</b>	

## 6 DIRECTORATE ACTIVITIES

At ENISA's Directorate, the reporting lines ensure the horizontal functions of Accounting and Internal Control co-ordination.

### 6.1 Accounting<sup>8</sup>

Accounting at ENISA is a discreet function that addresses the following tasks in line with the financial regulation:

- Annual accounts of the Agency
- Accounting ledgers that include a journal, a general ledger and an inventory
- Property inventories
- Payments etc.Ongoing

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget €
6.1	Payments and Accounts	Carrying out payments Reporting Annual accounts	Accuracy, timely responses, respect of formal deadlines	Ongoing	0
6.2	Co-ordination of audits	Opinions of Accountant Advice to management and staff on accounting matters Co-ordination with external stakeholders namely, the Court of Auditors, as appropriate etc.	Number of cases supported Timely responses	Ongoing	0

### 6.2 Internal control co-ordination<sup>9</sup>

Internal control co-ordination at ENISA is a function that is carried out within the Directorate. In 2009 the main activities include the following:

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget €
7.1	Internal control co-ordination	Opinions of Internal Control Co-ordinator Advice to management and staff on internal control Co-ordination with external stakeholders namely internal control consultants, the Commission Internal Audit Service, as appropriate etc.	Number of cases supported Timely responses	Ongoing	p.m.
7.2	Assistance to the ED	Regular carrying out of public procurement procedures and appropriate assistance provided to all Departments. Procurement planning.	Number of requests handled Timely responses	Ongoing	0
7.3	Relations with the host Member State	Regular interactions with regard to tax status etc., associated with the host Member State	Number of requests handled Timely responses	Ongoing	0

<sup>8</sup> At ENISA Accounting belongs to the Directorate and the reporting line of the Accounting Section is directly linked to the Executive Director.

<sup>9</sup> At ENISA Internal Control belongs to the Directorate and the reporting line of the Internal Control Coordinator is directly linked to the Executive Director.

## Summary of Directorate Activities

ADA 1	Accounting	Budget line	Budget €	Man months	New activity
ED 1.1	Payments Accounts	N/A	N/A	22	NO
ED 1.2	Co-ordination of Audits	N/A	N/A	2	NO
	<b>TOTAL</b>		<b>0</b>	<b>24</b>	
ED 2	Internal Control Co-ordination	Budget line	Budget €	Man months	New activity
ED 2.1	Internal control co-ordination	N/A	p.m.	2	NO
ED 2.2	Assistance to the Executive Director	N/A	N/A	5	NO
ED 2.3	Relations with the host MS	N/A	N/A	9	NO
	<b>TOTAL</b>		<b>0</b>	<b>18</b>	
	<b>GRAND TOTAL</b>		<b>0</b>	<b>42</b>	





PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280  
[www.enisa.europa.eu](http://www.enisa.europa.eu)