ENISA Work programme 2016 with amendments

Including Multi-Annual Planning

Consolidated version

ENISA Work programme 2016 with amendments adopted by the Management Board on 15 March 2016 (Decision No MB/2016/5)

About ENISA

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

Contact

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

Email: info@enisa.europa.eu
Internet: http://www.enisa.europa.eu

ISSN: 2363-3115, ISBN 978-92-9204-169-4, DOI: 10.2824/150042, Catalogue no.: TP-AF-16-001-EN-N.

Contents

Acronyms 5

1. Introduction 6

1.1 Conventions 6

1.2 Structure of this document 6

1.3 Key goal indicators 7

2. Policy and legal context 8

3. Multiannual planning. Strategic objectives 2016-2018 11

3.1 Strategic objective 1 11

3.2 Strategic objective 2 11

3.3 Strategic objective 3 12

3.4 Strategic objective 4 13

4. Core operational activities 14

4.1 SO1. To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security 14

4.1.1 WPK1.1. Improving the expertise related to critical information infrastructures 15
4.1.2 WPK1.2. Network and information security threats landscape analysis 16
4.1.3 WPK1.3. Research and development, innovation 18

4.2 SO2. To assist the Member States and the European Union institutions and bodies in enhancing capacity building throughout the European Union 19

4.2.1 WPK2.1. Assist Member States' capacity building 20
4.2.2 WPK2.2. Support European Union institutions' capacity building 23
4.2.3 WPK2.3. Assist private sector capacity building 25
4.2.4 WPK2.4. Assist in improving general awareness 26

4.3 SO3. To assist the Member States and the European Union institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security 27

4.3.1 WPK3.1. Supporting European Union policy development 29
4.3.2 WPK3.2. Supporting European Union policy implementation 33

4.4 SO4. To enhance cooperation both between the Member States of the European Union and between related network and information security communities 40

4.4.1 WPK4.1. Cyber crisis cooperation and exercises 41
4.4.2 WPK4.2. Network and information security community building 43

4.5 Horizontal activities supporting core operations 45

4.5.1 Management board, executive board and permanent stakeholders group secretariat 45
4.5.2 National liaison officer network 45
4.5.3 European Union relations 45

4.5.4 Spokesperson, stakeholders communication and dissemination activities 45
4.5.5 Quality control and project office 46
4.5.6 Article 14 requests 46
4.5.7 Data protection officer 46

5. Management, administration and support activities 48

5.1 Executive director's office 48

5.2 Administration and support department 48

5.3 Activities 48

5.3.1 ASA 0 Executive director's office and general management 48
5.3.2 ASA 1 Quality management systems, ICC, security, facilities management, internal communications 48
5.3.3 ASA 2 Finance, accounting and procurement 49
5.3.4 ASA 3 Human resources 50
5.3.5 ASA 4 Information and communications technology 50

6. Summary of activities and budget allocation 51

6.1 Summary of core operational activities with strategic objectives, work packages and deliverables 51

6.2 Activity-based budgeting 53

6.2.1 Summary of core operational activities 54
6.2.2 Summary of administration and support activities 55

Annex 1 – Financing Decision 56

Acronyms

ABAC: accrual based accounting
ABB: activity-based budgeting
APF: annual privacy forum
ASA: administration and support activities
ASD: administration and support department
BEREC: Body of European Regulators of Electronic Communications
CE2014: Cyber Europe 2014
CEP: cyber exercise platform
CERT-EU: Computer emergency response team for the EU institutions, bodies and agencies
CEN: European Committee for Standardisation
CENELEC: European Committee for Electrotechnical Standardisation
CIIP: critical information infrastructure protection
CoA: Court of Auditors
COD: Core operations department
CSCG: ETSI CEN-CENELEC cybersecurity coordination group
CSIRT: computer security incidents response teams
CSS: cybersecurity strategy
D: a deliverable
DG: directorate-general
DPA: data protection authorities
DPO: data protection officer
DSM: digital single market
EB: executive board
EC: European Commission
EC3: Europol's European cybercrime centre
ECSM: European Cybersecurity Month
ED: executive director
EDPS: European Data Protection Supervisor
EFTA: European Free Trade Association (Stockholm Convention)
eID: electronic identification
eIDAS regulation: electronic identification and trust services for electronic transactions in the internal market
ENISA: European Union Agency for Network and Information Security
ECIs: European critical infrastructures
ETSI: European Telecommunications Standards Institute
EU: European Union
Europol: European Police Office
FAP: Finance, accounting and procurement unit
FI-ISAC: financial institutes — information sharing and analysis centre
FIRST: forum of incident response and security teams
FM: facilities management
FTEs: full-time equivalents
IAC: internal audit capability
IoT: the internet of things
ISMS: information security management system
ITIL: IT infrastructure library
KGI: key goal indicator
H2020: Horizon 2020
HR: human resources
IAS: internal audit service
ICC : internal control coordination
ICS: industrial control systems
ICT: information and communications technology
IS: information systems
ISPs: internet service providers
IT: information technology
IXP: internet exchange point
KII: key impact indicator
KPI: key performance indicator
LEA: law enforcement agency
M2M: machine to machine
MB: management board
MS: Member State(s)
NCSS: national CSS
NGO: non-governmental organisation
NIS: network and information security
NLO: national liaison officer
NRA: national regulatory authority
PETs: privacy-enhancing technologies
PPP: public-private partnership
PSG: permanent stakeholders group
Q: quarter
QC: quality control
R & D: research and development
SCADA: supervisory control and data acquisition
SLA: service level agreement
SMEs: small to medium-sized enterprises
SO: strategic objective(s)
SOP: standard operating procedures
TF-CSIRT: CSIRT task force
TRANSITS: CSIRT personnel training
TSP: trust service provider
US: United States
WP: work programme
WPK: work package

1. Introduction

This document provides a complete description of the work that the European Union Agency for Network and Information Security (ENISA) intends to carry out during 2016 and an associated multiannual planning for the years 2017 and 2018.

The work programme (WP) in its current state has been updated based on the feedback received from the European Commission (EC) and the Member States (MS) in August 2015 and covers also the changes of the ad hoc group meetings of May and September 2015. The initial draft was built on the conclusions of the ENISA strategic management board (MB) meeting of October 2014, updated with the feedback received from permanent stakeholders group (PSG) of November 2014 and addresses the recommendations of the two ad hoc group meetings that took place in November and December, respectively, 2014.

The multiannual planning component has been derived from the ENISA Strategy document, which has been developed together with the ENISA MB. As such, the planning is based on four strategic objectives (SO) (which are presented in section 3.1.). This approach ensures that future ENISA WPs reflect the SO of the agency.

1.1 Conventions

Terms and acronyms used in this document are listed in the acronyms section.

Throughout this WP and all associated documentation, ENISA uses the phrase 'capacity building' to refer to those activities that increase the preparedness of the relevant stakeholder communities to recognise and respond to cybersecurity incidents. Although the ENISA regulation refers to 'capability building', the use of the term 'capacity building' is more prevalent throughout the cybersecurity community and ENISA therefore adopt this practice. However, in no case does the Agency use this term to cover activities that are outside the ENISA mandate.

1.2 Structure of this document

This document is structured as follows:

- **SO and multiannual planning**. The SO and multiannual planning provide the link between the ENISA strategy document and future WPs. In this section, key goals are set for each core priority for the period 2016-2018.
- **Core operational activities 2016**. This section presents the core activities for 2016, which are structured around the SO of the agency. (Budget and resources are presented at the work package (WPK) level at the end of the document.) In addition, this section also covers the activities supporting the core operations of ENISA, such as the provision of the MB, executive board (EB) and PSG secretariat, national liaison officers (NLOs) and European Union relations, stakeholder communication activities, project office, data protection officer, etc.
- **Administration and support department, directorate and general management activities.** This section of the document summarises the activities of the Administration and support department (ASD) and the executive director (ED). Budget and resources requirements are presented at the end of this document.
- **Summary of budget and resource allocation.** Budget and resources are presented at the WPK level at the end of the document; the budget and the resource requirements for the ASD are also summarised at the end of this document.
- **Annex for financing decision.** The annex of this document provides a table which covers budget and resources which are planned to be used for procurement purposes and for financing decisions.

1.3 Key goal indicators

Key goal indicator (KGI) is a term that refers to pre-set indicator of process objectives (goals) that indicates what should be achieved by a process (it defines an objective). Metrics used must be measurable. KGIs provide a measure of what has to be accomplished in the attempt to respond to the question 'are we doing the right things?'

While the key performance indicators (KPIs) show how well the processes work, KGIs show how well the results and goals are being achieved.

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

2. Policy and legal context

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

No	Policy document	Complete title and link ([2])
1	**The new ENISA Regulation (EU) No 526/2013**	Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:L:2013:165:TOC Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.
2	**Cybersecurity strategy of the EU**	Joint communication on the cybersecurity strategy of the European Union: 'An open, safe and secure cyberspace', JOIN(2013) 1 final of 7 February 2013, available from: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
3	**The proposal for an NIS directive**	Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final of 7 February 2013, available from: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
4	**Council conclusions on the cybersecurity strategy**	Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy joint communication on the cybersecurity strategy of the European Union: An open, safe and secure cyberspace, agreed by the General Affairs Council on 25 June 2013. http://register.consilium.europa.eu/pdf/en/13/st12/st12109.en13.pdf
5	**Digital agenda**	Commission communication — 'A digital agenda for Europe', COM(2010) 245 final of 19 May 2010. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245&from=EN
6	**Directive on European critical infrastructures (ECIs)**	Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:jl0013
7	**Critical information infrastructure protection (CIIP) action plan**	Commission communication on critical information infrastructure protection, 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience', COM(2009) 149 final of 30 March 2009, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF
8	**Commission communication on critical information infrastructure protection**	Commission communication on critical information infrastructure protection, 'Achievements and next steps: towards global cyber-security' adopted on 31 March 2011 and the Council conclusion on CIIP of May 2011. http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf
9	**Electronic communications regulatory framework**	Telecommunications regulatory package (Article 13a. amended Directive 2002/21/EC framework directive).
10	**Review of the data protection framework**	Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation), COM(2012) 11 final of 25 January 2012,

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

([2]) Links available as of October 2015.

		available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
11	**Regulation on electronic identification and trusted services for electronic transactions in the internal market (eIDAS)**	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market. http://eur-lex.europa.eu/legal-tent/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
12	**Commission regulation on the measures applicable to the notification of personal data breaches**	Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF
13	**Framework to build trust in the digital single market (DSM) for e-commerce and online services**	Commission communication — 'A coherent framework for building trust in the digital single market for e-commerce and online services', COM(2011) 942 final of 11 January 2012. http://ec.europa.eu/internal_market/e-commerce/communication_2012_en.htm
14	**Directive on attacks against information systems (IS)**	Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013L0040
15	**Communication on Europol's European cybercrime centre (EC3)**	Commission Communication — 'Tackling crime in our digital age: Establishing a European cybercrime centre', European Commission, COM(2012) 140 final of 28 March 2012, available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/communication_european_cybercrime_centre_en.pdf
16	**Council resolution of December 2009 on a collaborative approach to network and information security (NIS)**	Council resolution of 18 December, 2009 on a collaborative approach to network and information security (2009/C 321 01), available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:C:2009:321:TOC
17	**Council conclusion on CIIP of May 2011**	Council conclusion on CIIP of May 2011, available at: http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf
18	**Action plan for an innovative and competitive security industry**	Commission communication on security industry policy, 'Action plan for an innovative and competitive security industry', COM(2012) 417 final of 26 July 2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF
19	**Single Market Act**	Single Market Act: Twelve levers to boost growth and strengthen confidence, 'Working together to create new growth', COM(2011) 206 final of 13 April 2011. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0206:FIN:en:PDF
20	**Internet of things — An action plan for Europe**	Commission communication — 'Internet of things — An action plan for Europe', COM(2009) 278 final of 18 June 2009. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF
21	**European cloud computing strategy**	Commission communication — 'Unleashing the potential of cloud computing in Europe', COM(2012) 529 final of 27 September 2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF
22	**Internal security strategy for the European Union**	An internal security strategy for the European Union (6870/10). http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/113055.pdf
23	**Telecom ministerial conference on CIIP**	Telecom ministerial conference on CIIP organised by the Presidency in Balatonfüred, Hungary, 14-15 April 2011
24	**Data protection directive**	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
25	**Digital single market (DSM) strategy**	Commission communication — 'A digital single market strategy for Europe', COM(2015) 192 final of 6 May 2015, available at: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf

26	**Communication on thriving data-driven economy**	Commission communication — 'Towards a thriving data-driven economy', COM(2014) 442 final of 2 July 2014, available at: https://ec.europa.eu/digital-agenda/en/news/communication-data-driven-economy

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

3. Multiannual planning. Strategic objectives 2016-2018

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

- SO1. To develop and maintain a high level of expertise of European Union (EU) actors, taking into account evolutions in network and information security (NIS).
- SO2. To assist the Member States (MS) and the EU institutions and bodies in enhancing capacity building throughout the EU.
- SO3. To assist the MS and the EU institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security.
- SO4. To enhance cooperation both between the MS of the EU and between related NIS communities.

The following sections provide high-level, multiannual planning for each of these objectives, thereby providing a basis for the definition of future ENISA WPs.

The total cost presented in the table includes, besides the actual budget for projects, the salary costs of staff working for the particular SO.

3.1 Strategic objective 1

SO1: To develop and maintain a high level of expertise of EU actors, taking into account evolutions in network & information security (NIS).		
KGI.1.1. Improve the expertise related to critical information infrastructure • **KPI.1.1.1. Number of sectors covered and mean level of coverage.** • **KPI.1.1.2. Good practices and recommendations delivered for the selected sectors** KGI.1.2. Improve the expertise on NIS threats • **KPI.1.2.1. Annual report on threat landscape.** • **KPI.1.2.2. Two risk assessments in the area.** KGI.1.3. Develop expertise related to NIS in research and development (R &D) and innovation • **KPI.1.3.1. Number of areas covered and mean level of coverage by NIS recommendations for new/specific areas.** • **KPI.1.3.2. Number of participations in steering committees/advisory boards of projects funded by EU linked to NIS.**		
	2017	2018
Resources (**full-time equivalents** (FTEs))	11.5	11
Total cost (EUR)	1 285 327.38	1 312 226.19

3.2 Strategic objective 2

SO2: To assist the MS and the EU institutions and bodies in enhancing capacity building throughout the EU.
KGI.2.1. Assist MS capacity building • **KPI.2.1.1.Number of updates of impact assessment/reports/training material related to capacity building.**

- **KPI.2.1.2. Number of operational training sessions and participants.**
- **KPI.2.1.3. Bi-annual update of good practice guide for establishment and management of national cybersecurity strategies (NCSS).**
- **KPI.2.1.4. Number of MS which participate in the NCSS group.**
- **KPI.2.1.4. Number of MS which participate in the government cloud area.**

KGI.2.2. Support/assist EU institutions and bodies: NIS capacity building

- **KPI.2.2.1. Number of Info notes and the number of topics covered.**
- **KPI.2.2.2. Number of European Union institutions engaged in dialogue on the reinforcement of their NIS.**

KGI.2.3. Assist private sector capacity building.

- **KPI.2.3.1. Report on best practices for MS to reach private sector on NIS-related dissemination activities.**
- **KGI.2.4. Assist in improving general awareness.**
- **KPI.2.4.1. Number of MS and participants in the cyber challenge.**
- **KPI.2.4.2. Number of MS reached/involved in the activitEURies related to NIS education/European Cybersecurity Month (ECSM)/online privacy and security tools portal.**

	2017	2018
Resources (FTEs)	23	23
Total cost (EUR)	2 213 654.76	2 273 154.76

3.3 Strategic objective 3

SO3: To assist the MS and the EU institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of NIS.

KGI.3.1. Support EU policy development linked to Secure Infrastructure and Services

- **KPI.3.1.1. Number of contributions to EU policy or to policy discussions in different areas (such as smart grids, industrial control systems (ICS)-Supervisory control and data acquisition (SCADA), information technology (IT) security certification, finance).**
- **KPI.3.1.2. Number of stakeholders contributing to/supporting the recommendations for improving NIS in EU standardisation policy for supporting policy development and standardisation.**
- **KPI.3.1.3. Impact assessment on NIS dependencies.**

KGI.3.2. Support EU policy implementation

- **KPI.3.2.1. Number of contributors and number of reports on recommendations/guidelines for implementation of proposed NIS directive after its entering into force.**
- **KPI.3.2.2. Number of events and number of contributions to NIS platform/NIS dialogue.**
- **KPI.3.2.3. Annual incident report in the context of Article 13a.**
- **KPI.3.2.4. Number of e-communication providers taking part in ENISA work on network resilience.**
- **KPI.3.2.5. Number of trust service providers taking part in ENISA's work on electronic identification and trust services for electronic transactions in the internal market (eIDAS) mandatory incident-reporting scheme.**
- **KPI.3.2.7. Number of stakeholders (public and private) engaged in the context of NIS directive.**
- **KPI.3.2.8. Number of sectors covered by ENISA recommendations in the context of proposed NIS directive.**

• **KPI.3.2.9. Number contributors and number of recommendations/guidelines/protective measures proposed/updated to address the NIS measures/needs of data protection legislation and upcoming/proposed EU data protection regulation.** • **KPI.3.2.10. Number of participants in the annual conference dedicated to support privacy debate from an NIS perspective.** • **KPI.3.2.11. Number of contributors and number of reports on incidents and on incidents reporting addressing different mandatory incident-reporting schemes/policies.** • **KPI.3.2.12. Number of reports on recommendations/guidelines for implementation of electronic identification and trust services legal framework.**		
	2017	2018
Resources (FTEs)	28	28
Total cost (EUR)	2 718 166.67	2 777 666.67

3.4 Strategic objective 4

SO4: To enhance cooperation both between the MS of the EU and between related NIS communities.		
KGI.4.1. Support cyber crisis cooperation and exercises • **KPI.4.1.1. Annual report on cyber crisis cooperation and exercises.** • **KPI.4.1.2. Exercise plan in 2017 and exercises in 2016 and 2018.** • **KPI.4.1.3. Average satisfaction level of participants in** international conference **on cyber crisis cooperation and exercises 60 % or better (in evaluation).** KGI.4.2. Support NIS community building • **KPI.4.2.1. Average satisfaction level of participations in** computer **security incidents response teams (CSIRT) community groups, programme committees and special interest groups 60 % or better (in evaluation).** • **KPI.4.2.2. Average satisfaction level of participants in the annual ENISA national and governmental CSIRT Workshop 60 % or better (in evaluation).** • **KPI.4.2.3. Average satisfaction level of participants in the annual ENISA/EC3 cybercrime workshop 60 % or better (in evaluation).** • **KPI.4.2.4. Supporting European network of MS CSIRTs.**		
	2017	2018
Resources (FTEs)	13	13
Total cost (EUR)	1 264 130.95	1 264 130.95

4. Core operational activities

Since 2015, ENISAs core operational activities are aligned with the SO from the strategy and the multiannual planning. The SO, as mentioned in the previous section are as follows.

- SO1. To develop and maintain a high level of expertise of EU actors, taking into account evolutions in NIS.
- SO2. To assist the MS and the EU institutions and bodies in enhancing capacity building throughout the EU.
- SO3. To assist the MS and the EU institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of NIS.
- SO4. To enhance cooperation both between the MS of the EU and between related NIS communities.

4.1 SO1. To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security

SO1 aims to develop and maintain a high level of expertise of EU actors, taking into account evolutions in network and information security (NIS). This SO covers the threat landscape and risk assessment, including new technologies and specific areas such as smart grids and e-health as well as information sharing and good practices and recommendations for critical information infrastructure protection (CIIP).

List of Work packages and short description

- **WPK1.1. Improving the expertise related to critical information infrastructures**

In this work package (WPK) ENISA aims to develop good practices on emerging smart critical infrastructures ([3]) and services. This work will provide smart critical information infrastructure and service providers and developers with good security and resilience practices when designing, developing and deploying such services in order to minimise the exposure of such network and services to all relevant cyberthreat categories.

- **WPK1.2. NIS threats landscape analysis**

Ensuring adequate levels of protection for modern IT systems in any context requires recognising and adapting to changes in the evolving threat environment. Whilst it is clearly not possible to predict all future threats (security practices have often been dramatically changed as a result of so called 'black swan' events, which are notoriously difficult to predict), it is possible to predict the evolution of certain threats with a reasonable degree of accuracy based on past data.
ENISA can support its stakeholders by compiling existing data on threat evolution and tailoring this data to the needs of specific stakeholder communities. The approach will be to cover threats across all sectors, whilst identifying specificities particular to particular communities in line with the goals of the WP. This is a more scalable approach than carrying out threat analysis directly.

- **WPK1.3. Research and development, innovation**

Although there is state-of-the-art research in Europe in the field of NIS, and this area is extensively supported by European-funded programmes, research is usually not focused on the aspects where NIS policies need available technologies to move forward on their implementation. ENISA aims in this WPK to contribute to the various consultations launched by the Commission in the area of NIS. Such consultations

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

may be conducted in the context of setting the research priorities for future calls for proposals or in the context policy initiatives launched or about to be launched by the Commission. Furthermore, during 2016 ENISA will prepare a set of recommendations on aligning research programmes with policy in the area of NIS.

4.1.1 WPK1.1. Improving the expertise related to critical information infrastructures

Desired impact

- By 2017, national authorities in at least five MS use ENISA's recommendations on smart cars and intelligent road systems.
- By 2017, national authorities in at least five MS use ENISA's recommendations on smart health devices, services and infrastructures.
- By 2017, national authorities in at least five MS use ENISA's recommendations on smart airports.

Description of tasks

In this WPK ENISA aims to develop good practices on emerging smart critical infrastructures and services using the concept of the internet of things (IoT) to deliver new, innovative business models and services.

The reports will provide smart critical information infrastructure and service providers and developers with good security and resilience practices when designing, developing and deploying such services in order to minimise the exposure of such network and services to all relevant cyberthreat categories. This builds on previous work of ENISA in the area of smart cities (WP 2015), smart grids (WP 2012-2015) and intelligent transportation systems (WP 2015).

The main areas of work of this WPK are as follows.

- Smart cars and intelligent road systems (not including public transportation means). ENISA, in cooperation with national competent authorities, will identify smart car and vehicle manufacturers and operators and will take stock of cybersecurity risks and challenges introduced by the use of IoT. The Agency will then develop good practices for private and public stakeholders (e.g. national competent authorities).
- Smart health services and infrastructures. ENISA will identify e-health critical service providers (e.g. hospitals, e-health cloud providers, insurance companies, smart laboratories) and will take stock of major cybersecurity risks and challenges introduced by the use of IoT. The Agency will then develop good practices for both private as well as public stakeholders (e.g. national competent authorities).
- Smart airports including supply chain integrity. ENISA will identify major airports that develop and operate smart services and take stock of the security challenges arising from the usage of these services. The Agency will then develop good practices for airports and relevant public authorities that address these challenges.
- These emerging areas are selected based on their criticality for citizens and the economy. The Agency expects these particular sectors and services to benefit the most from the wide adoption of IoT and machine to machine (M2M) technologies. The early adoption of these good practices will boost trust and confidence of potential users of such infrastructures and pave the way for the wide deployment of them. In this way ENISA will help EU industry to become more competitive and innovative.

For each area ENISA will identify all relevant public and private stakeholders, engage them in working groups and jointly take stock of and analyse the current situation in terms of cybersecurity and resilience giving emphasis on communication security. The Agency will also identify EU and national-funded projects in the area of IoT and M2M communication, liaise with them, analyse their findings and deliverables, and further engage them in corresponding expert groups. Special emphasis will be given to the resilience and robustness of such smart critical information infrastructure and services.

Based on the consultation with stakeholders and desktop analysis and research, ENISA will develop good practices and propose baseline security requirements targeted at EU and national policymakers, operators and manufacturers.

Outcomes and deadlines

D1: Good practices on the security and resilience of smart cars and intelligent road systems (report and a workshop, Q4, 2016).
D2: Good practices on the security and resilience of smart health services and infrastructures (report and a workshop, Q4, 2016).
D3: Good practices on the security and resilience of smart airports (report and a workshop, Q4, 2016).

Stakeholder impact

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

Legal base and policy context

- ENISA regulation Article 3, in particular 3.1.(c) (ii) and (iii) on promoting and sharing best practice, Article 3.4 on independent conclusions, guidance and advice.
- CIIP action plan 2009 and 2011.
- Digital agenda 2010.
- European strategy for cybersecurity.
- Cloud computing strategy.
- Council Resolution of 18 December 2009 on a collaborative European approach to network and information security (2009/C 321/01).
- Internal security strategy for the European Union.
- Commission communication — 'Smart grids: from innovation to deployment', COM(2011) 202 final of 12 April 2011.
- EC Recommendations on preparations for the roll-out of smart metering systems.

4.1.2 WPK1.2. Network and information security threats landscape analysis

Desired impact

- In 2016 at least 15 companies and five Member States participate in the ENISA stakeholder groups established to perform the work.
- By 2017 produced results are referenced by at least 500 stakeholders in the area of threat/risk assessment.
- By 2017 produced results are downloaded by at least 10 000 individuals.

Description of tasks

Objectives:

- To develop the current cyberthreat landscape.
- Collect, collate and analyse existing publicly available material on threats, risks, trends and emerging technologies application areas.
- Build synergies with and seeking input from the computer emergency response team for the EU institutions, bodies and agencies (CERT-EU), EU institutions, national bodies, industry and agencies.
- Liaise with experts/organisations to conduct detailed threat assessments in specific sectors/areas. Deliver information that can be fed to other upcoming initiatives, for example in the areas of research, standardisation, etc.

- Further enhance ENISA capabilities in information collection, analysis and dissemination by adopting practices that are (partially) tool-based. This will allow ENISA to import/export available data.
- Achieve a more complete coverage of the threat analysis life-cycle by adding additional elements such as attack vectors or classification schemes for cyberthreats (i.e. taxonomies).
- Develop practical, scenario-based advice on how threat information can flow into risk assessments.

The main goal of this WPK is to provide a comprehensive compilation of cyberthreats based on publicly available information. This is being done by means of top threats that are assessed by analysing collected information. Threat information contains strategic and tactical information on threats and it gives references to detailed documents describing the cyberthreat. Moreover, it provides information on threat agents. Threat information is then extrapolated to emerging technology areas. Based on some assessed/assumed vulnerabilities in those areas, we provide possible threat exposure data for those areas.

Another module within this WPK is the performance of dedicated assessments in some areas of particular interest to our stakeholders, usually with an emerging character. In the past years, for example, ENISA has performed assessments in the areas of smart grids, smart homes and internet infrastructure. With this kind of work we show the exposure of assets from one sector to cyberthreats. We then analyse existing good practices and show how this exposure can be reduced, while we identify gaps in existing practices.

All the types of information provided aim to support decision-makers in all kind of organisations to understand the threat landscape and to make informed decisions regarding cybersecurity. Another target group are security professionals who wish to be informed about the threat landscape and who are interested in having a neutral yet comprehensive list of cyberthreats together with relevant publications/resources.

In 2016, ENISA would like to expand the scope of the threat landscape to include information on attack vectors and also to provide useful information on various classification schemes for threat-related information (taxonomies). Moreover, ENISA would like to provide information on how cyberthreats target assets and what practices are available to protect these assets. This information will be derived from the specific sector assessments and other relevant ENISA activities and will be made public to interested organisations/individuals. Finally, more effective dissemination methods, eventually using a specialised web portal will be accounted for.

Outcomes and deadlines

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

D1: Annual threat analysis/landscape report (Q4, 2016).
D2: Assessments on two key technology/application areas (governments, small to medium-sized enterprises (SMEs), etc.) (Q4, 2016).

Stakeholder impact

The ENISA threat landscape is a document used by Member States and security experts worldwide to assess their exposure to threats and/or risks.

The primary beneficiaries of this WPK will be policymakers, organisations from the public and private sectors, but also NIS security experts who will receive integrated and consolidated information about the European NIS threat landscape and how it is evolving.

- Public and private organisations: other MS agencies, EC3, various governmental agencies.
- EU Commission: Directorate-General (DG) Communications Networks, Content and Technology, DG Informatics and DG Internal market, Industry, Entrepreneurhip and SMEs. .
- NIS experts: various experts willing to receive consolidated information about cyberthreats, cyberthreat agents, attack patterns and emerging trends.

- Power users, SMEs.

Public and private organisations may capitalise on the ENISA output to propose innovative R & D activities, input ENISA information into their own decision support and assessment processes. This will facilitate the development of secure products or services.

Detailed assessments help organisations to understand threat exposure within a specific sector/area. Moreover, it provides information on available good practices to mitigate resulting risks.

Legal base and policy context

- ENISA regulation, Article 3, particularly 3.1.(b).(i) and 3.1.(c).(v).
- The cybersecurity strategy of the EU.
- The proposal for NIS directive and digital agenda.

4.1.3 WPK1.3. Research and development, innovation

Desired impact

- At least 10 experts from the community to participate in the validation of the results of the studies.
- At least five independent high-level experts from the cryptography field to participate in the quality review and the panel for the cryptographic challenges.
- At least 50 individuals/teams participate in the cryptographic challenges.
- At least six research experts and networking experts from industry to contribute to the study on security aspects of virtualisation.

Description of tasks

ENISA will launch in 2016 a new activity, the cryptographic challenges, where the Agency will present to the public a set of cryptographic problems which can be solved by applying cryptanalysis techniques and analytical skills. The aim of this activity is to increase the interest and outreach of cryptography research in Europe, at all educational levels, by providing incentives in this area. The winner of each challenge will be the first contestant(s) to submit the correct solution to ENISA and will be awarded a symbolic prize by the Agency.

In order to ensure the quality of the questions, as well as the appeal to the audience, ENISA will be supported in the elaboration of the different challenges by renowned cryptographers, who will also take part in the panel assessing the correctness of the responses. In addition, and with the goal of expanding the target audience, the challenges will be divided into several categories with different levels of difficulty, aimed at secondary students, university graduates and cryptography researchers and practitioners. Participation will be open to any individual or team across Europe.

As was the case in previous years, ENISA will continue to support the Commission by providing experts in the evaluations of the calls for proposals which are published in the context of EU-funded R & D programmes. In this context, emphasis will be given to the areas which are important to the ENISA WP as presented in this document. It should be envisaged that ENISA may contribute up to two experts for the evaluation of calls for proposals during 2016.

Additionally, ENISA will prepare a set of recommendations in 2016 on aligning research programmes with policy in the specialised area of NIS. Although there is state-of-the-art research in Europe in the field of NIS, and this area is extensively supported by European-funded programmes, research is usually not focused on the aspects where NIS policies need available technologies to move forward on their implementation. ENISA will address both the research and policy communities in order to find means to improve coordination and to facilitate good support for policy areas that rely on a technological base.

Finally, in the context of the ENISA activities supporting research and innovation in security topics, the agency will tackle the subject of virtualisation in 2016. Virtualisation is a concept where there is an abstraction of the physical layers of information and communications technology (ICT) components and virtual versions are created in logical layers. It can be applied to hardware, operating systems, data, networks, etc. One of the concerns regarding virtualisation is its security aspects, namely if vulnerabilities could lead to a breach in the logical separation of components. However, virtualisation is reaching a very high deployment rate nowadays; therefore more research should be done on how virtualisation can be implemented with adequate levels of security.

In order to support the R & D in this area, ENISA will prepare a study on the security aspects of virtualisation. The study will analyse virtualisation from an ample perspective: hardware virtualisation (local virtual machines), desktop virtualisation (thin clients), application virtualisation (remote desktop services), etc. The report will collect existing work on this area, propose security best practices and identify gaps that need to be covered by further research. Furthermore, the study will focus on best practices on how to provide security by default to virtualised systems by addressing possible risk scenarios for these kind of architectures. This will support the decision-making process regarding how to optimise the cost of implementing virtualised systems.

Outcomes and deadlines

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

D1: ENISA cryptographic challenges (Q3, 2016).
D2: Recommendations on aligning research programme with policy in the specialised area of NIS (Q4, 2016).
D3: Study on security aspects of virtualisation (Q4, 2016).

Stakeholder impact

The direct beneficiaries of the results of this WPK will be the policymakers, framework programmes of EU-funded R & D, standardisation bodies and the end-user organisations from public and private sectors, in particular in the areas listed below.

- Standardisation related to NIS, privacy, cloud computing and smart grids.
- Harmonisation of EU-funded research and policy initiatives.
- Academic and industry research in networking innovations.

Legal base and policy context

- ENISA regulation, Article 3, particularly 3.1.(d).(ii).
- Council Resolution of 18 December 2009 on a collaborative European approach to network and information security (2009/C 321/01).
- European Committee for Standardisation (CEN)/European Committee for Electrotechnical Standardisation (Cenelec)/European Telecommunications Standards Institute (ETSI) CEN-Cenelec cybersecurity coordination group (CSCG) White Paper No 01 *Recommendations for a strategy on European cybersecurity standardisation*.

4.2 SO2. To assist the Member States and the European Union institutions and bodies in enhancing capacity building throughout the European Union

SO2 is design to provide assistance to MS and EU institutions and bodies, as well as the private sector by supporting NIS enhancement of capacity building through the EU. ENISA will work together with Member States and EU institutions to assist them in capacity building across the EU. In particular, the Agency will work together with all relevant stakeholders to ensure that the approach is coherent across the EU.

List of work packages and short description

- **WPK2.1. Assist Member States' capacity building**

One of the main goals of this work package (WPK) is to develop and improve the activities related to the operational security support programme. In 2016, ENISA will build upon its work in operational security area, and will update the impact assessment related to this area to concisely draw 'lessons learned' via a dialogue with relevant stakeholders, and to adjust the activities for the coming years.

Another main goal of this WPK is to help the EU Member States and other ENISA stakeholders, such as the EU institutions, bodies and agencies, to develop and extend the necessary capabilities in order to meet the ever-growing challenges to secure their networks.

- **WPK2.2. Support EU institutions' capacity building**

In this WPK ENISA aims to enhance the dialogue among EU institutions and support them in reinforcing their NIS capacity building. The Agency will also improve the mechanism to provide key stakeholders with timely and high-quality responses to NIS developments.

- **WPK2.3. Assist private sector capacity building**

One of the main obstacles for the implementation of wide and effective cybersecurity programmes in organisations is the lack of a common language among managers and technical staff, which makes it difficult for the later to transmit the current security scenario to the former. ENISA will look at best practices in Member States on how to reach the private sector in order to increase cybersecurity awareness and skills; as well as to promote a culture of cybersecurity.

The agency will gather information on successful experiences conducted in MS directed specifically to the private sector such as awareness campaigns, reference materials, web portals, etc.

- **WPK2.4. Assist in improving the general awareness**

Building on the work of WP 2015, in 2016 ENISA will move towards the implementation of the 2015 recommendations to address opportunities for the distance-learning delivery of NIS modules to large audiences. The approach under this WPK is to leverage existing material (courses) instead of developing new material (which is outside the scope and resources of the Agency.

In recent years, the European Cyber Security Month (ECSM) has expanded its outreach with numerous activities in the Member States, reaching a large number of European citizens. ENISA will continue to coordinate the ECSM in 2016.

Additionally, and in order to promote capacity building among the security community, ENISA will launch a competition in 2016, in the form a 'capture the flag' challenge, named the 'ENISA cyber challenge'. Its goal is to increase the interest in NIS by promoting excellence in the form of competitions, as well as to gather feedback on the areas of interest for the communities.

4.2.1 WPK2.1. Assist Member States' capacity building

4.2.1.1 WPK2.1.A. Assistance in the area of operational security and NIS operational training

Desired impact

- Support Member States in enhancing their national and governmental CSIRT baseline capabilities.
- Continued CSIRT services training will be provided to a minimum of 20 participants of different organisations in five Member States.
- Improved operational practices of CSIRTs in at least 15 Member States (ongoing support with best practices development).

Description of tasks

Objectives

- Facilitate voluntary information sharing techniques to enhance quality of collection.
- Extend mutual interactions with stakeholders in MS-wide area for incident response collaboration.
- Build upon successful work in the area of 'training methodologies and impact assessment'.
- Update training material for operational communities (e.g. CSIRTs).
- Develop new sets of training for NIS.
- Further develop and apply ENISA recommendations for baseline capabilities.
- Provide technical training for MS and EU bodies.

One of the main goals of this WPK is to perform sustainable research, development and improvement of activities related to the multiannual development for the operational security support programme.

In 2016, ENISA will update the training methodologies and 'baseline capabilities' report. The goal is to concisely draw 'lessons learned' via a dialogue with relevant stakeholders, and to reflect constantly developing CSIRT activities for the coming years.

Another main goal of this WPK is to help the EU Member States and other ENISA stakeholders, such as the EU institutions, bodies and agencies, to develop and extend the necessary capabilities in order to meet the ever-growing challenges to secure their networks.

Most of the activities in this WPK target maintaining and extending the collection of good practice guidelines in various areas of operational-capability building. In addition, ENISA will continue supporting Member States in enhancing their national and governmental CSIRT capabilities.

A special emphasis in this WPK is put on supporting operational bodies and communities (namely CSIRTs, but other communities where appropriate) via concrete advice (such as good practice material) and concrete actions (such as CSIRT training).

Outcomes and deadlines

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

D2: Follow-up/extension of the training methodologies work from 2014/15 (Q4, 2016).
D3: Update of existing training material (Q4, 2016).
D4: Development of a set of new training material (Q4, 2016).
D5: On-request training for MS and EU bodies (Q4, 2016).
D6: Good practice in incident tracking and taxonomy (Q4, 2016).
D7: Annual update of baseline capabilities (report) (Q4, 2016).

Stakeholder impact

- The Commission will obtain an expert opinion for current and future policy efforts in the incident response field.
- The agency will obtain an input for the future actions for operational community programme.
- Beneficiaries of this WPK will be the organisations and institutions responsible for cybersecurity incident response in both the public and private sectors; they will be able to obtain consolidated good practice material and training information or on-site training for cybersecurity operations.

Legal base and policy context

- ENISA regulation, Article 3, particularly 3.1.(b) and 3.1.(c).
- Proposed NIS directive.

4.2.1.2 WPK2.1.B. Assistance in the area of cybersecurity strategies

Desired impact

- By 2017, 10 Member State use ENISA's good practices on NCSS.
- By 2017, 15 private organisations use ENISA's good practices on NCSS.
- By 2017, 10 Member State use ENISA's good practices on national public-private partnerships (PPPs).
- By 2017, 15 private organisations use ENISA's good practices on national PPPs.

Description of tasks

This work package aims to help the EU MS and other ENISA stakeholders, such as the EU bodies, to develop and extend the necessary capabilities in order to meet the ever-growing challenges of securing their networks, services and information infrastructures.

ENISA will continue assisting EU MS to develop their capabilities in the area of NCSS. The Agency, building on previous years' work in this area, will assist MS to deploy its existing good practices in this area and offer targeted and focused assistance on specific aspects of NCSS (e.g. on the evaluation of NCSS).

ENISA will also act as a facilitator in this process by bringing together MS and the private sector with varying degrees of experience to discuss and exchange good practices, share lessons learned and identify challenges and possible solutions. Through this interaction with the MS, ENISA will validate and update its existing NCSS good practice guide and the evaluation/assessment framework of NCSS.

Outcomes and deadlines

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

D8: Assist and advise Member States on the establishing and evaluation of NCSS (workshops Q1-Q4, 2016).
D9: Update good practice guide on NCSS (report, Q4, 2016).

Stakeholder impact

- MS will better understand the key issues and challenges before setting up a national NCSS or PPP.
- MS will be able to share experiences and lessons learned with each other and better focus their efforts.
- MS will be able to identify key issues and by deploying ENISA's good practices can be more effective and productive.

Legal base and policy context

- ENISA regulation, in particular Article 3.1.b and 3.1.c on capacity building and cooperation and Article 3.4 on independent conclusions, guidance and advice.
- Council Resolution of 18 December 2009 on a collaborative European approach to network and information security (2009/C 321/01).
- Commission communication on critical information infrastructure protection, 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience', COM(2009) 149 final of 30 March 2009. (Especially sections 3.4.3, 5.1, 5.2 and 5.3.)
- Commission communication — 'A digital agenda for Europe', COM(2010) 245 final of 19 May 2010.
- Commission communication — 'The EU internal security strategy in action: Five steps towards a more secure Europe', COM(2010) 673 final of 22 November 2010.
- Commission communication on critical information infrastructure protection, 'Achievements and next steps: towards global cyber-security' COM(2011) 163 final of 31 March 2011.

4.2.1.3 WPK2.1.C. Assistance in the area of privacy and trust

Desired impact

- At least five data protection authorities (DPA) and 10 large EU data controllers to use the personal data breaches severity assessment tool.

Description of tasks

ENISA will support Member States in their own decision-making process, by providing advice and referencing the appropriate ENISA studies in the area of privacy and trust. This will be done on an on-demand basis. The agency will focus on providing appropriate tools that facilitate Member State implementation of the provisions set out in the trust Services regulation and the proposed data protection regulation. These activities will be conducted, as in previous years, in close collaboration with the supervisory bodies of the MS

Specifically, in the area of personal data breaches, ENISA will continue to enhance and promote the adoption of the data breach severity assessment tool the Agency developed in 2015. This tool, which has been implemented in close collaboration with several Member State DPAs, aims to provide a coherent framework for assessing data breach severity across EU MS. In 2016, ENISA will continue to support DPAs to adopt the proposed tool and to perform impact assessment exercises on various breach scenarios.

Outcomes and deadlines

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

D11: On-request support for MS decision-making in the areas of privacy and trust (Q4, 2016).

Stakeholder impact

The direct beneficiaries of the results of this work will be the MS DPA and Article 29 Working Party, which will receive advice and a series of proposed tools aimed to support them in the implementation of the European regulations in the areas of privacy and trust. These activities will also facilitate the harmonised adoption of the European regulatory framework in these fields.

Legal base and policy context

- ENISA regulation, Article 3, particularly 3.1.(b).(i) and 3.1.(c).(v).
- Cybersecurity strategy of the European Union.
- Data protection directive 95/46/EC.
- Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications.
- Proposal for a general data protection regulation.

4.2.2 WPK2.2. Support European Union institutions' capacity building

4.2.2.1 WPK2.2.A. Information notes on NIS: production and review mechanisms ("info notes")

Desired impact

- In 2017 improve information flows regarding NIS issues between the EU institutions.
- In 2017 improved mechanism for producing and distributing of info notes.
- At least two EU bodies and five public stakeholders will receive the timely information on NIS incidents and significant developments in the field.

Description of tasks

Objectives

- Improve the mechanism that will allow the Agency to provide timely and high-quality responses to NIS developments.
- Timely information provided to key stakeholders on NIS incidents and on significant developments in the field.

In the case of NIS issues and occurrences that reach a certain level of public and media attention it is crucial that the Agency, where appropriate in collaboration with EU institutions and bodies, e.g. CERT-EU, provide a more balanced set of information about the issues and occurrences. This is why ENISA will

continue to provide high-quality responses to NIS developments. Based on the practice and experience in 2014 and 2015, the Agency will review and adjust the mechanism for preparing and producing info notes.

ENISA's intention is to continue providing info notes in a timely manner as a reliable and continuous service to its stakeholders. The overall goal for each note should be to highlight fundamental facts and the shortcomings behind specific NIS issues and occurrences, concentrating on how such shortcomings can be addressed by improvements to processes and infrastructure, in order to give advice to its key stakeholders (in accordance with the Agency mandate) and to provide an independent and 'calm' opinion. Notes will only be made public if the topic is not an ongoing incident, and if the note is based on public information.

Outcomes and deadlines

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

D1: Review and adjust mechanism for production of info notes (Q1-4, 2016).
D2: Restricted and public info notes on NIS (Q1-Q4, 2016).

Stakeholder impact

- Improved collaboration with EU bodies (e.g. CERT-EU) concerning timely and high-quality info notes on NIS incidents and significant developments in the field.
- Timely information provided to key stakeholders on NIS incidents and on significant developments in the field.

Legal base and policy context

- ENISA regulation, Article 3, particularly 3.1.(b) and 3.1.(c).

4.2.2.2 WPK.2.2.B. Reinforcement of the NIS of Union institutions, bodies and agencies

Desired impact

- ENISA's expertise regarding the MS NIS capacity development is also to be offered to EU institutions, agencies and bodies (hereinafter: 'EU institutions'), in cooperation with CERT-EU.
- Enhanced knowledge of EU institutions regulations, policies, procedures related to their NIS.
- Identification of well-functioning practices that could be disseminated to all or relevant EU institutions, as well as information concerning critical weaknesses that should be addressed.
- Identification of future actions that ENISA could initiate in order to further reinforce the NIS of EU institutions.

Description of tasks

In this WPK ENISA aims to enhance the dialogue among European institutions and support them in reinforcing their NIS.

In 2016, concrete actions are planned.

- Identifying and liaising with all relevant stakeholders within European institutions and bodies.
- In cooperation with all relevant European institutions and bodies, taking stock of and initiating an analysis of all existing regulations, policies, procedures and practices of all EU institutions related to their NIS.

Through stocktaking and analysis, ENISA will identify overlaps and gaps between all these regulations and policies. These findings could also be discussed with all relevant stakeholders from EU bodies, EU MS and even the private sector. That might pave the way for a permanent strategic dialogue among all European institutions and bodies on the future of NIS policy in the EU.

This dialogue will result in important recommendations that would allow the simplification of policies, reduction of overlaps, identification of synergies, creation of awareness about NIS challenges and even proposals for new actions to address identified gaps. That would help European institutions and bodies to better focus their efforts and properly use their resources to meet the needs of EU MS and the private sector. ENISA is liaising and will continue to liaise, for this purpose with CERT-EU, the incident response team for the EU institutions. The expertise of CERT-EU on the reactive dimension of NIS of the EU Institutions will strongly benefit this process.

Considering the sensitiveness of the information that ENISA might be provided with by European institutions, deliverables will be restricted in distribution.

Building on this work ENISA will address in future work programmes the setting-up of a European institution NIS contingency plan, the organisation of dedicated EU institution cyber incidents exercises, and the launch of awareness-raising initiatives.

Outcomes and deadlines

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

D3: Restricted. Upon request, support the assessment of existing policies/procedures/practices on NIS within EU institutions (workshop, meetings, Q1-4, 2016).

Stakeholder impact

Dialogue among EU institutions on their NIS will be facilitated. EU institutions and bodies will:

- further benefit from each other's best practices on NIS.
- obtain insight and expert advice on how to reinforce their NIS.
- benefit from the establishment of cooperation between CERT-EU and ENISA.
- obtain insight and expert opinion on NIS field.
- better understand the synergies between existing policies, regulations and procedures.
- better understand the overlaps between existing policies, regulations and procedures.
- better understand how to address gaps in existing policies, regulations and procedures.

Legal base and policy context

- According to Article 3(b)iii of ENISA's 2013 regulation, the Agency shall […] assist the EU institutions, bodies, offices and agencies in their efforts to develop the prevention, detection and analysis of and the capability to respond to NIS problems and incidents, in particular by supporting the operation of a computer emergency response team […] for them.
- In its conclusions on the European cybersecurity strategy (11357/13 of 21 June 2013), the Council called upon all EU institutions, in cooperation with ENISA, to take the necessary actions to ensure their own cybersecurity, by reinforcing their NIS according to the appropriate standards.

4.2.3 WPK2.3. Assist private sector capacity building

Desired impact

- At least five MS and five private sector stakeholders contribute to the production of the guidelines for MS to reach the private sector through cybersecurity awareness dissemination activities.
- At least 15 private sector stakeholders coming from different MS, sectors of activity and size participate in the elaboration of the recommendations for ICT security staff on improving management level cybersecurity awareness.

Description of tasks

ENISA will look at best practices in Member States on how to reach the private sector in order to increase cybersecurity awareness and skills; as well as to promote a culture of cybersecurity. The agency will gather

information on successful experiences conducted in MS such as awareness campaigns, reference materials, web portals, etc.

The agency will focus on recommendations on how to improve cybersecurity awareness at the management level. Indeed, one of the main obstacles for the implementation of wide and effective cybersecurity programmes in organisations is that there is a lack of a common language among managers and technical staff, which makes it difficult for the later to transmit the current security scenario to the former.

The report will analyse how to tackle and overcome this culture dialogue issues. By taking stock from exiting guidelines in Member States and international security organisations, the agency will try to support security managers and professionals with references to existing guidelines on how to engage the senior level support for cybersecurity. The agency will propose best practices focusing exclusively in areas where existing gaps in reference materials have been detected.

Outcomes and deadlines

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

D1: Recommendations for creating a cybersecurity culture and improving management-level cybersecurity awareness (Q4, 2016).

Stakeholder impact

- The direct beneficiaries of the results of this work will be MS and EU companies, from all sectors and sizes, which will receive recommendations on how to improve cybersecurity awareness and create a cybersecurity culture, especially from an organisational level and managerial level.

Legal base and policy context

- ENISA regulation, Article 3, particularly 3.1.(c).(iv) and 3.1.(c).(v).
- ENISA stakeholder strategy.
- Cybersecurity strategy of the European Union (section 2.1).
- Commission communication — 'A digital agenda for Europe', COM(2010) 245 final of 19 May 2010.

4.2.4 WPK2.4. Assist in improving general awareness

Desired impact

- At least 50 individuals from MS participate in the ENISA cyber challenge.
- Representatives from the EU 28 MS and five partner countries participate in ECSM and the release of general NIS messages for citizens.
- At least five international stakeholders collaborate, for better coordination, in the ECSM.
- At least 10 experts from the community participate in reviewing the contents of the citizens' portal.

Description of tasks

Promoting capacity building among the security community, in 2016 ENISA will launch a competition in the form a 'capture the flag' challenge, named 'ENISA cyber challenge'. It will be aimed at university students from technical schools and security practitioners from the industry. Its goal will be to increase the interest in NIS in these communities by promoting excellence in the form of competitions, as well as to gather feedback on the areas of interest for the communities. In order to do so, ENISA will try to achieve large participation among individuals from different MS.

As one of its main activities in the area of improving public awareness, ENISA will continue to coordinate the ECSM. In recent years, the ECSM has expanded its outreach with numerous activities in the Member States, reaching a large number of European citizens. In 2016, the ECSM will be further developed following its basic principles, namely:

- support the multi-stakeholder governance approach,
- encourage common public-private activities,
- assess the impact of activities, optimising and adapting to new challenges.

In addition, ENISA conducted in 2015 a feasibility study and a pilot project for a web portal that allows European citizens to recognise and use tools for online privacy and security. In particular, the portal lists existing up-to-date and trustworthy open source/freeware tools that can be easily applied by non-expert users who wishes to protect themselves online (e.g. in web browsing, email, instant messaging, e-payment systems). To ensure a neutral perspective, tools are selected after the review of an independent panel of experts.

In 2016, ENISA aims to promote the use of technical tools that enhance user privacy and data protection. It does so by publishing relevant content, focusing on specific citizens groups, as well as disseminating relevant information through community portals and online media in order to reach out to more parties. Moreover, effort will be put into supporting users in recognising and selecting privacy tools in cooperation with other relevant stakeholders (DPA, industry, non-governmental organisations (NGOs), etc.).

Outcomes and deadlines

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

D2: ENISA cyber challenge (Q2, 2016).
D3: Provide guidance and support for ECSM (dissemination material, Q4, 2016).
D4: Upgrade the online privacy tools portal and involve privacy experts from different fields (dissemination material, Q4, 2016).

Stakeholder impact

The direct beneficiaries of the results of this work will be EU citizens, targeted by different categories, as well as end-user organisations from public and private sectors (in particular in the area of EU NIS education). These stakeholders are expected to reap the following benefits.

- Develop knowledge and corresponding ICT skills by being part of a best-practice-sharing community.
- Improve and enhance contacts with stakeholders of similar interests and profiles.
- Increase citizens' awareness and governance on privacy when using online tools.

Legal base and policy context

- ENISA regulation, Article 3, particularly 3.1.(c).(iv) and 3.1.(c).(v).
- ENISA stakeholder strategy.
- Cybersecurity strategy of the European Union (Section 2.1).
- Data protection directive 95/46/EC.
- Proposal for a general data protection regulation.

4.3 SO3. To assist the Member States and the European Union institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security

SO3 provides the framework for ENISA to assist the EU MS and the EU institutions in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security (NIS).

List of work packages and short description

- **WPK3.1. Supporting EU policy development**

The key objective of this work package (WPK) will be for ENISA to proactively contribute to the development of existing or new EU policy initiatives (before they are launched) and assists the Commission, Member States and the private sector in the implementation of existing policies in this area.

ENISA will achieve this objective by engaging with public and private stakeholders and leveraging its existing knowledge and expertise in the area of secure infrastructure and services.

Another key objective of this WPK is cybersecurity standardisation. From its creation, ENISA has tracked the development of standards in the area of NIS, maintaining close contacts and collaboration with international standardisation organisations. This approach enables ENISA to keep its activities up-to-date with the latest developments as well as informing its stakeholders on new NIS standardisation activities and to flag opportunities and/or risks as they develop.

Furthermore, ENISA will support this area, in cooperation with relevant stakeholders, by developing recommendations for improving NIS in EU standardisation policy, providing guidelines of the possible frameworks that can be adopted in order to achieve a harmonised scheme across MS, as well as setting recommendations for the stakeholders involved.

- **WPK3.2. Supporting EU policy implementation**

This WPK covers activities linked to the implementation of couple of directives and regulations (i.e. activities linked to electronic identification and trust services (eIDAS) regulation, ePprivacy directive and the proposed NIS directive) where ENISA has been assigned a role and responsibilities and where NIS is one of the main goals or means to achieve suitable implementation.

Subject to its adoption, ENISA will cooperate with all EU Member States and the Commission to define the scope of the NIS directive, the actions related to ENISA and the sectors and/or services affected. As a result of this the Agency will then identify all relevant public and private stakeholders (e.g. competent authorities, manufacturers and operators) and engage them in a structured dialogue on the key objectives of the NIS directive and how can be best implemented within each sector and/or service.

ENISA work in the areas of privacy and trust has been ongoing for several years now, and the Agency has extensively contributed to support the implementation of the personal data protection regulatory framework in many of its key technological aspects. ENISA will continue to support the implementation of EC Regulation 611/2013 by providing assistance regarding technical protective measures (appropriate cryptographic protective measures) as the abovementioned regulation requests ENISA to do.

ENISA will continue collecting and analysing annual national reports of security breaches from national regulatory authorities (NRAs) in accordance with Article 13a of the framework directive on electronic communications. The Agency, in cooperation with experts from NRAs and the private sector (e.g. ENISA's e-communications reference group, NIS platform.) will analyse the national reports, compare them with previous years, identify new trends and develop good practices and lessons learned.

Another area covered in this WPK is the support for the implementation of the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.

Trust services are a key enabler for increasing citizens' confidence in online services, and given their nature, they require a high level of security to ensure their integrity and reliability. ENISA has contributed extensively to the area of securing trust services in the past by providing best practices for providers, recommendations on audit schemes, standardisation guidance, security-breach reporting and recommendations, etc. Building on the work of 2015, in 2016 ENISA will focus on the key areas of interest

for stakeholders, where a contribution will be most useful to the community, the topics of assurance levels for electronic identification and security recommendations for relying parties of trust services.

4.3.1 WPK3.1. Supporting European Union policy development

4.3.1.1 WPK3.1.A. Contribution to EU policy linked to secure infrastructures and services

Desired impact

- By 2017, 15 companies and five MS competent authorities contribute to ENISA's efforts in the area of cloud computing.
- By 2017, 15 companies and five MS competent authorities contribute to ENISA's efforts in the area of smart grids and/or ICS-SCADA.
- By 2017, 10 companies and five MS competent authorities contribute to ENISA's efforts in the area of certification of components and systems.
- By 2017, 10 companies and five MS competent authorities contribute to ENISA's efforts in the area of finance.

Description of tasks

In this WPK, ENISA will engage with public and private stakeholders and deploy state-of-the-art recommendations and good practices in secure infrastructure and services with the objective of proactively contributing to the development of existing or new EU policy initiatives (before they are launched) and assist the Commission, Member States and the private sector in the implementation of existing policies in this area.

ENISA will achieve this objective by engaging with public and private stakeholders, by deploying existing expert groups (e.g. the European SCADA and control systems information Exchange (EuroSCSIE)) and by leveraging its existing knowledge and expertise in the area of secure infrastructure and services. One of the key vehicles to deliver this is actually the NIS platform (an EU-level PPP) but also dedicated, area-specific expert groups that develop useful insight, validate good practices and issue practical recommendations. Whenever it is necessary ENISA will liaise with standards bodies to provide its technical opinion on future standards in the areas below.

The main areas covered in this WPK are as follows.

EU cloud computing strategy and partnership

ENISA will continue to play an active role in the implementation of the EU's cloud computing strategy and partnership. The agency will also provide to the Commission and MS technical advice, recommendations and information related to the implementation of the NIS directive especially the part related to cloud computing. In all these areas ENISA will engage with all relevant public and private stakeholders and make sure that these efforts properly align with EU ECP, ETSI and CEN/Cenelec initiatives.

EU smart grids and ICS-SCADA strategy

ENISA will assist the Commission, the Member States and the private sector in the implementation of the EU's smart grid strategy and ICS-SCADA actions. The agency, building on this existing knowledge and expertise, will provide sound technical advice, recommendations and information on good practices in the area of minimum security measures for smart grids and ICS-SCADA, certification of smart grid components, industrial IoT and incident-reporting mechanisms for national critical industries. ENISA will engage with all relevant stakeholders, provide contributions to the Commission on policy initiatives (e.g. EU CSS, DG Energy's expert group 2 (EG2) and Energy expert cybersecurity platform (EECSP), CEN/CENELEC's M490, EuroSCSIE and distributed energy security knowledge (Densek)), and make sure that these efforts properly align with EU's overall smart grid policy.

Policy discussions on the certification of components and systems
ENISA will cooperate with the Commission, Member States and the private sector in order to foster EU policy discussion regarding a European framework for the certification of components and systems. The agency will support the discussion on the evolution of the existing initiatives. Through this, ENISA will be able to provide suggestions to key decision-makers on the way MS and the EU should address this issue.

EU policy on NIS matters of the finance sector
ENISA will continue its efforts in the area of the finance sector. The Agency will assist the Commission, MS competent authorities and the private sector in the definition and implementation of the EU's policy on NIS matters of the finance sector. ENISA, using its knowledge and expertise in this area, will contribute to the third-party payments debate, the risks in inter-banking transactions and secure communications debate, adoption of cloud computing by sector and the harmonisation of audits and policies and others. ENISA will cooperate closely with relevant key stakeholders such as the European Banking Authority (EBA), the European Central Bank (ECB) and leading financial institutions and providers to achieve the goals in this area.

Outcomes and deadlines

D1: Contribute to EU policy in the area of cloud computing (workshops, meetings, Q1-Q4, 2016).
D2: Contribute to EU policy in the area of smart grids and ICS-SCADA (workshops, meetings, Q1-Q4, 2016).
D3: Support the policy discussions in the area of IT security certification (workshops, meetings, Q1-Q4, 2016).
D4: Contribute to EU policy in the area of finance (workshops, meetings, Q1-Q4, 2016).

Stakeholder impact

Cloud computing

- Assist private and public sectors to develop a common policy on cloud computing security (e.g. on service-level agreements (SLAs)).
- Engage the private sector in the EU cloud strategy.

Smart grids and ICS-SCADA

- Providing an indication of a minimum level of security and resilience in the Member States, thereby avoiding the creation of the 'weakest link'.
- Ensuring a minimum level of harmonisation on security and resilience requirements across Member States and thus reducing compliance and operational costs.
- Facilitating the establishing of common preparedness, recovery and response measures and paving the way for mutual aid assistance across operators during crisis.
- Provide guidance to vendors and asset owners on how to manage and then disclose discovered vulnerabilities.
- Support the structured information sharing between vendors and asset owners as regards the vulnerabilities of their products.

Certification in complex ICT environments

- Bring together stakeholders from the certification loop and discuss challenges for better certification practices.
- More-harmonised and better-coordinated certification practices for both the EU and Member States.
- Awareness raising and improved education on certification.

Finance

- Banks would benefit from having an independent analysis and set of guidelines about inter-banking communications and transactions.

- Industry would be able to use a neutral (not vendor-specific) discussion platform with an improved exchange of good security and resilience practices in the area of telecommunications.

Legal base and policy context

- ENISA regulation, Article 3, in particular 3.1.(c) (ii) and (iii) on promoting and sharing best practice, Article 3.4 on independent conclusions, guidance and advice.
- CIIP action plans 2009 and 2011.
- Digital agenda 2010.
- European strategy for cybersecurity.
- Cloud computing strategy.
- Council Resolution of 18 December 2009 on a collaborative European approach to network and information security (2009/C 321/01).
- Internal security strategy for the European Union.
- Commission communication — 'Smart grids: from innovation to deployment', COM(2011) 202 final of 12 April 2011.
- Commission recommendations on preparations for the roll-out of smart metering systems.

4.3.1.2 WPK3.1.B. Policy development and standards

Desired impact

- At least six stakeholders from policymakers, industry and research experts in NIS standardisation to contribute in ENISA's recommendations for improving NIS in EU standardisation policy.

Description of tasks

The new ENISA mandate gives the Agency a more proactive role in the area of standardisation. The task assigned to ENISA by the new regulation is to support standardisation by facilitating the establishment and take-up of European and international standards for risk management and for the security of electronic products, networks and services. A key element towards the objective of improved security standardisation is to facilitate close collaboration between policymakers, standardisation organisations and industry. ENISA will facilitate the cooperation of stakeholders by engaging policymakers, standardisation organisations and industry, with the aim of putting forward common strategies to enhance NIS in EU standardisation policy.

Since 2012 ENISA has specifically participated in the creation and further work of the ETSI CEN-CENELEC Cyber Security Coordination Group (CSCG). This will continue in 2016 and ENISA will collaborate in the activities of the CSCG and try to further exploit synergies between the CSCG and its WP. The Agency will also involve standards bodies in the different WPKs in as far as this is appropriate.

Furthermore, in order to enhance cooperation in this area among the different stakeholders, in 2015 ENISA conducted a conference to align policymakers, industry and research experts in steering cybersecurity standardisation. Based on the input from the participating experts and the ongoing collaboration with the CSCG, ENISA will further develop the work done in 2015.

In 2016 the Agency will provide recommendations for improving NIS in EU standardisation policy and guidelines on the possible frameworks that can be adopted in order to achieve a harmonised scheme across MS.

Outcomes and deadlines

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

D5: Recommendations for improving NIS in EU standardisation policy (Q4, 2016).

Stakeholder impact

The direct beneficiaries of the results of this WPK will be the policymakers, framework programmes of EU-funded R & D, standardisation bodies and end-user organisations from the public and private sectors, in particular in the areas of standardisation related to NIS, privacy, cloud computing and smart grids.

Legal base and policy context

- ENISA regulation, Article 3, particularly 3.1.(d).(i) and 3.1.(d).(ii).
- Council Resolution of 18 December 2009 on a collaborative European approach to network and information security (2009/C 321/01).
- CEN/Cenelec/ETSI CSCG White Paper No 01 Recommendations for a strategy on European cybersecurity standardisation.

4.3.1.3 WPK3.1.C. Towards a digital single market for NIS and related IT products and services

Desired impact

- EU and national policymakers understand how the strengths and weaknesses of the NIS and related IT sector in Europe.
- EU and national policymakers understand how to develop a digital single market (DSM) for NIS and related products and services.

Description of tasks

The aim of this WPK is to analyse how the NIS and related IT sectors can play a decisive role in a DSM at EU level. ENISA will take stock of different market segments in the NIS and related IT areas and identify key European players having a major market role in products, services or infrastructures.

This task should help ENISA to advise the Commission and Member States to better identify where efforts should be placed in order to further support European NIS and related ICT industries and services in order to achieve and improve the adequate level of diversity and trust in the EU.

The agency will form an expert group with senior experts from these private sector stakeholders and selected experts from MS and the Commission to assess the technical competitive advantage of Europe in the area of NIS and provide insight on how Europe could become a sustainable market player in NIS and related IT products and/or services without setting up trade barriers or using other protectionist measures. Particular attention will be given to the DSM initiative of the Commission and its outcomes.

The Agency will then develop useful recommendations on how Europe can support the DSM for NIS and identify the areas and means to foster further actions.

Outcomes and deadlines

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

D6: Restricted. Towards a DSM for NIS products and services (workshop, report, Q4, 2016).

Stakeholder impact

- EU and national policymakers understand the strengths and weaknesses of the NIS sector in Europe.
- EU and national policymakers understand how to develop a DSM for NIS products and services.

Legal base and policy context

- ENISA regulation Article 3, in particular 3.1.(c) (ii) and (iii) on promoting and sharing best practice, 3.1 (d) and Article 3.4 on independent conclusions, guidance and advice.
- DSM strategy.

4.3.2 WPK3.2. Supporting European Union policy implementation

4.3.2.1 WPK3.2.A. Assist EU MS and Commission in the implementation of the NIS directive

Desired impact

- By 2017, 10 MS contribute to ENISA's efforts for harmonised implementation of the NIS directive.
- By 2017, 20 major private organisations contribute to ENISA's efforts for harmonised implementation of the NIS directive.
- By 2018, five MS deploy ENISA's guidelines on NIS directive in a 3 sectors/services.
- By 2018, 10 private organisations deploy ENISA's guidelines on NIS directive in a 3 sectors/services.

Description of tasks

This work package aims to help EU MS, the private sector and the Commission to implement the NIS directive.

More specifically ENISA will assist the Commission and MS in the establishment of the Cooperation Group envisaged in the NIS Directive. The Agency, as a member of this group, will provide ideas to the Commission and MS about its governance structure, its objectives and themes to focus on as well as its working relationship to the CSIRT Network.

DSPs

ENISA will also assist the Commission and MS in the development of the Implementing Acts envisaged in the NIS Directive on incident reporting schemes imposed on Digital Service Providers (DSPs).

More specifically ENISA will take stock of similar provisions, processes, laws and regulations (obligatory or voluntary) in MS and analyse them in order to identify commonalities. Emphasis will be given on identifying the parameters determining the impact of an incident which will trigger the notification (Art 15 a (2) in conjunction with Art 15 a (4a)). Also the Agency will discuss with private sector about their practices and relate them with the findings found in the public sector.

ENISA will do its utmost to achieve consistency and alignment among the different implementation approaches by synthesising the different views.

The Agency will then provide to the Commission and MS advice on how such a scheme can be best implemented in the context of these implementing acts and any other related future action. By doing this we hope to develop an easy, consistent and affordable implementation scheme across the different DSP sectors.

In addition ENISA will also assist the Commission and MS in the development of the Implementing Acts related to security measures imposed on Digital Service Providers (DSPs).

In that respect the Agency will take stock of and analyse all existing national (e.g. UK: Cyber Essential), EU and international cybersecurity frameworks and requirements imposed on or deployed by DSPs. The Agency will then identify good practices and propose to the Commission and MS advice on security requirements for DSPs to be considered in the relevant implementing acts.

Essential services

Moreover, if called upon to do so, ENISA will assist MS in their efforts to identify operators of essential services. That would be fully in line with the role envisaged for ENISA in the NIS Directive and fully respecting the role and competences of Member States.

In that respect ENISA will start collecting well established approaches different MS use to identify their operators of essential services. The Agency will analyse the different approaches in use and try to identify commonalities that could constitute a basis for a harmonised approach. If agreed by the MS, this work is not expected to conclude in 2016 but will continue in 2017 and 2018. During this period ENISA will continue helping MS to develop more knowledge and expertise on this topic and will contribute in the discussions towards an aligned EU approach, if possible. That would allow operators of essential services operating across several MS to be treated in a seamless and consistent way.

In this effort ENISA will leverage its existing knowledge and expertise in stakeholder engagement with the public and/or the private sector. The agency will also deploy its existing stakeholder communities such as the NIS platform, existing national PPPs and other expert groups established by ENISA and others in different sectors. ENISA will also capitalise on its domain knowledge and expertise in the DSP sectors and try to reuse already developed good practices and recommendations.

Outcomes and deadlines

D1: Contribute to the establishment of the cooperation group (meetings, workshops, Q2-Q4, 2016)
D2: Advice on the implementation of mandatory incident reporting for DSPs – input to the Implementation Acts (report, workshop, Q4, 2016).
D3. Advice on the implementation of security requirements for DSPs – input to the Implementation Acts (report, workshop, Q4, 2016)
D4: Assist MS in the identification of operators of essential services (workshop, Q2-Q4, 2016)

Stakeholder impact

- MS, the Commission and the private sector will better understand how to implement the NIS directive, which are the key issues and challenges to consider in order to achieve harmonised implementation across sectors.
- MS and private sector will debate the implementation of the NIS directive and jointly develop possible solutions that would pave the way for harmonised implementation.
- MS and private sector can better understand how to use existing ENISA's work in this area to quicker implement the NIS directive.

Legal base and policy context

- ENISA regulation Article 3, in particular 3.1.(c) (ii) and (iii) on promoting and sharing best practice, Article 3.4 on independent conclusions, guidance and advice.
- Council Resolution of 18 December 2009 on a collaborative European approach to network and information security (2009/C 321/01).
- Commission communication on critical information infrastructure protection, 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience', COM(2009) 149 final of 30 March 2009. (Especially sections 3.4.3, 5.1, 5.2 and 5.3.)
- Commission communication — 'A digital agenda for Europe', COM(2010) 245 final of 19 May 2010. (Especially section 2.3.)
- Commission communication — 'The EU internal security strategy in action: Five steps towards a more secure Europe', COM(2010) 673 final of 22 November 2010. (Especially objective 3.)
- Commission communication on critical information infrastructure protection, 'Achievements and next steps: towards global cyber-security' COM(2011) 163 final of 31 March 2011.
- European Council — 'The Stockholm Programme — An open and secure Europe serving and protecting citizens' (2010/C 115/01). (For example, sections 2.5. 'Protecting citizen's rights in the information society', 4.2.3. 'Mobilising the necessary technological tools', and 4.4.4. 'Cybercrime').

- Commission communication — 'Towards a general policy on the fight against cybercrime', COM(2007) 267 final of 22 May 2007.

4.3.2.2 WPK3.2.B. Assistance in the implementation of NIS measures of EU data protection regulation

Desired impact

- At least five representatives from different MS contributing to ENISA guidelines and best practice recommendations regarding technological measures to protect privacy and trust and privacy-enhancing technologies (PETs), at least 10 actors in the field validating the results of the studies.
- At least six experts from the health sector and DPA to contribute on the study on online and mobile applications, and six stakeholders to validate the results of the study.
- More than 80 participants in Annual Privacy Forum (APF) 16: (researchers, policymakers and industry participants).
- At least six stakeholders from policymakers, industry security practitioners and data controllers to contribute to the study on guidelines for data controllers on securing the automated processing of personal data, and six stakeholders to validate the results of the study.

Description of tasks

ENISA work on the areas of privacy and trust has been ongoing for several years now, and the Agency has contributed extensively to assist the implementation of the personal data protection regulatory framework in many of its key technological aspects. As an example of this support, the Commission published in 2013 the Regulation 611/2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications. Article 4(3) of the regulation sets out that the Commission will publish an indicative list of appropriate technological protection measures which shall render the data unintelligible to any person who is not authorised to access it, after consultation with the Article 29 Working Party, ENISA and the European Data Protection Supervisor (EDPS).

As a core activity in supporting the protection of personal information, ENISA provided recommendations on technological measures to protect the confidentiality, integrity and authenticity of personal data. In this respect, since 2013 ENISA has produced a report on the appropriate technological measures to protect information and communication through the use of cryptographic techniques. In 2016, ENISA will shift the focus of the deliverable on appropriate technological protection measures, from algorithms to the application domain, providing guidelines on how to specifically apply existing cryptographic technologies to protect privacy and trust. The study will address current and emerging technologies for data confidentiality, integrity and authenticity; both in storage and in transit. The report aims to be a useful tool for data controllers on how to better apply cryptography to improve the protection of personal data. ENISA will create an expert group (with representatives from MS) that will participate in the elaboration process of the study to maximise alignment with national guidelines.

Furthermore, ENISA will ensure continuity for the activities where the Agency has achieved high expertise in the area of privacy, as well as introducing some emerging new topics which have become relevant for the privacy community. For example, the Agency will carry on with its work on privacy enhancing technologies (PETs). Based on the findings of previous years, the report on the evolution, newest ideas and most up-to-date features of PETs and their building blocks, will explore the landscape of PETs and associated organisational measures, their specific applications and how they can be used to fulfil the legal requirements. The report will empower the competent authorities in the Member States to detail their own guidelines for their respective communities. Furthermore, the report will bring the different levels of maturity of technologies into the picture. This will help the EU and MS funding agencies to call for targeted R & D efforts to improve the overall availability of PETs.

Another area where ENISA will work in 2016 is the protection of personal data and security in electronic applications (i.e. healthcare). As new mechanisms and tools for online information processing appear (including storage, merging and correlation of data), in particular with the use of cloud services and smart mobile devices, the risk of exposure of sensitive medical data seriously increases. Therefore, using — among others — the results of the Agency's 2015 study on big data, ENISA will focus especially on the new and/or emerging means of personal data processing in online and mobile applications and the threats and risks that these create for these data. In particular, ENISA will provide a state-of-the-art analysis of the aforementioned risks and will propose a list of technical and organisational measures for managing and mitigating them. The result of the overall work will aim primarily at supporting users of online and mobile applications to protect their personal data, as well as data controllers who offer relevant services to citizens.

In 2016 ENISA will host the fourth edition of the Annual Privacy Forum (APF). The APF aims to provide an open forum where policymakers, researches and industry experts can discuss the key topics and new challenges in the field of data protection. Already in its fourth edition, the APF has become a reference conference for the privacy community in Europe. The objective of the Agency for 2016, as in previous years, will be to address the topics which are of current interest for the privacy community, in order to reach the maximum number of relevant participants, representing different stakeholder communities across Member States.

Regarding new activities, the agency conducted in 2015 a Europe wide survey on new directions on securing personal data, with the aim of gathering stock on the opinions of relevant experts in the area of privacy. Based on the results of this study, in 2016 ENISA will implement guidelines for data controllers on technological measures for securing the automated processing of personal data. This study will cover best practices and specific recommendations for the appropriate protection of personal data in automated systems. The report will focus especially on SMEs and other small-scale data controllers, where there is a currently a lack of documentation, as well as a high demand for guidelines to mitigate the risk of breaches and to achieve compliance with existing regulations.

Finally, during 2016 ENISA will support the European Commission (DG CONNECT) in the upcoming revision of the Directive 2002/58/EC (ePrivacy Directive). In particular, ENISA will act as technical advisor of the EC on the following topics

(1) Effectiveness and efficiency of security rules in the electronic communications sector; this includes an assessment of relevance and added value of specific security rules in the electronic communications sector; (art. 4), taking into account the revised relevant provisions of GDPR;

(2) Assessment of the option to enlarge the scope of security rules to encompass other critical actors in the electronic communications value-chain, such as component manufacturers, software providers, etc.

Time permitting, ENISA will also support in the evaluation and review of the cookies consent provision (assessment of adding new exceptions, assessment of possible solutions to reinforce the protection, including mandating technical standards).

To this end, ENISA will produce where necessary relevant working papers and technical reports, as well as support the EC on the online consultation for the review of the ePrivacy Directive (planned for March 2016).

Outcomes and deadlines

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

D5: Evolution and state of the art of privacy enhancing technologies and their building blocks (Q4, 2016).
D6: 2016 edition of the report on appropriate technological protection measures to preserve privacy and trust (Q4, 2016).
D7: Data protection and security in online and mobile applications (i.e. healthcare) (Q4, 2016).
D8: Annual Privacy Forum (Q2, 2016).
D9: Guidelines for data controllers on securing the automated processing of personal data (Q4, 2016).

Stakeholder impact

By supporting the development of guidelines for a broad range of privacy topics in the light of the new data protection regulation, the direct beneficiaries of the results of this WPK will be policymakers, supervisory bodies, research organisation and data controllers.

Legal base and policy context

- ENISA regulation, Article 3, particularly 3.1.(a).(ii), 3.1.(b).(i) and 3.1.(c).(ii).
- Cybersecurity strategy of the European Union.
- Data protection directive 95/46/EC.
- Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications.
- Proposal for a general data protection regulation.

4.3.2.3 WPK3.2.C. Assistance in the implementation of mandatory incident-reporting schemes

Desired impact

- By 2017, 15 Member States make direct use of the outcomes of Article 13a work by explicitly referencing it or by adopting it at nationally level.
- By 2017, 10 major e-communication providers across the EU comply with ENISA's minimum security measures.
- By 2017, 15 Member States contribute to ENISA's efforts on harmonised implementation of Article 19 of eIDAS regulation.

Description of tasks

This work package focuses on assisting regulatory authorities in the implementation of EU regulations related to mandatory incident reporting. It builds on successful work done in this area over the years in the area of Article 13a.

The main tasks of this work package are to support the following.

- NRAs and EU MS on the implementation of Article 13a (security-breach notification) and Article 4 (personal data breach notification) and developing synergies among them.
- NRAs and EU MS on the implementation of Article 19 of new regulation on eIDAS.
- ENISA will continue collecting and analysing annual, national reports of security breaches from NRAs in accordance with Article 13a of the framework directive on electronic communications. The Agency, in cooperation with experts from NRAs and the private sector (e.g. ENISA's e-communications reference group, NIS platform.), will analyse the national reports, compare them with previous years, identify new trends and develop good practices and lessons learned. ENISA will also assess the use of ENISA's security measures by eCom providers and identify any new missing measures to be included in such guidelines. NRAs can use these guidelines in a consistent and harmonised way across the sector and across MS.

ENISA will cooperate with electronic communications providers and MS competent authorities (e.g. NRAs and DPAs) to address security, privacy and confidentiality issues in an integrated and holistic manner. In that respect the Agency, in cooperation with the Commission, will continue its efforts towards a

harmonised reporting scheme for the e-communication providers that would address both Article 4 and Article 13a requirements.

ENISA will continue its efforts to develop common guidelines for a cost-effective mandatory security-breach notification scheme implementing Article 19 of eIDAS regulation. The Agency, building on the Forum of European supervisory authorities for electronic signatures (FESA) and other related public and private stakeholder groups, will bring all competent authorities of the EU together to discuss the scope of the scheme, the services affected, the impact of the incidents reported (e.g. parameters and thresholds), the reporting attributes, the reporting modalities, the reporting tools and others. ENISA will also try to exploit all possible implementation and conceptual synergies with Article 13a and Article 4.

Outcomes and deadlines

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

D10: Annual incident analysis report (Article 13a) (workshop and report, Q3, 2016).
D11: Analysis of security measures deployed by e-communication providers (workshop and report, Q4, 2016).
D12: Contribute to EU policy in the area of electronic communications sector (workshops, meetings, Q1-Q4, 2016).
D13: Engaging eIDAS competent authorities in the implementation of Article 19 (workshops, Q1-Q4, 2016).
D14: Guidelines for mandatory incident reporting in the context of eIDAS (report, Q4, 2016).

Stakeholder impact

Telecommunications sector

- Supervisory authorities will have practical references and technical guidelines to implement the legislation.
- Within the area of Article 13a, the industry, NRAs and the Commission will be able to develop a better understanding of the significant incidents at European level as well as a comparison with earlier years and recommendations, which will support mitigation decisions and actions.
- The Commission (DG Communications Networks, Content and Technology, DG Migration and Home Affairs and DG Justice and Consumers) will achieve harmonisation of incident reporting, breach notifications and security measures, following international standards and can in this way forego further detailing of the legislative text.
- Industry (network providers, internet service providers (ISPs), cloud providers, etc.) will be able to adopt a single framework of incident reporting/breach notification and security measures, so there is a level playing field across the EU MS and no complications for working across borders.
- Cooperate with Member States and private sector to develop an e-communications networks resilience.
- ISPs and internet exchange points (IXPs) will be able to better use the existing technology to better serve customers during crises and offer related services.

Regulation on electronic identification and trusted services

- NRAs and DPAs will be able to implement an efficient reporting scheme which is very similar to the Article 13a scheme currently in place, and in this way lay the basis for a coherent and holistic picture of security incidents across key service providers.
- A single reporting scheme will allow trust service providers to operate more easily across borders, effectively paving the way for a single market of trust service providers across the EU. In turn this facilitates cross-border online services, such as e-commerce and e-government.

Legal base and policy context

- ENISA regulation Article 3, in particular Articles 3.1.(a), 3.1.(b) on capacity building and 3.1.(c).

- Cybersecurity strategy of the European Union: Council Resolution of 18 December 2009.
- CIIP action plan 2009 and 2011.
- Internal security strategy for the European Union.

4.3.2.4 WPK3.2.D. Support for policy implementation in the area of electronic identification and trust services

Desired impact

- At least six stakeholders from trust service providers, online services providers, conformity assessment bodies and supervisory authorities contribute in ENISA guidelines and best practices recommendations regarding electronic identification and trust services.
- At least 10 experts from the community participate in the validation of the results of the studies.

Description of tasks

The main objective of this WPK is to continue to support the large-scale adoption of secure electronic identification means and trust services across Europe. Trust services are a key enabler for increasing citizens' confidence in online services, and given their nature, they require a high level of security to ensure their integrity and reliability. ENISA has contributed extensively to the area of securing trust services in the past by providing best practices for providers, recommendations on audit schemes, standardisation guidance, security-breach reporting recommendations, etc.

From the policy perspective, a milestone in this area was achieved with the adoption of the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market. ENISA aims to support the implementation of the regulation by further focusing on the security aspects related to trust services providers.

In order to identify key aspects and gaps this area, in 2015 ENISA launched, in collaboration with the EC, a forum that brings together communities, namely: trust service providers from the EU trusted lists, conformity assessment bodies and supervisory authorities. The forum has proven to be a useful tool for identifying gaps and areas where further work is needed, and its activities will continue in 2016.

ENISA will continue working on the implementation and update of the guidelines for security-breach notification to supervisory bodies by trust service providers (facilitating the application of the obligation stemming from Article 19 of the regulation).

ENISA will continue supporting the EC in the assessment of the candidate standards that might be listed in implementing acts that may be adopted by the EC. The scope will be enlarged to include electronic identification (eIDs), the issues of conformity assessment and certification frameworks.

The study on security recommendations for relying parties of trust services, will produce guidelines for online services providers acting as relying parties for trust services provided by third parties, on how to ensure the correct implementation of the trust chain. The report will focus on the area of website authentication; the trust service with the highest impact on online transactions. Web site authentication is a key element to create trust between online service providers and citizens. Online service providers, which can range from small SMEs to large public administrations, rely on website authentication certificates and protocols to prove their identity to their consumers. However, website authentication protocols and their building blocks are one of the main targets for emerging attacks and new vulnerabilities appear frequently.

Finally, the 2016 edition of the report on appropriate technological protection measures to preserve privacy and trust will also support the implementation of the eIDAS regulatory framework, by addressing technological aspects and building blocks for trust services.

Outcomes and deadlines

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

D15: Update on standards for trust services and electronic identification (Q4, 2016).
D16: Report on security recommendations for relying parties of trust services (Q4, 2016).

Stakeholder impact

The direct beneficiaries of the results of this WPK will be:

- trust service providers
- online service providers
- regulatory authorities
- supervisory bodies
- conformity assessment bodies.

Stakeholders will benefit by receiving guidance on how to implement the new regulatory framework, as well as recommendations on security measures to ensure integrity and reliability of the trust services they provide or consume.

Legal base and policy context

- ENISA regulation, Article 3, particularly 3.1.(a).(ii), 3.1.(b).(i) and 3.1.(c).(ii).
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.
- Commission communication — 'A coherent framework for building trust in the digital single market for e-commerce and online services', COM(2011) 942 final of 11 January 2012.

4.4 SO4. To enhance cooperation both between the Member States of the European Union and between related network and information security communities

SO4 covers aspects of cooperation between the EU MS and the EU and between related NIS communities where ENISA could play a hole to enhance NIS cooperation.

List of work packages and short description

- **WPK4.1. Cyber crisis cooperation and exercises**

In the context of this work package (WKP), ENISA will further enhance its methodology, seminars, training and technical capabilities on the organisation and management of large-scale cyber crisis exercises. The Agency will continue enhancing its internal capabilities for managing complex, distributed exercises, by building on its previous efforts. ENISA will explore new opportunities which will enhance the overall realism of cyber exercises.
In 2016, ENISA will organise the fourth pan-European cyber exercise, Cyber Europe 2016 (CE2016). This exercise will build on the experience gained in previous exercises and will take into account previously identified recommendations and findings.
Furthermore ENISA will continue supporting Member States towards the development of a sound and implementable European cyber crisis cooperation framework and procedures.

- **WPK4.2. NIS community building**

The key goal of this WPK is to build upon the good experience ENISA has in supporting different operational communities (CSIRT network, law enforcement communities, European financial institutes — information sharing and analysis centre (FI-ISAC), A-ISAC, etc.) to enhance mutually satisfactory ways to collaborate.
ENISA will develop and provide guidance based on best practice in the area of operational community efforts (operational cooperation, information exchange, etc.). Where possible, synergies with other ENISA collaboration- and community-supporting efforts such as the NIS platform will be extended and, where needed, developed.

The Agency will continue its work and support of the Transits training in the area of CSIRTs in order to build communities through a 'learning by doing' approach.

ENISA will also continue to support the collaboration between CSIRT and law enforcement communities, based on the recent policy and technical developments in this area in Member States.

4.4.1 WPK4.1. Cyber crisis cooperation and exercises

Desired impact

- At least 10 Member States and EU institutions take part in the study on cyber crisis cooperation and exercise activities and findings.
- At least 24 EU Member States and European Free Trade Association (Stockholm Convention) (EFTA) countries confirm their support for Cyber Europe 2016 (CE2016).
- At least 20 EU Member States will attend the ENISA event which aims to promote cyber crisis cooperation activities within the context of the existing NIS policy framework.

Description of tasks

Objectives

- Continue the work in the area of pan-European cyber exercises (Cyber Europe 2016) by adapting to the needs of ENISA stakeholders.
- Enhance the capacity to support and organise cyber exercises in Europe by organising small-scale regional exercises (EuroSOPEx).
- Identify good practices and improve operational procedures for cyber crisis cooperation in Europe within the context of the NIS policy framework.
- Promote best practices in the area of cyber crisis cooperation and exercises at EU and international level by engaging the NIS community.
- Draft in close cooperation with the Member States a pan-European roadmap for cyber exercises.

Pan-European cyber exercises: Cyber Europe 2016

In 2016, ENISA will organise the fourth pan-European cyber exercise; CE2016. This exercise will closely follow up and build on the lessons learned and actions from previous exercises, such as Cyber Europe 2014 (CE2014).

CE2016 will be an exercise programme focusing on testing and training on large-scale incident management cooperation procedures at EU and national-levels. The efforts will not focus only on organising a one-off event but rather to be a continuous effort throughout the year, offering preparatory training and cooperation opportunities such as small exercises to Member States and the EU institutions (EuroSOPEx). The exercise escalation and build-up will be realistic and focused in order to better capture how incidents are managed and cooperation happens in real-life. The high-level exercise programme brief will have to be prepared based the lessons learned from CE2014, approved by the Member States and the ENISA MB, and drive the whole planning process.

Following that, the detailed setup and exercise plan will be agreed with the EU, EFTA members and EU institutions, in line with the existing NIS policy context. Each country will be represented in the exercise planners group. This group will be responsible for the approval of the detailed exercise setup and plan. The approach that will be followed will be that of an opt-in scheme for the identification of stakeholders in the countries which are interested to play in the exercise (e.g. policy level), allowing for the countries who wish and have the appropriate resources to extend their national play.

As previously established, ENISA will not invite international organisations or participants from countries other than EU and EFTA members to participate in EU cybersecurity exercises without having first obtained the approval of the ENISA MB.

Enhancing the capacity to support and organise cyber exercises
ENISA will further enhance its methodology, seminars, training and technical capabilities on the organisation and management of cyber crisis exercises. The Agency will continue enhancing its internal capabilities for managing complex, distributed exercises by building on its previous efforts. ENISA will explore new opportunities which will enhance the overall realism of cyber exercises.

Furthermore, ENISA will support smaller-scale exercises, bilateral or regional, within the EU upon request. The requests can be sent based on Article 14 of the ENISA regulation. Support could be offered with seminars and exercise planning training, as well as actual exercise planning support including the utilisation of the cyber exercise platform (CEP), given the resource availability of the Agency.

ENISA, in close cooperation with the EU Member States and institutions, will draft a proposal for a pan-European roadmap for cyber exercises. This proposal will be built on the foundation of previous consultations done with the EU Member States and institutions.

Cyber crisis cooperation and exercises activities overview
ENISA will continue supporting Member States towards the development of sound and implementable European cyber crisis cooperation framework and procedures. The Agency will continue exploring requirements for developing infrastructures for cooperation, e.g. secure communications channels or directories.

In this context, ENISA will host a workshop on EU-SOPs as a follow-up the exercise activities. Also ENISA will issue an update of its report on activities in the area of cyber crisis cooperation. In addition, this report will help ENISA to reach out to other communities/sectors.

ENISA will also ensure that adequate feedback and follow-up to previous findings and recommendations are reported back to the stakeholders.

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

D1: Cyber Europe 2016: exercise plan and exercises (exercise Q4, 2016).
D2: EuroSOPEx 2016: exercise plan and exercises (exercises Q4, 2016).
D3: Pan-European cyber exercises roadmap (report Q4, 2016).
D4: Cyber crisis cooperation procedures: follow up the NIS policy framework (report Q4, 2016).

Stakeholder impact
The primary beneficiaries of this WPK will be policymakers and organisations from public and private sectors, who will receive integrated and consolidated information about the European NIS threat landscape and how it is evolving.

EU and Member States' national cybersecurity agencies, cyber crisis management units, national cyber crisis structures and partnerships.

- Assess the current level of preparedness for large-scale events and cooperation capacities.
- Develop an overview of pan-European and international efforts in the area.
- Obtain input, insight and recommendations for future actions in policy and technical measures.

The Commission

- Obtain insight and an expert base for current and future policy efforts in: cyber crises cooperation, contingency plans, cyber exercises and other areas related to the EU cybersecurity strategy.

The private sector

- Obtain input on current level of internal preparedness for large-scale events and inter-operator cooperation as well as public-private sector cooperation and coordination.
- Obtain insight on which requirements future actions may bring in the area of preparedness measures and continuity planning.

Legal base and policy context

- ENISA regulation Article 3, in particular 3.1.(b) and 3.1.(c).
- Cybersecurity strategy of the European Union Council Resolution of 18 December 2009.
- CIIP action plan 2009 and 2011.
- Internal security strategy for the European Union.

4.4.2 WPK4.2. Network and information security community building

Desired impact

Work of ENISA successfully reflected by existing communities when appropriate (Forum of incident response and security teams (FIRST), CSIRT task force (TF-CSIRT-TI), European FI-ISAC, CSIRT network, etc.).

- At least 15 Member States participating at ENISA annual national and governmental CSIRT workshop and also in the joint ENISA-EC3 workshop on CSIRT-law-enforcement agency (LEA) collaboration.
- In 2017 enhanced operational community efforts (e.g. operational cooperation, information exchange).

Description of tasks

Objectives:

- Support incident-response community building and information exchange.
- Contributing to the existing communities' efforts in incident response field.
- Enable continuous trust and collaboration building for communities through regular events.
- Information provided to key stakeholders on NIS policy developments.

The key goal of this WPK is to build upon the good experience ENISA has acquired in supporting different operational communities (CSIRT, law enforcement communities, European FI-ISAC, A-ISAC, CSIRT network provided for by the NIS directive, etc.) to enhance mutually satisfactory ways to collaborate.

ENISA will develop and provide guidance based on best practice in the area of operational community efforts (operational cooperation, information exchange, etc.). Where possible, synergies with other ENISA collaboration- and community-supporting efforts such as the NIS platform will be extended and, where needed, developed.

The Agency will continue its work and support of the TRANSITS training in the area of CSIRTs in order to build communities through a 'learning by doing' approach.

ENISA will also continue to support the collaboration between CSIRT and law enforcement communities, based on the recent policy and technical developments in this area in Member States. This work will include close collaboration with other institutions which are active in this field, namely the EC3. Activities agreed upon in the collaboration agreement between ENISA and EC3 will be further developed, for example in the area of encouraging a more practical and regular flow of information between CSIRTs and law enforcement communities, the exchange of specific knowledge and expertise, elaboration of general situational reports, reports resulting from strategic analyses and best practice and strengthening capacity building through training and awareness raising in order to safeguard NIS at EU level. For better coordination and in order to avoid overlaps ENISA will stay engaged in the EC3 programme board. The very well established, commonly organised ENISA-EC3 workshop will be continued.

Following its successful mechanism for building the European national and governmental CSIRT community trust and collaboration, ENISA will organise its traditional workshop to support the national and governmental CSIRT community grow. (11th CSIRTs in Europe workshop).

In its Article 8b, the NIS directive will establish a CSIRTs network "in order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation". It is "composed of representatives of the Member States' CSIRTs and CERT-EU".

The CSIRTs Network will provide a forum where Member States' National CSIRTs can cooperate, exchange information and also build trust. Member States CSIRTs will be able to improve the handling of cross-border incidents, and even discuss how to respond in a coordinated manner to specific incidents.

ENISA will provide the secretariat of the CSIRTs Network and actively support the cooperation among the CSIRTs. In 2016 the Agency will organise a meeting of the CSIRTs Network adjacent to its 11th CSIRTs in Europe workshop. ENISA will also provide its expertise and advice both to the Commission and Member States, either in the form of guidance or in answer to specific requests. At the request of a Member State, the Agency can support the MS to develop a National CSIRT.

Outcomes and deadlines

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

D1: Continuation of existing community efforts (European FI-ISAC, FIRST, TF-CSIRT-TI, etc.).
D2: Annual ENISA national and governmental CSIRT workshop (Q4, 2016).
D3: Annual ENISA/EC3 cybercrime workshop (Q4, 2016).
D4: Supporting European network of MS CSIRTs.
D5: Review on new operational communities' development (A-ISAC, etc.) (Q4, 2016).

Stakeholder impact

- More effective information flows between the existing community efforts (FIRST, etc.).
- Timely information provided to key stakeholders on NIS incidents and on significant developments in the field.
- Enhanced collaboration and trust building for different communities (European national and governmental CSIRT community, CSIRT and law enforcement communities, CSIRT network, etc.).
- Regular updates on current and future policy efforts and developments in the incident response area.

Legal base and policy context

- ENISA regulation, Article 3, particularly 3.1.(b) and 3.1.(c).
- Proposed NIS directive.

4.5 Horizontal activities supporting core operations

4.5.1 Management board, executive board and permanent stakeholders group secretariat

During 2016, ENISA will continue to support its formal bodies, the management board (MB) and the PSG as well as the executive board (EB) in their functions by providing secretariat functions.

For the MB, one ordinary meeting will be organised during 2016 and informal meetings will be held as necessary. The existing electronic newsletter will be continued throughout 2016, as will support for the MB portal. For the PSG two formal meetings will also be organised in the course of the year.

For the EB formal meetings will be organised during 2016; once per quarter (Q).

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

The MB, executive board and PSG secretariat reports directly to the ED.

4.5.2 National liaison officer network

Since 2014, ENISA has initiated a number of activities with the aim to strengthen cooperation within the national liaison officers' (NLO) network. NLOs are key actors for the Agency's daily work and interaction, assuring, in terms of outreach, effective liaison with the MS and dissemination of ENISA deliverables.

In 2016, ENISA will build upon these efforts and improve its cooperation with the NLO network, the first point of contact for ENISA in the MS. In particular, the Agency will continue working on the following actions.

- An NLO meeting will be organised where possible improvements of the collaboration will be discussed. Improvements aim at leveraging the NLO network for the dissemination of ENISA deliverables.
- Information will be sent to the members of the NLO network at regular intervals on upcoming ENISA project-related tenders, vacancy notices, and events organised by ENISA or which the Agency contributes to (for example co-organiser, etc.).
- The agency will maintain and share with the NLO network information on all relevant ENISA project activities (e.g. unit responsible for the project, relevant tender results).

4.5.3 European Union relations

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

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

4.5.4 Spokesperson, stakeholders communication and dissemination activities

In 2016, ENISA will seek to improve its focus on its key activities and to provide regular information to the press and media regarding these activities. In order to achieve this, the Agency spokesperson will be located in the Athens office and will be in constant contact with the operational teams.

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

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

4.5.5 Quality control and project office

The quality control (QC) of the Agency aims to respond to a mix of regulatory and stakeholder requirements in an effort to improve organisational performance and compliance. Scheduled annual activities associated with the promulgation and maintenance of standard operating procedures (SOP) and a methodology, support the operational processes of the Agency. The primary goal of the QC is to improve performance across the core operations, while reducing operational costs and enhancing stakeholder satisfaction. The methodology is based on the plan-do-check-act (PDCA) cycle.

The project office in the Core operations department (COD) seeks to better coordinate the increasing number of activities that cut across multiple operational areas within the department. Such activities include the preparation of briefings on global issues and coordinating the coherence of recommendations across the department, the preparation of formal documents, follow up on performance management, project management etc.

Information security management systems (ISMS). In 2016 ENISA plans to further develop the management of information security risks and controls under the authority of the Agency's management. The ISMS includes people, processes, IT systems and policies. While elements of an ISMS (e.g. risk assessment, assets inventory) are well developed, targeted efforts aim to improve both (a) the management of recurrent intrusion detection and vulnerabilities analysis exercises and (b) the documented policy framework which is currently at the disposal of the Agency for the purpose of enhancing the compliance position of the Agency. While these efforts are likely to lower the risk profile of the Agency, they will also provide the added benefit of hands-on experience and allow the Agency to better guide other similar organisations and agencies among its stakeholders, as need be.

4.5.6 Article 14 requests

Article 14 requests are a mechanism that allows the MS or EU institutions to make direct requests to ENISA for carrying out particular activities. This mechanism has become increasingly accepted in the last few years and it has grown in significance to the extent that the Agency believes that it needs to be explicitly planned for in the annual WP. Under SO2, both WPKs WPK2.1 Assist MS capacity building and WPK2.2 Support EU institutions include deliverables dedicated to assistance/on-request support for EU MS and institutions.

Although, by definition, it is not possible to predict the exact number or the orientation of the requests that the Agency will receive in 2016, based on past experience the allocated resources are indicated in the summary of activities and budget allocation section at the end of this document.

4.5.7 Data protection officer

The main tasks of the data protection officer (DPO) include the following.

- Inform and advise ENISA of its obligations pursuant to Regulation 45/2001/EC and to document this activity and the responses received.
- Monitor the implementation and application of ENISA's policies in relation to the protection of personal data.
- Monitor the implementation and application of Regulation 45/2001/EC at ENISA, including the requirements for data security, information of data subjects and their requests in exercising their rights under the regulation, as well as the requirements for prior check or prior consultation with the EDPS.
- Monitor the documentation, notification and communication of personal data in the context of ENISA's operations.

- Act as ENISA's contact point for the EDPS on issues related to the processing of personal data; to cooperate and consult with the EDPS whenever needed.

5. Management, administration and support activities

5.1 Executive director's office

The executive director (ED)'s office consists of the ED and personal assistant. The ED is responsible for the overall management of the Agency.

The two heads of department (Administration and support department and Core operations department), the corporate communications officer and the Management Board & Permanent Stakeholders Group Secretariat report directly to the ED.

5.2 Administration and support department

The Administration and support department (ASD) consists of Finance, accounting and procurement unit (FAP), the HR section, the IT unit (ITU), and the team supporting the department.

The ASD is responsible for ensuring that the management of the Agency is in line with the regulatory framework established by the competent EU institutions, the MB, and the ED. The regulatory framework is composed of the financial regulation and the staff regulations and their respective implementing rules, as well as administrative procedures, the internal control framework and other control mechanisms put in place to ensure compliance with the rules.

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

The head of the ASD (HoASD) develops the agency strategy for the administration and support activities (ASA) in line with the WP and with the required compliance with the abovementioned bodies and rules. The HoASD is also the main contact point as regards administrative matters, with external stakeholders such as European Commission services and DGs, the European Parliament, the Council, the ENISA EB, ENISA MB, Hellenic authorities, etc. The head of department is supported by the legal officer and two assistants who also support the units in the department.

5.3 Activities

5.3.1 ASA 0 Executive director's office and general management

The activities of the executive director's (ED's) office and general management consist of defining and implementing the Agency's strategy, planning, decision-making and overall management activities.

5.3.2 ASA 1 Quality management systems, ICC, security, facilities management, internal communications

The main activities of ASA 1 supervised by the HoASD include quality management systems, internal control function (head of administration provides the ICC), facilities management (FM) and internal communications (ICom).

ASA1 also covers: physical security and safety; support to the ICC (including risks assessment, *ex post* controls, etc.); Hellenic authorities (value–added tax (VAT) management; individual privileges management, etc.) and protocol; FM (including building maintenance and management); internal communication and staff welfare; management reporting; support IAS/CoA (including external audit) etc.;

ENISA general report; multiannual staff policy plan. Quality management (QM) systems include policies, procedures, internal workflows, compliance, organisation structure, resources to meet internal and external stakeholder's requirements and expectations.

In 2016 ENISA will continue to re-engineer selected operational processes, to align organisational requirements with actual implementation and pursue process improvements across the board. Measuring the performance of recently designed processes, e.g. the ENISA project management guide, for the purpose of proposing suitable adjustments will be a priority. A risk assessment methodology will be implemented for agency-wide risks, as necessary. A set of tools such as electronic signatures, electronic workflows and enterprise resource management tools are likely to be further integrated to facilitate collaboration. Regular presentations and updates are made available to provide guidance and promote the performance of the quality management system.

Physical security and FM is carried out in a coherent manner across both ENISA sites and both functions report into the head of administration. These activities will ensure that staff benefit from an ergonomic and secure environment in both agency locations. Furthermore, the agency will ensure that the approach to logical and physical security is aligned in order to ensure appropriate protection of data.

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

- Logistics, transport and delivery services.
- Buildings and inventory management.
- Purchase of stationery and consumables.

In 2016, the ICC and internal audit capability (IAC) function will monitor the Agency's activity in administrative transactions, assess the risk framework and the controls in place, contribute to mapping and monitoring the key risk areas, follow-up of the implementation of the auditors' recommendations (CoA and the IAS) and issue exception management reports.

ENISA will outsource the IAC to the Commission IAS and support all preventive or corrective activities resulting from the audits performed by IAS.

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

5.3.3 ASA 2 Finance, accounting and procurement

The activities of the FAP unit consist of managing the budget of the Agency, conducting all procurement procedures and accounting.

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

The activities of the unit are listed below.

- Financial transactions' initiation.
- Central financial verification of all financial transactions.
- Budget preparation and management.
- Mission management and helpdesk.
- Financial helpdesk and reporting.

- Accounting activities.
- Statutory reporting activities, including discharge procedure.
- Procurement procedures' overall management, including procurement planning.
- Overall contracts' management.
- Coordination of audits and support to all other audit assignments.
- Internal training related to FAP activities.
- Single point of contact for financial management matters to DG Budget (e.g. ABAC implementation).
- Drafting internal financial policies.
- Introducing solutions to optimise internal financial workflows.

5.3.4 ASA 3 Human resources

The activities of human resources (HR) consist in managing the rights and obligations of ENISA staff, recruitment and training.

- Management of individual staff rights and obligations, according to the stipulations of the staff regulations (SR).
- Recruitment procedures.
- Entitlements and leave management.
- Drafting internal HR policies and implementing rules of the SR.
- Medical services and health in work environment.
- Training plan and career development.
- Management of interim services.
- Work environment and welfare.

5.3.5 ASA 4 Information and communications technology

The IT unit (named ITU) delivers internal IT systems and services to the Agency, across its two fully functional offices, as well as to a highly mobile user-base. The IT team uses the IT Infrastructure Library (ITIL) framework as a source of good practice in service management. Both human and financial resources are organised according to ITIL, as shown in the summary table in the following section.

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

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

- service strategy
- service transition
- service security
- service operations
- external services
- service support.

6. Summary of activities and budget allocation

6.1 Summary of core operational activities with strategic objectives, work packages and deliverables

SO1.	**To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security**
WPK1.1.	**Improving the expertise related to critical information infrastructures**
	D1: Good practices on the security and resilience of smart cars and intelligent road systems (report and a workshop, Q4, 2016).
	D2: Good practices on the security and resilience of smart health services and infrastructures (report and a workshop, Q4, 2016).
	D3: Good practices on the security and resilience of smart airports (report and a workshop, Q4, 2016).
WPK1.2.	**Network and information security threats landscape analysis**
	D1: Annual threat analysis/landscape report (Q4, 2016).
	D2: Assessments on two key technology/application areas (governments, small to medium-sized enterprises (SMEs), etc.) (Q4, 2016).
WPK1.3.	**Research and development, innovation**
	D1: ENISA cryptographic challenges (Q3, 2016).
	D2: Recommendations on aligning research programme with policy in the specialised area of NIS (Q4, 2016).
	D3: Study on security aspects of virtualisation (Q4, 2016).
SO2.	**To assist the Member States and the European Union institutions and bodies in enhancing capacity building throughout the EU**
WPK2.1.	**Assist Member States' capacity building**
WPK2.1.A.	Assistance in the area of operational security and NIS operational training
	-
	D2: Follow-up/extension of the training methodologies work from 2014/15 (Q4, 2016).
	D3: Update of existing training material (Q4, 2016).
	D4: Development of a set of new training material (Q4, 2016).
	D5: On-request training for MS and EU bodies (Q4, 2016).
	D6: Good practice in incident tracking and taxonomy (Q4, 2016).
	D7: Annual update of baseline capabilities (report) (Q4, 2016).
WPK2.1.B.	Assistance in the area of Cybersecurity Strategies
	D8: Assist and advise Member States on the establishing and evaluation of NCSS (workshops Q1-Q4, 2016).
	D9: Update good practice guide on NCSS (report, Q4, 2016).
	-
WPK2.1.C.	Assistance in the area of privacy and trust
	D11: On-request support for MS decision-making in the areas of privacy and trust (Q4, 2016).
WPK2.2.	**Support European Union institutions' capacity building**
WPK2.2.A.	Information notes on NIS: production and review mechanisms ("info notes")
	D1: Review and adjust mechanism for production of info notes (Q1-4, 2016).
	D2: Restricted and public info notes on NIS (Q1-Q4, 2016).
WPK.2.2.B.	Reinforcement of the NIS of Union institutions, bodies and agencies
	D3: Restricted. Upon request, support the assessment of existing policies/procedures/practices on NIS within EU institutions (workshop, meetings, Q1-4, 2016).
WPK2.3.	**Assist private sector capacity building**
	D1: Recommendations for creating a cybersecurity culture and improving management-level cybersecurity awareness (Q4, 2016).

WPK2.4.	**Assist in improving the general awareness**
	-
	D2: ENISA cyber challenge (Q2, 2016).
	D3: Provide guidance and support for ECSM (dissemination material, Q4, 2016).
	D4: Upgrade the online privacy tools portal and involve privacy experts from different fields (dissemination material, Q4, 2016).
SO3.	**To assist the Member States and the European Union institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security**
WPK3.1.	**Supporting European Union policy development**
WPK3.1.A.	Contribution to EU policy linked to secure infrastructures and services
	D1: Contribute to EU policy in the area of cloud computing (workshops, meetings, Q1-Q4, 2016).
	D2: Contribute to EU policy in the area of smart grids and ICS-SCADA (workshops, meetings, Q1-Q4, 2016).
	D3: Support the policy discussions in the area of IT security certification (workshops, meetings, Q1-Q4, 2016).
	D4: Contribute to EU policy in the area of finance (workshops, meetings, Q1-Q4, 2016).
WPK3.1.B.	Policy development and standards
	D5: Recommendations for improving NIS in EU standardisation policy (Q4, 2016).
WPK3.1.C.	Towards a DSM for NIS and related IT Products and Services
	D6: Restricted. Towards a DSM for NIS products and Services (workshops, report, Q4, 2016).
WPK3.2.	**Supporting European Union policy implementation**
WPK3.2.A.	Assist EU MS and Commission in the implementation of the NIS directive
	D1: Contribute to the establishment of the cooperation group (meetings, workshops, Q2-Q4, 2016)
	D2: Advice on the implementation of mandatory incident reporting for DSPs – input to the Implementation Acts (report, workshop, Q4, 2016).
	D3. Advice on the implementation of security requirements for DSPs – input to the Implementation Acts (report, workshop, Q4, 2016)
	D4: Assist MS in the identification of operators of essential services (workshop, Q2-Q4, 2016)
WPK3.2.B.	Assistance in the implementation of NIS measures of EU data protection regulation
	D5: Evolution and state of the art of privacy enhancing technologies and their building blocks (Q4, 2016).
	D6: 2016 edition of the report on appropriate technological protection measures to preserve privacy and trust (Q4, 2016).
	D7: Data protection and security in online and mobile applications (i.e. healthcare) (Q4, 2016).
	D8: Annual Privacy Forum (Q2, 2016).
	D9: Guidelines for data controllers on securing the automated processing of personal data (Q4, 2016).
WPK3.2.C.	Assistance in the implementation of mandatory incident-reporting schemes
	D10: Annual incident analysis report (Article 13a) (workshop and report, Q3, 2016).
	D11: Analysis of security measures deployed by e-communication providers (workshop and report, Q4, 2016).
	D12: Contribute to EU policy in the area of electronic communications sector (workshops, meetings, Q1-Q4, 2016).
	D13: Engaging eIDAS competent authorities in the implementation of Article 19 (workshops, meetings, Q1-Q4, 2016).
	D14: Guidelines for mandatory incident reporting in the context of eIDAS (report, Q4, 2016).
WPK3.2.D.	Support for policy implementation in the area of electronic identification and trust services
	D15: Update on standards for trust services and electronic identification (Q4, 2016).
	D16: Report on security recommendations for relying parties of trust services (Q4, 2016).
SO4.	**To enhance cooperation both between the Member States of the European Union and between related NIS communities**
WPK4.1.	**Cyber crisis cooperation and exercises**
	D1: Cyber Europe 2016: exercise plan and exercises (exercise Q4, 2016).
	D2: EuroSOPEx 2016: exercise plan and exercises (exercises Q4, 2016).

	D3: Pan-European cyber exercises roadmap (report Q4, 2016).
	D4: Cyber crisis cooperation procedures: follow up the NIS policy framework (report Q4, 2016).
WPK4.2.	**Network and information security community building**
	D1: Continuation of existing community efforts (European FI-ISAC, FIRST, TF-CSIRT-TI, etc.).
	D2: Annual ENISA national and governmental CSIRT workshop (Q4, 2016).
	D3: Annual ENISA/EC3 Cybercrime Workshop (Q4, 2016).
	D4: Supporting European network of MS CSIRTs.
	D5: Review on new operational communities' development (A-ISAC, etc.) (Q4, 2016).

6.2 Activity-based budgeting

The work programme 2016 activities consist of well-defined actions to which resources are allocated and converted into outcomes. Core activities are those aiming to create the impact in the core field of NIS, required by the regulation of ENISA and interpreted in the current policy and legal context. ASA, on the other hand, aim to provide strategic and overall management orientation, support the core activities with infrastructure and competence, and ensure compliance with the regulatory framework.

The purpose of activity-based budgeting (ABB) is to ensure that resource allocation is consistent with the activities of the Agency, as described in the annual WP.

In this regard, resources engaged in ASA are re-allocated to core and horizontal operational activities in such a way that the effort and the respective HR costs engaged in the support of the operational activities (e.g. procurement procedures to award a contract related to a WPK/deliverables) are attributed to the latter.

While the Commission job screening methodology used for benchmarking resources employed across EU agencies is looking at the HR allocated to functions and gives weight to job profiles and descriptions (operational, neutral, administration), the ABB concept allocates the administrative and support resources according to their contribution to the Agency's work. Therefore the figures in following tables refer to the administration and support resources necessary to ensure the smooth operation of the Agency, with focus on the strategic as well as day-to-day management of the Agency and compliance with the legal and regulatory framework (e.g. risk management, internal controls, engagement with the CoA and IAS, statutory reporting).

NB: Full time equivalents (FTE) and costs of activities are reported on ABB basis. Costs of activities, ABB values cover also costs including salaries.

6.2.1 Summary of core operational activities

Core operational activities (Strategic objectives 1 to 4)	Operational activities — FTEs	Total cost of activities — ABB
SO1. To develop and maintain a high level of expertise of EU actors, taking into account evolutions in network and information security	**9,5**	**983.568,48**
WPK1.1. Improving the expertise related to critical information infrastructures	4,1	432.760,90
WPK1.2. Network and information security threats landscape analysis	2,6	263.248,57
WPK1.3. Research and development, innovation	2,8	287.559,01
SO2. To assist the Member States and the European Union institutions and bodies in enhancing capacity building throughout the European Union	**14,4**	**1.360.163,16**
WPK2.1. Assist Member States' capacity building	8,0	802.056,15
WPK2.2. Support European Union institutions' capacity building	2,6	191.966,98
WPK2.3. Assist private sector capacity building	1,1	93.736,24
WPK2.4. Assist in improving the general awareness	2,7	272.403,79
SO3. To assist the Member States and the European Union institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security	**25,7**	**2.412.864,85**
WPK3.1. Supporting European Union policy development	8,1	720.366,59
WPK3.2. Supporting European Union policy implementation	17,6	1.692.498,26
SO4. To enhance cooperation both between the Member States of the European Union and between related network and information security communities	**11,6**	**1.078.885,75**
WPK4.1. Cyber crisis cooperation and exercises	6,6	642.417,45
WPK4.2. Network and information security community building	5,0	436.468,30

Horizontal activities supporting core operations stakeholders relations, corporate communication, project support activities	Operational Activities — FTEs	Total cost of activities — ABB
HA. Horizontal activities supporting core operations	**14.5**	**1.393.318.38**
HA1. Management board, executive board and permanent stakeholders group secretariat	1.3	298.483.49
HA2. National liaison officer network	0.7	61.241.74
HA3. European Union relations	1.3	82.483.49
HA4. Spokesperson, stakeholders communication and dissemination activities	2.6	324.966.98
HA5. Quality control and project office	7.2	543.659.19
HA6. Article 14 requests	0.7	41.241.74
HA7. Data protection officer	0.7	41.241.74

Operational activities	Operational Activities — FTEs	Total cost of activities — ABB
Total operational activities	**75.6**	**7 228 800.63**

6.2.2 Summary of administration and support activities

Administration and support activities	Operational activities — FTEs	Total cost of activities — ABB
ASA. Administration and support activities	**8.4**	**3 231 763.37**
ASA0. Executive director's office and general management	1.1	73 233.88
ASA1. Quality management systems, ICC, security, facilities management, internal communications	1.6	1 309 469.54
ASA2. Finance, accounting and procurement	2.5	158 248.87
ASA3. Human resources	1.3	1 126 124.43
ASA4. Information and communications technology	1.9	564 686.65

Missions for all staff		**600 000.00**

TOTAL	**84.0**	**11 060 564.00**

Annex 1 – Financing Decision[4]

	Deliverable description	Budget by Deliverable / WPK	Unit	Specific procurement procedure planned	Using existing Framework contracts, List of Experts etc.	Budget for 2016 tenders	Budget expenditure - existing FWC etc.	Planned contract start date	Planned deliverable date
	Core operational activities								
SO1		**€424.000,00**							
WPK1.1.	**WPK1.1. Improving the expertise related to critical information infrastructures**	**€210.000,00**							
D1	Good practices on the security and resilience of smart cars and intelligent road systems (report and a workshop, Q4, 2016).	€70.000,00	COD1	Reopening of Comp (under FWC)	SMART INF_F-COD-15-C02	€65.000,00		15/02/2016	01/11/2016
					Events Organisation Services F-COD-15-C37		€5.000,00	01/06/2016	01/10/2016
D2	Good practices on the security and resilience of smart health services and infrastructures (report and a workshop, Q4, 2016).	€70.000,00	COD1	Reopening of Comp (under FWC)	SMART INF_F-COD-15-C02	€65.000,00		15/02/2016	01/11/2016
					Events Organisation Services F-COD-15-C37		€5.000,00	01/06/2016	01/10/2016
D3	Good practices on the security and resilience of smart airports (report and a workshop, Q4, 2016).	€70.000,00	COD1	Reopening of Comp (under FWC)	SMART INF_F-COD-15-C02	€65.000,00		15/02/2016	01/11/2016
					Events Organisation Services F-COD-15-C37		€5.000,00	01/06/2016	01/10/2016
WPK1.2.	**WPK1.2. NIS threats landscape analysis**	**€100.000,00**							
D1	Annual threat analysis/landscape report (Q4, 2016).	€50.000,00	COD2	Negotiated tender (< €60k)		€40.000,00		15/02/2016	15/12/2016
	Workshop or related Issue				Events Organisation Services F-COD-15-C37		€10.000,00		
D2	Assessments on two key technology/ application areas (governments, SMEs, etc.) (Q4, 2016).	€50.000,00	COD2	Negotiated tender (< €60k)		€40.000,00		01/03/2016	30/09/2016
	Workshop for above				Events Organisation Services F-COD-15-C37		€10.000,00		
WPK.1.3.	**WPK1.3. Research and development, innovation**	**€114.000,00**							
D1	ENISA cryptographic challenges (Q3, 2016). Challenge design	€44.000,00	COD2	Reopening of Comp (under FWC)	CRYPTO_F-COD-13-C23	€34.000,00		01/04/2016	01/11/2016
				Negotiated tender (< €60k)		€10.000,00		01/08/2016	01/10/2016
D2	Recommendations on aligning research programme with policy in the specialized area of NIS (Q4, 2016).	€35.000,00	COD2	Negotiated tender (< €60k)		€35.000,00		01/03/2016	01/10/2016

[4] Adopted by the Management Board of the European Union Agency for Network and Information Security: Decision No MB/2015/14.

D3	Study on security aspects of virtualization (Q4, 2016).	€35.000,00	COD2	Negotiated tender (< €60k)		€30.000,00		01/03/2016	30/09/2016
	Workshop for above				Events Organisation Services F-COD-15-C37		€5.000,00		
SO2		**€458.000,00**							
WPK2.1.	**WPK2.1. Assist member states' capacity building**	**€302.000,00**							
D2	Follow up / extension of the "training methodologies" work from 2014/15 (Q4, 2016).	€30.000,00	COD3	Reopening of Comp (under FWC)	CERT SUPP_F-COD-13-C22	€30.000,00		01/03/2016	30/09/2016
D3	Update of existing training material (Q4, 2016).	€25.000,00	COD3	Reopening of Comp (under FWC)	CERT SUPP_F-COD-13-C22	€40.000,00		01/03/2016	30/09/2016
D4	Development of a set of new training material (Q4, 2016).	€90.000,00	COD3	Reopening of Comp (under FWC)	CERT SUPP_F-COD-13-C22	€75.000,00		01/03/2016	30/09/2016
D6	Good practice in incident tracking and taxonomy (Q4, 2016).	€90.000,00	COD3	Reopening of Comp (under FWC)	CERT SUPP_F-COD-13-C22	€90.000,00		15/02/2016	30/09/2016
D7	Annual update of baseline capabilities (report) (Q4, 2016).	€7.000,00	COD3		N/A	€7.000,00		15/01/2016	15/05/2016
D8	Assist and advice Member States on the establishment and evaluation of NCSS (workshops Q1-Q4, 2016).	€15.000,00	COD1		Events Organisation Services F-COD-15-C37		€7.500,00	01/02/2016	15/10/2016
					Web Development services F-TCI-13-C17		€7.500,00	01/02/2016	15/10/2016
D9	Updated good practice guide on NCSS (report, Q4, 2016).	€35.000,00	COD1	Reopening of Comp (under FWC)	CIIP SCADA_F-COD-15-C01	€35.000,00		15/02/2016	01/11/2016
D11	On-request support for MS decision making in the areas of privacy and trust (Q4, 2016).	€10.000,00	COD2				€10.000,00		
WPK2.2.	**WPK2.2. Support EU institutions' capacity building**	**€27.000,00**							
D1	Review and adjust mechanism for production of info notes (Q1-4, 2016).	€7.000,00	COD3		N/A	€7.000,00		01/06/2016	30/09/2016
D3	Restricted. Upon request, support the assessment of existing policies/procedures/practices on NIS within EU institutions (workshop, meetings, Q1-4, 2016).	€20.000,00	COD1		Events Organisation Services F-COD-15-C37		€20.000,00	01/02/2016	15/10/2016
WPK.2.3.	**WPK2.3. Assist private sector capacity building**	**€25.000,00**							
D1	Recommendations for creating a cybersecurity culture and improving management level cybersecurity awareness (Q4, 2016).	€25.000,00	COD2		ENISA List of Experts		€20.000,00		
					Events Organisation Services F-COD-15-C37		€5.000,00		
WPK.2.4.	**WPK2.4. Assist in improving the general awareness**	**€104.000,00**							
D2	ENISA cyber challenge (Q2, 2016).	€10.000,00	COD3		N/A	€10.000,00		01/01/2016	30/11/2016

D3	Provide guidance and support for European Cyber-Security Month (dissemination material, Q4, 2016).	€25.000,00	COD2		ENISA List of Experts		€20.000,00		
					Events Organisation Services F-COD-15-C37		€5.000,00		
D4	Upgrade the online privacy tools portal and involve privacy experts from different fields (dissemination material, Q4, 2016).	€69.000,00	COD2	Negotiated tender (< €60k)		€59.000,00		01/03/2016	01/10/2016
					ENISA List of Experts		€10.000,00		
SO3		**€811.000,00**							
WPK3.1.	**WPK3.1. Supporting EU policy development**	**€210.000,00**							
D1	Contribute to EU policy in the area of cloud computing (workshops, meetings, Q1-Q4, 2016).	€15.000,00	COD1		Events Organisation Services F-COD-15-C37		€5.000,00	01/02/2016	01/10/2016
					ENISA List of Experts		€10.000,00	01/02/2016	15/10/2016
D2	Contribute to EU policy in the area of Smart Grids and ICS-SCADA (workshops, meetings, Q1-Q4, 2016).	€25.000,00	COD1		ENISA List of Experts		€20.000,00	01/02/2016	01/11/2016
					Events Organisation Services F-COD-15-C37		€5.000,00	01/02/2016	15/10/2016
D3	Support the policy discussions in the area of IT security certification (workshops, meetings, Q1-Q4, 2016).	€45.000,00	COD1	Reopening of Comp (under FWC)	CIIP SCADA_F-COD-15-C01	€40.000,00		01/03/2016	01/11/2016
					Events Organisation Services F-COD-15-C37		€5.000,00	01/02/2016	15/10/2016
D4	Contribute to EU policy in the area of finance (workshops, meetings, Q1-Q4, 2016).	€25.000,00	COD1		ENISA List of Experts		€25.000,00	01/02/2016	01/11/2016
D5	Recommendations for improving NIS in EU standardization policy (Q4, 2016).	€45.000,00	COD2		ENISA List of Experts		€20.000,00	01/01/2016	01/03/2016
					ENISA List of Experts		€25.000,00	01/01/2016	30/10/2016
D6	Restricted. Towards a DSM for NIS products and services (workshops, report, Q4, 2016).	€55.000,00	COD1	Open tender (> €60k)	N/A	€55.000,00		15/03/2016	01/11/2016
WPK.3.2.	**WPK3.2. Supporting EU policy implementation**	**€601.000,00**							
D1	Contribute to the establishment of the cooperation group (meetings, workshops, Q2-Q4, 2016)	€20.000,00	COD1		Events Organisation Services F-COD-15-C37		€15.000,00	15/02/2016	01/11/2016
					ENISA List of Experts		€5.000,00	01/02/2016	15/10/2016
D2	Advice on the implementation of mandatory incident reporting for DSPs – input to the Implementation Acts (report, workshop, Q4, 2016).	€100.000,00	COD1		ENISA List of Experts		€20.000,00	01/02/2016	01/11/2016
					Events Organisation Services F-COD-15-C37		€30.000,00	01/02/2016	01/11/2016
				Tender		€50.000,00		01/03/2016	10/12/2016
D3	Advice on the implementation of security requirements for DSPs – input to the Implementation Acts (report, workshop, Q4, 2016)	€100.000,00	COD1	Reopening of Comp (under FWC)	CIIP SCADA_F-COD-15-C01	€50.000,00	-	01/03/2016	01/11/2016
					Events Organisation Services F-COD-15-C37		€25.000,00	01/02/2016	15/10/2016
					ENISA List of Experts		€25.000,00	01/03/2016	10/12/2016

D4	Assist MS in the identification of operators of essential services (workshop, Q2-Q4, 2016)	€7.000,00	COD1		Events Organisation Services F-COD-15-C37		€7.000,00	01/03/2016	01/11/2016
D5	Evolution and state of the art of privacy enhancing technologies and their building blocks (Q4, 2016). -Report	€44.000,00	COD2	Negotiated tender (< €60k)		€39.000,00		01/04/2016	01/09/2016
	Evolution and state of the art of privacy enhancing technologies and their building blocks (Q4, 2016). -Event		COD2		Events Organisation Services F-COD-15-C37		€5.000,00	01/01/2016	30/10/2016
D6	2016 edition of the report on appropriate technological protection measures to preserve privacy and trust (Q4, 2016).	€40.000,00	COD2	Reopening of Comp (under FWC)	CRYPTO_F-COD-13-C23	€35.000,00		01/02/2016	01/02/2016
					ENISA List of Experts		€5.000,00		
D7	Data protection and security in online and mobile applications (i.e. healthcare) (Q4, 2016).	€35.000,00	COD2	Negotiated tender (< €60k)		€30.000,00		01/03/2016	01/10/2016
					ENISA List of Experts		€5.000,00	01/01/2016	30/10/2016
D8	Annual Privacy Forum (Q2, 2016).	€20.000,00	COD2	Cooperation contract		€20.000,00		01/07/2016	01/10/2016
D9	Guidelines for data controllers on securing the automated processing of personal data (Q4, 2016).	€35.000,00	COD2	Open tender (> €60k)		€35.000,00		01/02/2016	01/09/2016
D10	Annual incident analysis report (article 13 a) (workshop and report, Q3, 2016).	€21.000,00	COD1		Web Development services F-TCI-13-C17		€21.000,00	01/02/2016	01/09/2016
D11	Analysis of major root causes - Good Practices and Recommendations for NRAs and e-communication providers (workshop and report, Q4, 2016).	€45.000,00	COD1	Reopening of Comp (under FWC)	ECOM SEC_F-COD-15-C03	€45.000,00		15/03/2016	01/11/2016
D12	Contribute to EU policy in the area of electronic communications sector (workshops, meetings, Q1-Q4, 2016).	€25.000,00	COD1		ENISA List of Experts	€25.000,00		01/03/2016	01/11/2016
D13	Engaging eIDAS Competent Authorities in the implementation of article 19 (workshops, Q1-Q4, 2016).	€10.000,00	COD1		Events Organisation Services F-COD-15-C37		€10.000,00	01/02/2016	01/11/2016
D14	Guidelines for mandatory incident reporting in the context of eIDAS (report, Q4, 2016).	€20.000,00	COD1		ENISA List of Experts		€20.000,00	01/02/2016	01/11/2016
D15	Update on standards for trust services and electronic identification (Q4, 2016).	€34.000,00	COD2	Reopening of Comp (under FWC)		€34.000,00		01/03/2016	01/10/2016
D16	Report on security recommendations for relying parties of trust services (Q4, 2016).	€35.000,00	COD2	Reopening of Comp (under FWC)		€30.000,00		01/02/2016	01/09/2016
					ENISA List of Experts		€5.000,00	01/01/2016	30/10/2016
SO4		**€352.000,00**							
WPK.4.1.	**WPK4.1. Cyber crisis cooperation and exercises**	**€230.000,00**							
D1	Cyber Europe 2016: exercise plan and exercise (exercise Q4, 2016).	€170.000,00	COD3	Open tender (> €60k)		€100.000,00		01/02/2016	01/12/2016
				Reopening of Comp (under FWC)	3C EX_F-COD-13-C26	€40.000,00		01/03/2016	01/12/2016

					ENISA List of Experts		€10.000,00	01/02/2016	01/12/2016
					Events Organisation Services F-COD-15-C37		€20.000,00	01/01/2016	01/12/2016
D2	EuroSOPEx 2016: exercise plan and exercises (exercises Q4, 2016).	€20.000,00	COD3		Events Organisation Services F-COD-15-C37		€20.000,00	01/03/2016	01/11/2016
D3	Pan-European cyber exercises roadmap (report Q4, 2016).	€0,00	COD3			€0,00		01/01/2016	01/09/2016
D4	Cyber crisis cooperation procedures: follow up the NIS policy framework (report Q4, 2016).	€40.000,00	COD3	Reopening of Comp (under FWC)	3C EX_F-COD-13-C26	€30.000,00		01/02/2016	01/09/2016
					Events Organisation Services F-COD-15-C37		€10.000,00	01/04/2016	01/09/2016
WPK4.2.	**WPK4.2. NIS community building**	**€122.000,00**							
D1	Continuation of existing community efforts (European FI-ISAC, FIRST, TF-CSIRT-TI, etc.).	€20.000,00	COD3	Cooperation contract		€20.000,00		01/01/2016	01/05/2016
D2	Annual ENISA national and governmental CSIRT Workshop (Q4, 2016).	€10.000,00	COD3		Events Organisation Services F-COD-15-C37		€10.000,00	15/03/2016	31/05/2016
D3	Annual ENISA/EC3 Cybercrime Workshop (Q4, 2016).	€10.000,00	COD3		Events Organisation Services F-COD-15-C37		€10.000,00	15/06/2016	30/10/2016
D4	Supporting European network of MSs CSIRTs.	€42.000,00	COD3	Negotiated Procedure			€42.000,00	Q2	Q2
D5	Review on new operational communities' development (A-ISAC, etc.) (Q4, 2016).	€40.000,00	COD3	Negotiated tender (< €60k)		€40.000,00		15/04/2016	30/09/2016
	Total Budget for Strategic Objectives 1-4 (WP 2016)	**€2.000.000,00**				€1.497.000,00	€503.000,00		

	Horizontal operational activities								
HA1	**Management Board, Executive Board and PSG Secretariat**	**€216.000,00**							
	Directorate, MB, PSG, EB Secretariat	€130.000,00	DIR		Events Organisation Services F-COD-15-C37		€130.000,00	Q1-Q4	Q1-Q4
	Directorate Evaluation of Agency activities	€86.000,00	DIR		F-DIR-15-C12				20/05/2016
HA2	**National Liaison Officer Network**	**€20.000,00**							
	NLO Meeting	€20.000,00	COD4		Events Organisation Services II - F-COD-15-C37		€20.000,00	t.b.c.	Q2
HA3	**EU Relations**	**€0,00**							
HA4	**Spokesperson, Stakeholders Communication and Dissemination Activities**	**€160.000,00**							
	Media support and press release distribution, and outreach				Media Outreach & Monitoring Services P/22/11/PAU		€50.000,00	t.b.c	t.b.c

	Communications related events				Events Organisation Services F-COD-15-C37		€24.000,00	t.b.c	t.b.c
	Communication Support Services				Communication Support Services F-DIR-15-C33		€26.000,00	t.b.c	t.b.c
	Stakeholders Communication	€60.000,00	COD4						
	ENISA website redesign - follow up project				Web Development services - F-TCI-13-C17		€10.000,00	t.b.c	t.b.c
	ENISA templates update/corrections			Negotiated Procedure		€5.000,00		t.b.c	t.b.c
	AAR 2015			Negotiated Procedure		€3.500,00		t.b.c	t.b.c
	Work programme 2017			Negotiated Procedure		€3.500,00		t.b.c	t.b.c
	Image Library			Negotiated Procedure		€3.000,00		t.b.c	t.b.c
	Other agency-wide projects			Negotiated Procedure		€35.000,00		t.b.c	t.b.c
HA5	**Quality control and project office**	**€90.000,00**							
	Web Hosting		COD4		Web Hosting services - F-TCI-13-C17		€15.100,00	t.b.c	t.b.c
	Web Development		COD4		Web Development services - F-TCI-13-C17		€42.000,00	t.b.c	t.b.c
	Cloud resources		COD4	Negotiated Procedure		€9.500,00		t.b.c	t.b.c
	Other agency-wide projects		COD4			€22.400,00		t.b.c	t.b.c
	Total Operational budget (title 3) for Horizontal operational activities (WP2016)	**€486.000,00**							

ENISA

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

Athens office

1 Vasilissis Sofias and Meg. Alexandrou
Marousi
151 24 Athens
GREECE

Numéro de catalogue	ISBN	ISSN	DOI
TP-AF-16-001-EN-N	978-92-9204-169-4	2363-3115	10.2824/150042

PO Box 1309, 710 01 Heraklion, GREECE
Tel: +30 2814409710
info@enisa.europa.eu
www.enisa.europa.eu