Draft ENISA Work programme 2017

STATUS: DRAFT

VERSION: JANUARY, 2016

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.

Table of Contents

Foreword

The digital environment and digital economy are becoming increasingly important driving forces for growth in Europe. It is clear however, that the EU will not be able to achieve 'digital growth' in the absence of an approach to cybersecurity that engenders trust in the wider community. It is therefore logical that the roles and responsibilities of the European Union Agency for Network and Information Security (ENISA) have been evolving to support this move towards a more digital society. This can be seen as a recognition of the fact that Network and information security (NIS) plays a central role in the activities of designing, developing and maintaining information systems, networks and services.

The rate at which the area of NIS is currently growing presents a major challenge to the Agency, which seeks to optimise its performance by prioritising those areas where it can make the biggest impact. ENISA sets these priorities through its annual programme, which is developed in close cooperation with the ENISA Management Board (MB) and the Permanent Stakeholders Group (PSG). This document is the result of several rounds of consultations carried out since September 2015 till January 2016.

The operating model of, the Agency is based on the delivery of three main types of services to and in collaboration with the NIS community:

- Recommendations mainly in the form of reports addressed to its stakeholders.
- Support for policy development and implementation.
- 'Hands on' work involving and developing operational communities.

Through these activities, which have been formalised in terms of a number of strategic objectives, ENISA supports the EU and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security issues and incidents.

Document Structure

In this Work program the planned activities for 2017 to 2019 are presented alongside the detailed planning for 2017. The document follows the structure laid down by the new EC guidelines for Work programming documents provided in the context of Framework Financial Regulation.

A number of new tasks are foreseen in WP2017, which are linked with the implementation of the NIS directive. These tasks require additional resources and budget. The additional resources and budget are detailed in a separate Annex, Annex B.

The budget and resources allocations within the summary tables and Annexes are covering the request for additional resources in addition to the COM Multiannual Financial Framework (MAFF) 2014-2020.

List of Acronyms

ABB: Activity Based Budgeting
APF: Annual Privacy Forum
ASA: Administration and Support Activities
ARD: Administration and Resources Department
BEREC: Body of European Regulators of Electronic Communications
CE2016: Cyber Europe 2016
CEF: Connecting Europe Facility
CEP: Cyber Exercises Platform
CERT-EU: Computer Emergency Response Team for the EU Institutions, Bodies and Agencies
CEN: European Committee for Standardization
CENELEC: European Committee for Electrotechnical Standardization
CIIP: Critical Information Infrastructure Protection
CSCG: ETSI CEN-CENELEC Cyber Security Coordination Group
CSIRT: Computer Security Incidents Response Teams
COD: Core Operational Department
CSS: Cyber Security Strategy
DG: EC Directorate-General
DG CONNECT: EC Directorate-General CONNECT
DPA: Data Protection Authorities
DSM: Digital Single Market
E: Event, type of output i.e. conference, workshop, and seminar
EC: European Commission
EC3: European Cybercrime Centre, Europol
ECSM: European Cyber Security Month
ED: Executive Director
EDPS: European Data Protection Supervisor
eID: electronic Identity
ENISA: European Union Agency for Network and Information Security
ETSI: European Telecommunications Standards Institute
EU: European Union
FAP: Finance, Accounting & Procurement section
FIRST: Forum of Incident Response and Security Teams
FM: Facilities Management
FTE: Full Time Equivalents
KGI: Key Goal Indicator
H2020: Horizon 2020
HoD: Head of Department
HR: Human Resources Section
IAS: Internal Audit Service
ICC & IAC: Internal Control Coordination and Internal Audit Capability
ICS: Industrial Control Systems
ICT: Information and Communication Technologies
IS: Information Systems
ISP: Internet Service Providers
IXP: Internet exchange point
KII: Key Impact Indicator
KPI: Key Performance Indicator
LEA: Law Enforcement Agency
MAFF: Multi Annual Financial framework

M2M: Machine to Machine
MB: Management Board
MS: Member State
NCSS: National Cyber Security Strategies
NIS: Network and Information Security
NLO: National Liaison Officer
NRA: National Regulatory Authority
O: Output
OQ: Operational Quality
P: Publication, type of output covering papers, reports, studies
PDCA: Plan-Do-Check-Act
PETs: Privacy Enhancing Technologies
PPP: Public Private Partnership
PSG: Permanent Stakeholders Group
Q: Quarter
R&D: Research and Development
S: Support activity, type of output
SCADA: Supervisory Control and Data Acquisition
SDO: Standard Developing Organization
SME: Small and Medium Enterprise
SO: Strategic Objectives
SOP: Standard Operating Procedure
TF-CSIRT: Task Force of Computer Security Incidents Response Teams
TLR: Traffic Light Rating
TRANSITS: Computer Security and Incident Response Team (CSIRT) personnel trainings
TSP: Trust Service Provider
US: United States of America
WP: Work programme
WPK: Work Package

List of Policy References

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

Nr.	Policy document	Complete title and link
1	**The new ENISA Regulation (EU) No 526/2013**	REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:L:2013:165:TOC Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.
2	**The Cybersecurity Strategy of the EU**	Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, available at: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
3	**The proposal for NIS directive**	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52013PC0048
4	**Council Conclusions on the Cybersecurity Strategy**	Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, agreed by the General Affairs Council on 25 June 2013, http://register.consilium.europa.eu/pdf/en/13/st12/st12109.en13.pdf
5	**Digital Agenda**	A Digital Agenda for Europe, COM(2010)245, May, 2010
6	**Directive on ECIs**	Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
7	**The CIIP Action Plan**	The Commission Communication “Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience” COM(2009)149, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF
8	**Commission Communication on Critical Information Infrastructure Protection**	The Commission Communication on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security" adopted on 31 March 2011 and the Council Conclusion on CIIP of May 2011, http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf
9	**Electronic Communications Regulatory Framework**	Regulatory framework for electronic communications (including article 13a and whole Chapter IIIa “Security and Integrity of networks and services”, More links available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al24216a
10	**Review of the Data Protection Framework**	Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM 2012/11 final of 25.1.2012, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
11	**Regulation on electronic identification and trusted services for electronic transactions in the internal market (eIDAS regulation)**	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
12	**Commission Regulation on the measures applicable to the notification of personal data breaches**	Commission Regulation (EU) No 611/2013, of 24 June 2013, on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF
13	**Framework to build trust in the Digital single market for e-commerce and online services**	European Commission, “A coherent framework for building trust in the Digital Single Market for e-commerce and online services” COM (2011)942, 11.1.2012, http://ec.europa.eu/internal_market/e-commerce/communication_2012_en.htm
14	**Directive on attacks against information systems**	Directive 2013/40/EU of the European Parliament and the Council of 12 August 2013 replacing Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013L0040

15	**Communication on EC3**	Commission Communication 'Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre', European Commission, COM(2012) 140 final, 28.3.2012, available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/communication_european_cybercrime_centre_en.pdf
16	**Council Resolution of December 2009 on a collaborative approach to Network and Information Security**	Council resolution of 18 December, 2009 on a collaborative approach to network and information security (2009/C 321 01), available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:C:2009:321:TOC
17	**Council conclusion on CIIP of May 2011**	Council Conclusion on CIIP of May 2011, available at: http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf
18	**Action Plan for an innovative and competitive Security Industry**	Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee regarding an Action Plan for an innovative and competitive Security Industry, COM(2012) 417 final
19	**Single Market Act**	Single Market Act – Twelve levers to boost growth and strengthen confidence "Working Together To Create New Growth", COM(2011)206 Final
20	**Internet of Things – An Action Plan for Europe**	Communication of the Commission to the Parliament, the Council, the EU Economic and Social Committee and the Committee of Regions on the Internet of Things, COM(2009)278 final of 18. June 2009.
21	**European cloud computing strategy**	The Communication COM(2012)529 'Unleashing the potential of cloud computing in Europe', adopted on 27 September 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF
22	**Internal Security Strategy for the European Union**	An internal security strategy for the European Union (6870/10), http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/113055.pdf
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 Strategy**	A Digital Single Market Strategy for Europe, COM(2015) 192 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the regions, May 2015, available at: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf
26	**Communication on Thriving Data Driven Economy**	Towards a thriving data-driven economy, COM(2014) 442 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the regions, July, 2014, available at: https://ec.europa.eu/digital-agenda/en/news/communication-data-driven-economy
27	**Framework Financial Regulation**	Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R1271

Mission Statement

The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe. ENISA supports the EU and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents. This is reflected in ENISA's mission statement:

Securing Europe's information society

In terms of the vision statement, By 2020 ENISA should:

- Be '**the hub'** for exchange of information on cybersecurity between the EU public sector and Member States.
- Have developed its operational model, based on recommendations, policy support and 'hands on' work so as to provide seamless support to its stakeholders in all areas covered by the mandate.
- Have an established presence in all key industry sectors and be a recognised name among security professionals.
- Be able to demonstrate a positive contribution to EU economic growth through its initiatives.

Adding Value through Complementarity

ENISA is a 'Centre of Expertise' in Network & Information Security and, as such, supports all phases of the security lifecycle including policy definition, policy implementation and maintenance and improvement of live operational solutions.

The Agency is complementary to other EU institutions in that it concentrates on identifying and disseminating pragmatic solutions to current problems in live operational environments. This enables EU industry to learn from each other and to implement strong security solutions at optimal cost, thereby contributing to their competitiveness in international markets.

The lessons learned from these environments are also communicated to EU and national policy makers so as to ensure that future policy initiatives are based on sound experience and solutions that are known to work. This 'bottom-up' approach to defining EU policy is well illustrated by the pan-European Cybersecurity Exercise in which all EU Member States participate.

Achieving Results by Leveraging the Stakeholder Community

ENISA believes strongly that the people best positioned to solve the security issues facing its stakeholder communities are the communities themselves. For this reason, every ENISA project is carried out in close collaboration with representatives of the appropriate stakeholder community. ENISA's results are therefore produced 'by the community, for the community'. Such an approach is inherently scalable and ensures a high degree of buy-in by those concerned.

Creating European Solutions to Enable EU Industry

The role of ENISA is to guide experts towards security solutions that are adapted to the needs of the internal market. By encouraging strong cooperation across national borders and across communities, the Agency promotes the development of approaches to security that are not hampered by national

restrictions or the ideas of particular communities. This results in solutions that are interoperable across the EU, thereby decreasing costs and enabling EU industry to benefit from a wider market.

Using Security to Strengthen Privacy

In addition to supporting EU industry, ENISA plays a unique role in supporting fundamental human rights through appropriate implementation of security techniques.

In recent years the Agency has been active in the area of privacy and Data Protection and we are well positioned to offer guidance on suitable implementation measures for implementing the General Data Protection Legislation when it comes into force. By concentrating on implementation measures, the Agency will complement the significant work that has gone into defining the legal framework.

Bridging Public & Private Sectors

One of the key roles of ENISA is to stimulate an active dialogue on cybersecurity between the public and private sectors and to ensure that this dialogue results in concrete action plans and ultimately impact in the form of improved cybersecurity practices.

ENISA achieves this through a variety of mechanisms, including support for public private partnerships, collaboration with standardisation and certification bodies, liaison with research communities and consultation of specialist groups (consumer protection, human rights, etc.).

Acting as a neutral third party with a mandate to improve EU cybersecurity, we are uniquely positioned to bring groups with differing interests together in order to define mutually beneficial solutions.

1. Section I – General Context

The ENISA Threat Landscape for 2015 drew a number of interesting conclusions regarding the evolution of the threat environment.

Cyber-threats have undergone significant evolution and breaches have increasingly covered front pages of media. Cyber-threat agents have had the time and resources to implement a series of advancements in malicious practices. In particular:

- Performing persistent attacks based on hardware, far below the "radar" of available defence tools and methods.
- Achieving enhancements in the provision of "cyber-crime-as-a-service", tool developments for non-experts and affiliate programmes.
- Highly efficient development of malware weaponization and automated tools to detect and exploit vulnerabilities.
- Campaigning with highly profitable malicious infrastructures and malware to breach data and hold end-user devices to ransom.
- Broadening of the attack surface to include routers, firmware and internet of things.

Where mitigation efforts are concerned, improvements have been achieved in coordinated campaigns to disturb operations of malicious infrastructures, strengthen the legal/governmental cyber-defence framework and develop more efficient products. In particular:

- Performing orchestrated actions to take down malicious infrastructure but also to analyse incidents and improve attribution.
- Strengthening governmental awareness, cyber-defence expenses, capabilities and level of cooperation among states.
- Performing exercises, development of threat intelligence, proliferation of information sharing, tools and products to enhance awareness, preparedness and efficiency of defence.
- Focusing on research and development to accommodate developments of the cyber-threat landscape to existing protection measures and methods and tools.

These are qualities that have been consistently developed throughout 2015 and have reached a momentum that allows for a persistent course of action.

The report notes that threat intelligence collection, management and sharing should become an inherent part of the national cybersecurity capabilities. In order to achieve this, policy makers should encourage voluntary reporting and perform analysis of reported incidents, recycling results for better planning. Finally, cyber-threat knowledge should be disseminated to all players in cyber-space, including end-users.

Businesses need to continuously adapt protection and detection tools to the threats. They should also strive to simplify the content of threat intelligence to achieve wider uptake in the stakeholder community. Threat agent models need to be improved and become an inherent part of threat intelligence.

Looking further ahead, research projects should develop applied statistic models to increase comparability of cyber-threat and incident information. Similarly, we need new models for security controls to be included in complex, smart end-user environments. The fact that the Internet of Things (IoT) is actively being rolled out means that developing trust models for the ad hoc interoperability of devices within smart environments now becomes a priority.

Finally, regarding the overall highlights for the future cyber-threat landscapes, two overarching trends for defenders and adversaries respectively have been identified:

- The need for "*Streamlining and consolidation*" of existing policies, defences and cooperation to accommodate changes in threat landscape and
- Ongoing activities towards "*Consumerization of cyber-crime*", that is, making malicious tools available to everybody.

2. Section II Multi-annual programming 2017 – 2019

2.1 Multi-annual objectives

The multiannual objectives of the Agencies are inspired from the ENISA regulation and are part of ENISA strategy. The objectives of the Agency are structured around 5 activities, presented in more detail in section 2.2, and referred throughout the document with the following suggestive names: expertise, policy, capacity, community and enabling. Next to these activities, one more activity is the administration and resourcing functions of the Agency.

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

In section 2.3 a summary of indicators and targets is presented, providing the mechanisms to quantify the progress and the achievements of the Agency.

2.2 Multi-annual programme

This section reflects the long term core priority objectives for the Agency and presents them in a structured and concise manner following the structure of the ENISA strategy.

The ENISA strategy was built with the aim to support ENISA's Executive Director and MB in the elaboration and adoption of consistent multiannual and annual work programmes[1]. This strategy defines five strategic objectives that will form the basis of future multi-annual plans[2].

ENISA's strategic objectives are derived from the ENISA regulation, inputs from the Member States and relevant communities, including the private sector. These objectives state that ENISA, in cooperation and in support to the Member States and the Union institutions, will:

#Expertise. Anticipate and support Europe in facing emerging network and information security challenges, by collating, analysing and making available information and expertise on key NIS issues potentially impacting the EU taking into account the evolutions of the digital environment.

#Policy. Promote network and information security as an EU policy priority, by assisting the European Union institutions and Member States in developing and implementing EU policies and law related to NIS.

#Capacity. Support Europe maintaining state-of-the-art network and information security capacities, by assisting the Member States and European bodies in reinforcing their NIS capacities.

[1] Annual and multiannual work programmes (article 5 §2)
[2] In order to achieve the 5 year strategic objectives laid out in this document, the multiannual work programme will provide prioritized mid-term operational objectives to be achieved by ENISA within a period of 3 years. Annual concrete activities (outputs) will be identified in the annual work programmes, according to a recursive approach in order to achieve the mid-term operational objectives and in the long term the strategic objectives.

#Community. Foster the emerging European network and information security community, by reinforcing cooperation at EU level among Member States, European Union bodies and relevant NIS stakeholders, including the private sector.

#Enabling. Reinforce ENISA's impact, by improving the management of its resources and engaging more efficiently with its stakeholders, including Member States and Union Institutions, as well as at international level.

In addition to these five strategic objectives, the Agency will seek to:

#Compliance and resourcing. Comply with legal and financial requirements and provide Human resources, Budget, IT infrastructure, etc. in line with the operational objectives.

2.2.1 Activity 1 – Expertise. Anticipate and support Europe in facing emerging network and information security challenges

In order to achieve this objective, ENISA will collate, analyse and make available information and expertise on key NIS issues potentially impacting the EU taking into account the evolutions of the digital environment.

ENISA will collate, analyse and make available information on global cyber issues with a view to developing insights on issues of high added-value for the EU. In this analysis, ENISA will cover both existing as well as new technologies and their integration, such as smart infrastructures, Internet of Things, Cloud and Big Data and evaluate their impact on NIS and related challenges such as NIS aspects of data protection.

To that end, ENISA will bring together Member States relevant stakeholders, such as industry, providers of electronic communications networks or services available to the public, consumer groups, academic experts in network and information security, and representatives of national regulatory authorities related to NIS in order to discuss and explore NIS problems and challenges that they have encountered.

By compiling, comparing and evaluating these experiences alongside publicly available data, ENISA will help to anticipate future risks and threats and identify those technologies and services that pose specific security challenges in particular with regard to critical infrastructures, businesses at large and citizen's private data.

In response to this the agency will develop and disseminate best practices which can be used to inform across a number of different horizontal fields including research and development, innovation, standardization, IT Security certification and other relevant industrial practices.

This activity has 4 main objectives:

- Objective 1.1. Improving the expertise related to Critical Information Infrastructures
  - Under this objective, the Agency carries out work designed to improve the expertise related to CII.
- Objective 1.2. NIS Threats Landscape and Analysis
  - The objective here is to support NIS community by providing NIS threat analysis as well as to provide analysis reports linked to the activities carried out by the Agency in collection of incidents.
- Objective 1.3. Research & Development, Innovation

- The objective of this work is to assist in bridging the gap between research, innovation and deployment in the area of NIS as well as to provide ideas for future research that could contribute to better NIS.
- Objective 1.4. Response to Article 14 requests under Expertise activity
  - Under this Objective the Agency will perform tasks following Article 14 Requests.

2.2.2 Activity 2 – Policy. Promote network and information security an EU policy priority

In order to achieve this objective, ENISA will assist and advise the Union institutions and the Member States in developing and implementing EU policies, guidance and law on all matters relating to NIS.

Building upon its expertise gathered while achieving objective 1, ENISA will assist and advise the Union institutions and the Member States in

- Developing European NIS related policies and laws. To this end, ENISA will proactively engage with Union institutions, and in particular all relevant DGs of the European Commission, in order to advise, including by providing preparatory work, advice and analyses relating to the development and update of Union NIS policy and law.
  In cooperation with the Member States, in particular as part of the work of the Cooperation group, as well as with other relevant public and private stakeholders, ENISA will promote a vision on how to significantly strengthen NIS across the EU, using adequate EU policy levers. ENISA will, in particular, promote the inclusion of NIS aspects within policies including – directly or indirectly – a digital dimension. ENISA will also actively contribute to the reinforcement of NIS as a driver of the DSM and more generally of economic growth in Europe, including the development of NIS and related ICT industries in Europe.
- Implementing, at EU level, NIS related policies and law, following their adoption. While ENISA, focusing in particular on the implementation of the NIS Directive, will support cooperation among Member States regarding EU policies and law including a NIS dimension in order to foster consistent EU-wide approach to their implementation. ENISA will bring together Member States and other relevant public and private stakeholders, and will seek to produce recommendations taking into account their needs and constraints (national, sectorial).[3]

Activities carried out under this objective are grouped in 3 main areas/sub-objectives:

- Objective 2.1. Supporting EU policy development.
  - This objective covers developing European NIS related policies and laws.
- Objective 2.2. Supporting EU policy implementation
  - This objective covers all the activities linked to implementing, at EU level, NIS related policies and law, following their adoption.
- Objective 2.3. Response to Article 14 requests under Policy activity
  - Under this Objective the Agency will perform tasks following Article 14 Requests.

[3] This objective should not be confused with ENISA's support provided to single Member States requesting assistance pursuant to Art. 14 of ENISA Regulation (EU) No 526/2013 in implementing EU regulations' specific provisions at national level, as part of objective 3 regarding ENISA's support to capacity building.

2.2.3 Activity 3 – Capacity. Support Europe in maintaining state-of-the-art network and information security capacities

In order to achieve this objective, ENISA will assist the Member States and the Union institutions in reinforcing their NIS capacities.

ENISA will support capacity building across the Union to make national public and private sectors and the Union institutions' networks more resilient and secure. This will involve working closely with Member States and liaising, in cooperation with them, with various different stakeholders across the Union to develop skills and competencies in the field of NIS.

ENISA will focus its effort on the following actors:

- Member States: ENISA will support the development of Member States' national NIS capabilities by providing recommendations on key dimensions of NIS capacity building and will focus in priority on those highlighted in the NIS Directive, including on the development and efficient functioning of National/Governmental CSIRTs and policy level collaboration between national competent authorities in the framework of the Cooperation Group, the development of national strategies, the establishment of necessary national frameworks to aid implementation of national incident reporting schemes and on training to improve skills. ENISA will as well offer, upon their request, direct to support to single Member States[4]. To that end, the Agency will develop proactive relationships with Governments across the EU.
- Private sector: ENISA will support Member States to engage with private sector on their NIS, encouraging companies to take a whole-business approach to cyber threats from the top of the board down. ENISA will also work with private sector stakeholders to help improve cyber security of networks within companies.
- Union institutions: in close coordination with the Union institutions, ENISA will support them in reinforcing and coordinating their NIS capabilities and to that end, will establish a close and sustainable partnership with CERT-EU. As part of this mission, ENISA will advise on key orientations and, upon request, on actions to be implemented in order to achieve a high level of NIS across all Union institutions. ENISA will, also, produce with CERT-EU information notes on threats and risks with a view to making the EUIs and agencies more secure. ENISA will, whenever this is adequate, build on experience gained by CERT-EU and the Union institutions to contribute to the broader EU NIS community.
- Citizens: alongside Member States, ENISA will help EU citizens to gain essential cyber security knowledge and skills to help protect their digital lives. This will include promoting an annual European Cyber Security month and working with the Member States delivering projects like the Cyber Security Challenge as well as national initiatives, upon request from a Member State.

While aiming at supporting different types of actors, ENISA will take into account the transversal aspects of NIS capacity building such as activities supporting the increase of the number of NIS experts in Europe (e.g. academic training) and the spread of basic cyber hygiene in public and private organizations as well as in the general public.

To achieve this, the activities covering capacity building are structured in 5 objectives, targeting the above mentioned four main actors:

- Objective 3.1. Assist Member States' capacity building.

[4] Article 14 of ENISA Regulation (EU) No 526/2013

- Under this objective, ENISA will support the development of Member States' national NIS capabilities.
- Objective 3.2. Support EU institutions' capacity building.
  - This objective covers all activities that ENISA will carry in close cooperation with the Union institutions to support them in reinforcing their NIS capabilities.
- Objective 3.3. Assist private sector capacity building.
  - ENISA will work with private sector stakeholders, supporting Member States to help improve cyber security of networks and information..
- Objective 3.4. Assist in improving general awareness
  - This objective covers the activities addressed to EU citizens built together with EU institutions and MS, such as promoting an annual European Cyber Security month and working with the Member States delivering projects like the Cyber Security Challenge.
- Objective 3.5. Response to Article 14 requests under Capacity activity
  - Under this Objective the Agency will perform tasks following Article 14 Requests. ENISA will offer, upon request, direct support to single Member States and to EU institutions.

2.2.4 Activity 4 – Community. Foster the emerging European Network and Information Security Community

Beyond its support to the development and the implementation of EU NIS related policies (Activity 2) and to Member States and Union institutions towards the development of their NIS capabilities (Activity 3), ENISA will actively support cooperation at EU level on NIS.

ENISA will in particular seek to support in priority:

- CSIRT cooperation among the Member States, by supporting voluntary cooperation among Member States CSIRTs, within the CSIRT network established by the NIS Directive. As part of this activity, ENISA will provide the secretariat of this network and actively support its functioning by suggesting ways to improve cooperation among CSIRTs and supporting this cooperation, including by developing and providing guidance on best practices in the area of operational community efforts, such as on information exchange.
- Cyber crisis cooperation among Member States, by continuing to support the organization of the Cyber Europe exercises which shall remain one of ENISA's key priority activities, while ensuring adequate synergies with the CSIRT network.
- Dialogue among NIS related communities, including between CSIRTs and law enforcement and data privacy communities, in order to support consistent EU-wide approach to NIS. To that end, ENISA will continue to interact with Europol (EC3).
- Dialogue among public and private sectors on relevant NIS issues of European general interest, in particular with a view to contribute to the objectives of the Digital Single Market, such as stimulating the development and the competitiveness of NIS and ICT related industries and services in Europe.

In order to achieve this scope, ENISA will enhance cooperation at EU level among Member States, Union institutions and related NIS stakeholders, including private sector and will focus on three objectives:

- Objective 4.1. Cyber crisis cooperation.
  - ENISA will rely upon its expertise developed within the framework of the organization of the Cyber Europe exercises that it will continue to develop and which shall remain one of ENISA's key priority activities.

- Objective 4.2. CSIRT and other NIS community building.
  - In line with the proposed NIS Directive, ENISA will support the cooperation among CSIRTs, within an EU Member States CSIRTs network, subject to its establishment. As part of this activity, ENISA will provide the secretariat of this network and actively support its functioning by suggesting ways to improve cooperation among CSIRTs and supporting this cooperation, including by developing and providing guidance on best practices in the area of operational community efforts, such as on information exchange.
  - Furthermore the agency will contribute to the dialogue among NIS related communities, including between CSIRTs and law enforcement and data privacy communities, in order to support consistent EU-wide approach to NIS.
- Objective 4.3. Response to Article 14 requests under Community activity
  - Under this Objective the Agency will perform tasks following Article 14 Requests linked to the previous 2 objectives.

2.2.5 Activity 5 – Enabling. Reinforce ENISA's impact

This activity aims to improve coordination of the Agency's activities and to improve the cooperation with Agency's relevant stakeholders.

In order to achieve this horizontal objective, ENISA will improve the management of its resources and engage more efficiently with its stakeholders, including Member States and Union institutions, as well at international level.

- Objective 5.1. Management
  - The Agency will act according to the following key general principles and rules:
    - ENISA will ensure a responsible financial management of its resources. In the next five years, ENISA will continue to improve processes for monitoring financial flows and expects to maintain high commitment and payment rates.
    - ENISA will guarantee a high level of transparency regarding its internal processes and way of working.
    - ENISA will increase and maintain internal IT-security expertise within the Operational Department, with a view to lowering the need to rely upon external experts, in particular in developing and maintaining a high level of expertise (objective 1 of the ENISA Regulation).
- Objective 5.2. Engagement with stakeholders
  - ENISA will continue to improve the quality and effectiveness of its relations with Member States' NIS competent authorities. ENISA will, in particular, make it easier for the national competent authorities to engage with the Agency, while offering better visibility on its activities. To this end, ENISA will define Standard Procedures regarding the principles and modalities of the participation and consultation of national competent authorities and other NIS related communities as part of its activities. It will also engage with the national competent authorities actively participating in the work of Cooperation Group established by the NIS directive. ENISA will also establish an updated list of its ongoing and future activities, including relevant contact and calendar information for Member States and NIS communities to facilitate their engagement with ENISA.
  - ENISA will reinforce and structure its cooperation with all Union institutions, entities and bodies on NIS related issues, in particular the European Commission, as well as CERT-EU on the NIS of the Union institutions, and Europol (EC3) with regard to community building between national NIS and law enforcement communities.

- ENISA will continue to improve the quality and effectiveness of its relations with other relevant stakeholders, such as NIS and ICT related industries and services, essential operators, providers of electronic communications networks or services available to the public, consumer groups, academic experts in network and information security.
- While developing its expertise, ENISA will avoid duplicating existing work at National level and will focus on issues of real-added value for Europe.

- Objective 5.3. International activities
  - ENISA will act at international level according to EU and Member States' external policies and guiding principles to be defined and adopted by the MB. ENISA's international relations should primarily aim at supporting EU's external policy initiatives including a cyber dimension and promoting the EU and its NIS expertise outside its borders.

2.2.6 Activity 6 – Compliance and resourcing

The ENISA Administration and Resources strives to operate a cost-efficient strategy to resource the Agency with appropriate means to enable the other objectives. Administration and Resources allows a compliant decision making process vis-à-vis ENISA internal and external stakeholders in respect of the European taxpayers, resulting in innovative solutions and quality results for the staff members and external stakeholders, under our legal and financial framework.

The main activities includes Human Resources, Finance, Accounting, Procurement, Information and Communication Technology, Security Protocol, Host Country Relations, Internal Communication, Legal Affairs, Internal Quality Management Systems and Internal Control Coordination.

The Human Resources ensure that the best and most qualified personnel are recruited in the Agency.

The activities of Finance, Procurement & Accounting consist in resourcing the Agency management through efficient management of budget and expenditure.

The activities of Information and Communication Technology include delivering IT systems and services to the Agency across its two fully functional offices and to its highly mobile user-base keeping a high level of IT security.

Organisational culture is inextricably linked with internal communication. Without communication an organisational culture cannot be built and changed. Internal communication mirroring culture within the organisation helps keeping employees satisfied and thereby ties employees to an organisation.

Legal Affairs is to support all the legal aspects associated with the operation of the Agency.

Quality Management Systems are to reach internal systems to effectively improve procedures, efficiency and resilience, reduce risks by having an internal control framework that allow recognition of events, analysis and improvement. This also result into a learning organization with preventive and remedied actions.

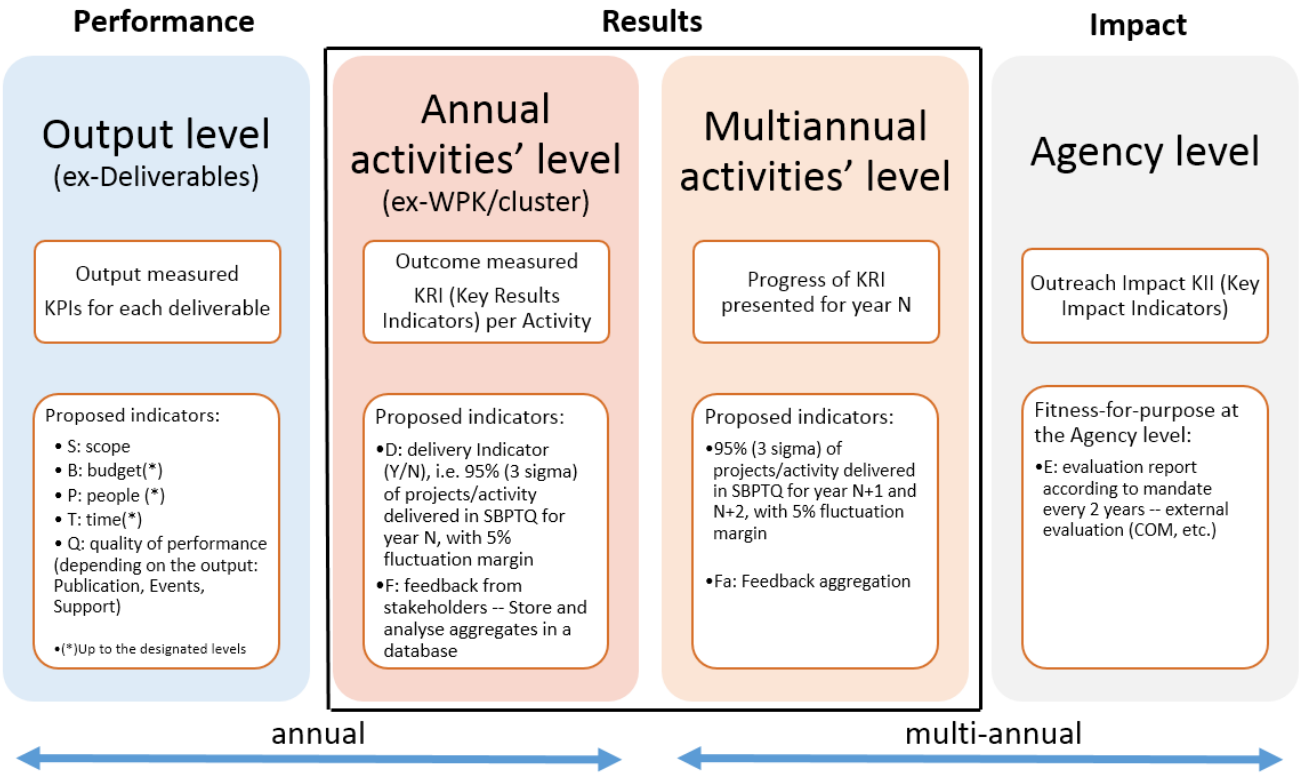
The Internal Control Coordination activities are to coordinate the risks, driving Risk Management as a regular process. It drives and coordinate the assessment of the Internal Control systems as a regular process (ICS 15). He facilitate and coordinate the Risk Assessment (ICS6) process and exercise inside the Agency. It support relationship between the European Court of Auditors and the Internal Audit Services.

2.3 Monitoring the Progress and the Achievements of the Agency. Summarizing the Key Indicators for the multi-annual activities

The Agency has started a process for improving the standing of its key indicators for the purpose of measuring and reporting better and more accurately against its annual work program, in line with the prescribed Commission approach.

The purpose of key indicators for ENISA is to provide the metrics to measure against performance, results and impact of the Agency's outcome, output and impact. Key indicators seek to better support policy dynamics on network and information security, an area of policy that largely still remains under development at the EU level, as technology and business models evolve.

The chosen approach initially sets the designated levels of key indicators; each type of indicator is grouped alongside other similar ones at the appropriate level. This approach has been developed taking into account the capability of the Agency to report, and the need to avoid any unnecessary burden on the Agency. The Agency capability to report reflects, effort, organisational measures as well as tools available or that can be obtained relatively easily. Measuring operational performance that concerns the policy raison d'être of the Agency remains the focal point for the key indicators introduced. The key notions and main vectors of annual and multi-annual measurements are presented hereunder:



Key indicators at ENISA seek to measure:

- Performance that is a concern at the output level when deliverables are produced. Metrics used, are project management-based and they include:
  a. Adherence to the scope of the deliverable or project
  b. Budget (or financial resources) available to the output or project, remaining within prescribed levels with a ±5% margin
  c. People (or human resources) available to the output or project, remaining within prescribed levels with a ±5% margin
  d. Time available to carry out the output or project remaining within prescribed levels with a ±5% margin
  e. Quality of performance depending on the type of output, according to the classification of output in the work program (being, publication, event, support).

- Results that are a concern at the annual and at multi-annual activities' level. The indicators used are as follows:
  a. Delivery indicator aiming at delivery of at least 95% against work program planning. This is equivalent to a 3σ (3 Sigma) organisation (reaching between 93.3% and 99,3%); clearly the Agency has historically proven its operational ability to deliver at much higher level, meeting 6σ (6 Sigma) specification requirements (at 99,99%). However allowing for a 3 Sigma level meets the above-mentioned deviation rate of ±5%.[5] The criteria used, being scope, budget, people, time and quality, they all refer to the proper execution of the project leading up to the production of output. This evaluation is done at the end of the project within ENISA.
  b. Following the production process that leads up to an output, feedback from stakeholders is collected on each output. Results are further aggregated on a multi-annual basis by the Agency.

- Impact is measured at the Agency level only; it is based on feedback received from the evaluation of the Agency's performance (own initiatives and commissioned consulting at the Agency's initiative) and/or institutional third party evaluations such as those commissioned by the European Commission, the European Court of Auditors etc.

[5] In a normal distribution σ (or sigma) denotes the distance between the mean value and the inflexion point. Shortening this distance is an indicator of enhanced quality of performance. While a Six Sigma (or, 6σ) methodology is beyond the scope of the current version of the QMS of the Agency portions thereof, are used in select areas, such as key indicators. In ENISA, the reference Standard Operating Procedure (SOP) hereto is the SOP PDCA (Plan-Do-Check-Act) that is a simplified version of the DMAIC (define-measure-analyse-improve-control) approach typically associated with Six Sigma. The choice for simplicity is obviously desirable while the implementation of a quality system is an ongoing concern. Six Sigma focuses on process control for the purpose of reducing or eliminating waste. Six Sigma utilizes historical data along with statistical analysis to measure and improve a company's operational performance e.g. processes, practices, and support systems. Six Sigma is a measure of process quality the variation of which is measured in six standard deviations from the mean.

The key indicators broken down at the output level, the activities level and the agency level, are presented hereunder:

Key indicators in ENISA								
Output level			**Activities level**			**Agency level**		
Scope (e.g. Scope drift as compared to approved WP plan)	S	Variable: TLR	Deliverables (number of deliverables realised against the WP plan)	D	Numerical: quantitative target	Evaluation (results' aggregates) Periodic Agency evaluation e.g. COM (2018), Ramboll etc.)	E	Variable: TLR
Budget (e.g. appropriations utilised and staff engaged in a project plus or minus 5%)	B	Variable: TLR	Feedback (number of positive and not so positive feedback) (*)	F	Numerical: quantitative target			
People (e.g. staff engaged in a project plus or minus 5%)	P	Variable: TLR	Feedback aggregates for multi-annual performance (**)	Fa	Numerical: quantitative target			
Time (e.g. duration of project plus or minus 5%)	T	Variable: TLR	(*) *Feedback via e.g. survey associated with deliverables on website*					
Quality (e.g. citations, downloads, MS participation etc.)	Q	Integer: quantitative target	(**)*Aggregations of deliverables or categories thereof*					

All rating indicators follow a variable Traffic Light Rating (TLR) system that is laid out as follows:

- Green, that reflects 5% deviation meaning that the planning / performance are appropriate and within prescribed levels.
- Yellow, that reflects 20% deviation meaning that the planning / performance need to be revisited.
- Red, which reflects deviation above 20% meaning that the planning / performance need thorough review.

Feedback is collected by means of surveys. It is envisaged that the deliverables part of the web-site will be leveraged to channel targeted feedback against each deliverable downloaded. This is a task however that will be made available as from 2018, at the earliest.

Below follows an example of output related indicators to be collected concerning the key types of Agency output, being Publication, Event, Support types of output.

#	KPI	Description	Output type (P) *	Output type (E)**	Output type (S)***
1	S	Defined in the planning phase and confirmed throughout delivery	Scope in start remains identical to scope in the end		
2	B	Budget remains within ±5% of designated budget level to cover requirements defined	Working group, external supplier, experts etc.	Logistics, reimbursements for speakers, catering, communication etc.	Technical equipment, services, communication, market research etc.
3	P	Staff allocated to remain within ±5% of designated FTEs	REF: Matrix data		
4	T	Project duration to remain within ±5% of planned time	REF: Matrix data		
5	Q	Any of the following quality indicators as appropriate	Number of MS involved, experts from MS authorities, Industry representatives, R&D etc., % population (survey) etc.	Number of participants, aggregation of feedback in event survey etc.	Number of subscribers, aggregation of feedback of participants; feedback of the Policy principal (e.g. COM /MS etc.)
*Publication e.g. methods for security and privacy cost analysis **Event e.g. WS on privacy and security ***Support e.g. NIS portal					

Below follows an example of outcome related indicators to be collected concerning the key types of Agency activities, at the annual and at the multi-annual level.

Aggregated outcome at the annual activity level in years n, n+1 and n+2				Multi-annual level
	Annual activity $_{x,y,z}$ in year n	Annual activity $_{x,y,z}$ in year n+1	Annual activity $_{x,y,z}$ in year n+2	Multi-annual activity $_{x,y,z}$ evolution
Delivery related	e.g. output instantiations 70% Green 20% Yellow 10% Red	e.g. output instantiations 80% Green 10% Yellow 10% Red	e.g. output instantiations 90% Green 10% Yellow 0% Red	In each 3 year period we aggregate on a per activity level: 80% Green 13% Yellow 7% Red
Feedback (external)	e.g. green feedback Out of 200 responses 45% positive 45% neutral 10% negative	e.g. green feedback Out of 200 responses 50% positive 40% neutral 10% negative	e.g. green feedback Out of 200 responses 55% positive 40% neutral 5% negative	In each 3 year period we aggregate on a per activity level: 50% positive 41% neutral 9% negative

2.4 Human and financial resource outlook for the years 2017-2019

2.4.1 Overview of the past and current situation.

WP 2017 is following the new COM guidelines and has a structure similar but not overlapping with previous years. Furthermore, the Work Programme is structured following the objectives and the priorities of the Agency as described in the new ENISA strategy.

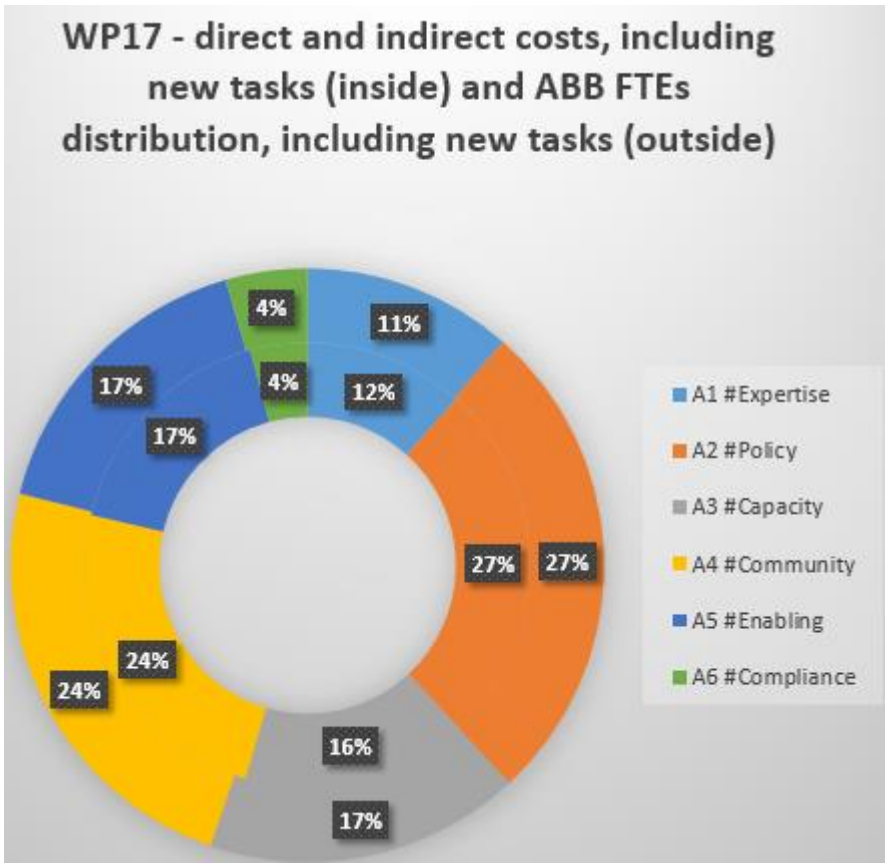
The human and financial resources of past and current situation are presented in the Annexes of this document.

2.4.2 Resource programming for the years 2017-2019

The distribution of budget and resources for 2017 for the activities A1 to A6 is presented in the chart hereunder. The budget and resources for each activity are presented in Section 3.7.2 in the summary table.

For years 2017-2019, the Agency will gradually increase the share of the activity 3, Capacity Building. The aim is to achieve a better balance of the resource distribution between capacity building and policy activities in the future, as policy is currently consuming significantly more resources than capacity building.

The budget and resources allocations within the summary table and Annexes are covering the request for additional resources in addition to the COM Multiannual Financial Framework (MAFF) 2014-2020. The additional resources and budget are detailed in a separate Annex, Annex B.



3. Section III. Work Programme Year 2017

The ENISA Work Programme for the year 2017 follows the structure presented in the multi-annual programming Section II. In this section clear objectives, results and indicators are identified for each activity.

The Activities presented in this section follow the structure of the ENISA strategy document. After a short description of the activity the Objectives are presented. A short narrative is included, consisting of a description and added value of the activity, the main challenges in Year N+1 and link to the multi-annual objectives.

The main outputs/ actions in the specific year, for this case for 2017, are listed within each Objective. For each Objective there are several Outputs defined.

Each Output includes:

- A description of the specific actions and outcome which are expected to contribute to the achievement of the objective,
- The type of output:
  - P: publication i.e. report, study, paper
  - E: event i.e. conference, workshop, seminar
  - S: support activity, involving assistance to or close collaboration with e.g. EU Institutions or Bodies or Member States as appropriate, with reference to a specific activity that features defined and shared objectives.
- Key performance indicators tailored for the type of Output.
- Resources and budget, in a summary table at the end of the section in aggregated form at activity level.

For each activity there is an Objective defined that covers the actions that the Agency is carrying to respond to Article 14 requests. Article 14 requests, named after the Article 14 of the ENISA regulation, allow the MS and EU institutions to make direct requests to ENISA seeking assistance or advice on specific activities.

3.1 Activity 1 – Expertise. Anticipate and support Europe in facing emerging network and information security challenges

This activity aims at developing and maintaining a high level of expertise of EU actors taking into account evolutions in NIS.

It covers the baseline security requirements, the threat landscape and activities related to research, development and innovation.

3.1.1 Objective 1.1. Improving the expertise related to Critical Information Infrastructures

The objective of the studies under this objective is to provide public and private stakeholders of Critical Information Infrastructures (CII) baseline security recommendations.

The objective will focus on 4 specific areas, namely energy, transport in the context of smart cities, IoT for CIIs and eHealth.

The baseline security recommendations will be based on existing national requirements, industry good practices and widely used relevant standards (e.g. ISO). The proposed outputs will be validated by the relevant stakeholders

3.1.1.1 Output O.1.1.1 – Baseline Security Recommendations for the Energy Sector

This study will develop baseline cyber security recommendations for energy operators, energy regulators and other relevant stakeholders.

The Agency will identify and analyse existing security practices (e.g. Germany's BNETZA's IT security requirements) and standards (e.g. ISO 27001) in all energy subsectors namely electrical power, renewable energy, oil and gas industries. ENISA will analyse and compare these practices and standards so as to identify the minimum common denominator to be adopted. The Agency will focus, among others, on energy distribution, energy supply and interdependences among operators.

Based on the analysis a different set of security measures will be developed for the three different elements of the energy production and delivery line: production, transmission and distribution. Privacy and data protection requirements will be addressed with a focus on the distribution element.

In this endeavour the Agency will take into account the EU policy and regulatory context (especially Cybersecurity of Energy supply – new legislative initiative), follow the activities of the European Energy Sector Cyber Security Platform (EECSP) and participate as member in the Expert Group on European Energy Sector Cyber Security Strategy.

The Agency will also validate the results of the study with relevant information sharing initiatives such as TNCEIP, EE-ISAC and ENTSO-E cyber security subgroup and finally interact with all important energy sector stakeholders from public sector such as DG-ENER, JRC, ACER and CEER and from the private sector such as ENTSO-E, ENTSO-G, ESMIG, Eurelectric and EDSOs. That would allow the Agency to develop a map of key stakeholders and initiatives in Europe.

The proper validation of the proposed baseline security requirements by the private and public sector would pave the way for a wide, de-facto, tacit adoption of it which could constitute the basis for EU harmonisation.

This work item builds on previous work of ENISA in the area of Minimum Security Measures (WP 2016) and Smart Grids (WP 2012-2015).

Type of Output:

- P: Baseline Security Recommendations for the Energy Sector, Q4
- E: 1 validation workshop with targeted stakeholders, Q3-Q4

Performance Indicator:

- By 2017 engage 10 leading energy operators and 10 MS Competent Authorities in the study
- By 2019 more than 12 EU MS de-facto use ENISA's baseline security requirements

3.1.1.2 Output O.1.1.2 – Baseline Security Recommendations for the Transport Sector in the context of Smart Cities

This study will develop baseline cyber security recommendations for transport operators in the context of smart cities.

The Agency will identify and analyse existing security practices and standards in the area of transportation for smart cities. ENISA will compare these practices and standards and develop baseline security measures to be adopted by relevant stakeholders.

The Agency will focus, among others, on traffic and vehicle management, power distribution systems, intelligent vehicles, vehicle to vehicle communication, vehicle to internet, vehicle to infrastructure communication, and interdependences among multi-modal operators in the context of smart cities. Also the study will analyse the interface between city authorities and transport operators and take a full-systems approach ranging from user payment mechanisms to privacy of data shared between operators.

In this endeavour the Agency will take into account existing EU policy and regulatory context (e.g. EU's Action Plan for the Deployment of Intelligent Transport Systems in Europe, and EU's Digital Single Market Strategy, and the Roadmap to a Single European Transport Area – Towards a competitive and resource efficient transport system).

The Agency will also validate the results of the study with relevant national and EU initiatives (e.g. ERTRAC) and interact with all important transport/smart cities stakeholders from public sector such as DG-MOVE, JRC, ERA (European Railway Agency) and from the private sector.

The proper validation of the proposed baseline security requirements by the private and public sector would pave the way for a wide, de-facto, tacit adoption of it which could constitute the basis for EU harmonisation.

This work item builds on previous work of ENISA in the area of intelligent transportation systems used in the context of smart cities (WP 2015 - 2016).

Type of Output

- P: Baseline Security recommendations for the Transport Sector in the context of Smart Cities, Q4
- E: 1 validation workshops with targeted stakeholders, Q2-Q4

Performance Indicator

- By 2017 engage 10 leading urban transport infrastructure operators and 10 MS Competent Authorities in the study
- By 2019 more than 15 EU MS de-facto use ENISA's baseline security requirements

3.1.1.3 Output O.1.1.3 – Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures

This study will develop baseline cyber security recommendations for Critical Information Infrastructure asset owners who use the concept of IoT to provide their services.

The Agency will identify and analyse existing security practices and standards in the area of IoT security for CII (e,g. Industry 4.0, M2M communications, SDN and 5G networks). ENISA will compare these practices and standards and develop baseline security measures to be adopted by all relevant stakeholders.

The Agency will focus, among others, on IoT resilience and communication, interoperability with proprietary systems, trustability of IoTs, and other. Special emphasis will be given to the privacy issues of such smart infrastructure and services.

In this endeavour the Agency will take into account and contribute to existing EU policy and regulatory initiatives (e.g. Internet of Things - An action plan for Europe, The Alliance for the Internet of Things (AIOTI), the 5G Infrastructure Pubic Private Partnership (5G PPP)).

The Agency will also validate the results of the study (e.g. via joint workshops) with relevant national and EU initiatives (e.g. AIOTI) and interact with all important IoT stakeholders from public sector such as DG-CNECT, JRC, and from the private sector including CII providers, integrators and manufacturers.

The proper validation of the proposed baseline security requirements by the private and public sector would pave the way for a wide, de-facto, tacit adoption of it which could constitute the basis for EU harmonisation.

This work item builds on previous work of ENISA in the area of IoTs, intelligent Cars, Smart Cities, Smart Hospitals and Smart Airports (WP 2015 - 2016).

Type of Output

- P: Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, Q4
- E: 1 validation workshop with targeted stakeholders, Q2-Q4

Performance Indicator

- By 2017 engage 7 leading IoT developers, 7 leading CII operators and 5 EU MS in the study
- By 2019 the Commission and more than 7 EU MS use ENISA's baseline security requirements

3.1.1.4 Output O.1.1.4 – Baseline Security Recommendations for the eHealth Sector

This study will develop baseline cyber security recommendations for critical assets and services owned and operated by the eHealth sector.

The Agency will identify and analyse existing security practices and standards in the area of critical assets and services for eHealth and start developing requirements only if the analyses shows that no suitable practices/standards exists. In this case the Agency will compare them appropriately and develop baseline security measures to be adopted by all relevant stakeholders. The study will build on existing national provisions (e.g. protection profiles and technical guidelines as well as certification concepts).

The Agency will focus, among others, on Health Information systems, clinical data repositories, electronic Health Record components, patient Health Record services and ePrescription services.

In this endeavour the Agency will take into account existing EU policy and regulatory context (e.g. EU 2020 Strategy, the Digital Agenda for Europe, the eHealth Action Plan 2012-2020[6]).

The Agency will also validate the results of the study with relevant national authorities (e.g. Ministries of Health, relevant cyber security agencies and specialised bodies like Gematik in Germany) including data protection ones and EU initiatives and interact with all important IoT stakeholders from public sector such as DG-CNECT, DG Health and Food Safety, JRC, and from the private sector including eHealth service providers (e.g. hospitals), IT and Network solution providers, and eHealth system/service manufacturers.

[6] http://ec.europa.eu/health/eHealth/docs/com_2012_736_en.pdf

The proper validation of the proposed baseline security requirements by the private and public sector would pave the way for a wide, de-facto, tacit adoption of it which could constitute the basis for EU harmonisation.

This work item builds on previous work of ENISA in the area of eHealth and Smart Hospitals (WP 2015 - 2016).

Type of Output

- P : Baseline Security Recommendations for the eHealth Sector, Q4
- E : 1 validation workshop with targeted stakeholders, Q2-Q4

Performance Indicator

- By 2017 engage 5 leading eHealth Service Providers, 5 leading eHealth ICT providers and 5 EU MS in the study
- By 2019 more than 7 EU MS use ENISA's baseline security requirements

3.1.2 Objective 1.2. NIS Threats Landscape and Analysis

The Objective NIS Threat landscape and Analysis has two parts:

- The ENISA Threat Landscape focuses on a general analysis of the threat landscape
- The NIS annual analysis reports, covers the analysis carried out by the Agency on the reported data collected according to the legal requirements/mandate of the Agency.

NIS Threat Landscape

ENISA Threat Landscape (ETL) is one of the ENISA flagship endeavours. The resulting annual report enjoys major attention both within Member States, Commission, as well as expert and lay communities. This objective follows up on past achievements, to deliver an overview of the cyber-threat landscape, along with a series of related information. This material is free of technical details and is seeks to be very comprehensive.

In 2017, ETL will be further developed to include more interactive elements both in the presentation as well as the dissemination of related information. Hence, besides the availability of collected information over the entire year, produced threat information will be presented more intuitively by using more graphics.

The impact of ETL is varied: it is used as a consolidated summary of existing material in the area of cyber-threats; it provides strategic and tactical information that can be used within security management tasks; it can be imported to risk management methods; it can be used as basis for building up threat intelligence; and it can be used for training purposes; finally the ENISA collection and analysis process can be used by other organisations to create their own threat landscapes.

3.1.2.1 Output O.1.2.1 – Annual ENISA Threat Landscape

This report will provide an overview of current threats and their consequences for emerging technology areas. This report contains tactical and strategic information about cyber-threats. It also refers to threat agents and attack vectors used. The produced report is based on an intensive information collection exercise, including annual incident reports, followed by analysis and consolidation of publicly available information on cyber threats.

The ENISA ETL, provides information regarding reduction of threat exposure. This information will consist of available controls that are appropriate in order to reduce the exposure and consequently mitigate the resulting risks. In addition to the report, we will make available to the public all relevant material as this has been collected during the year.

Hence, besides informing security experts and decision makers, ETL will provide information on reduction of threat exposure. In doing so, synergies with related experts (i.e. ENISA ETL Stakeholder Group) and vendors will be implemented. We will invest in visualisation and quick availability of the resulting material.

Type of Output:

- P: Report and online information offering; report in Q4, information offering during the year.

Performance Indicator:

- Involvement of at least 5 representatives from different bodies/MS in the stakeholder group;
- By 2018, receive 100 references in media, including online ones, and 10K downloads of the ENISA report.

3.1.2.2 Output O.1.2.2 – Thematic Threat Landscape reports

This work will deliver 2 thematic landscape reports. Thematic landscapes are detailed threat assessments in a particular technology area. The aim of this work is to complement the generic ETL, to provide an assessment in one emerging area, usually an area identified under emerging technology areas in the ETL report.

Besides threat analysis, a thematic threat landscape provides information on related assets in that area, their threat exposure and controls/good practices for mitigation. In a similar manner as ETL, these reports are based on publicly available information. ENISA will provide two thematic landscape reports, that is, two emerging technology areas will be assessed

Type of Output:

- P: two thematic landscape reports, covering assessment of two emerging technology areas, Q4.

Performance Indicators:

- Involvement of at least 5 experts in the expert group of each thematic landscape;
- By 2018, receive at least 20 references in media, including online ones, and 4K downloads of the ENISA report

NIS Annual Analysis Reports

ENISA is mandated by the article 13a of the Telecom Framework Directive and article 19 of the eIDAS Regulation to collect reports from competent authorities in the area of telecom operators and trust service providers respectively. The Agency analyses the reports and produces useful insights.

Reports on annual incidents are useful tools for providing stakeholders with insights on security incidents that have had significant impact. Based on the analysis the Agency draws lessons learned, identifies security trends and good practices and assess root causes. Furthermore, the reports provide a consistent and factual aggregate analysis of incidents for policy makers, the public and the industry, describing overall frequency and impact of ICT security incidents across the EU.

3.1.2.3 Output O.1.2.3 – Annual Incident Analysis Report for the Telecom Sector (article 13 a)

This report provides an aggregated analysis of the major cyber security and network integrity incidents affected European electronic communications' sector in 2016.

According to article 13a of the Telecom Framework Directive ENISA shall collect from National Regulatory Authorities (NRAs) incidents of significant impact. The Agency has developed over the years, together with NRAs, the process to follow and the reporting modalities (e.g. parameters, thresholds, etc.).

The Agency analyses the reported incidents and then identifies trends, lessons learned and good practices. All these are part of an Annual Incident Analysis Report. The report is validated by the NRAs through a series of physical, community building workshops organised by ENISA.

Type of Output

- P: Annual Incident Analysis Report for the Telecom Sector, Q4
- E: 2 workshops with NRAs, Q1-Q4

Performance Indicator

- By 2017 more than 25 NRAs/EU MS participate in ENISA's workshops with NRAs

3.1.2.4 Output O.1.2.4 – Annual Incident Analysis Report for Trust Service Providers (article 19)

This report provides an aggregated analysis of the major cyber security incidents affected Trust Service Providers in 2016.

According to article 19 of the Electronic Identification and Trust Services (eIDAS) Regulation, once per year the National Supervisory Bodies (SBs) should notify ENISA about the security breaches or loss of integrity of the trusted services and on the personal data contained therein.

ENISA collects from SBs the annual reports about the reported incidents. The Agency analyses the reported incidents and then identifies trends, lessons learned and good practices for protecting trust service providers from such incidents. All these are part of Annual Incident Analysis Report which is validated by the NRAs through a series of physical, community building workshops organised by ENISA.

Type of Output

- P: Annual Incident Analysis Report for the Trust Service Providers, Q4
- E: 2 workshops with national SBs, Q2-Q4

Performance Indicator

- By 2017 more than 15 NRAs/EU MS participate in ENISA's workshops with Competent Authorities

3.1.3 Objective 1.3. Research & Development, Innovation

The actions presented in this Objective are structured in two dimensions. The first dimension covers the ICT standardisation in the EU and aims to assess the existing needs and gaps in the field. Second dimension has as goals to identify research priorities from NIS perspective and from the EU perspective and to use such priorities in collaboration with EU Commission in funding programmes.

3.1.3.1 Output O.1.3.1 – Guidelines for the European standardisation in the field of ICT security

This activity will provide the assessment of the situation of European standardisation in the area of ICT security. It will analyse the gaps and provide guidelines for, in particular, the development of standards, facilitation of the adoption of standards and governance of EU standardisation in the area of ICT security.

Type of output:

- P: Guidelines for the European standardisation in the field of ICT, Q4.

Performance indicator:

- Participation in drafting and review of at least 5 representatives of European Standard Developing Organizations (SDOs) and relevant services of the European Commission

3.1.3.2 Output O.1.3.2 – Priorities for EU Research & Development in the context of H2020

This study will provide an analysis of areas covered by the NIS Directive and General Data Protection Regulation where R&D activities funded in the context of H2020, CEF (Connecting Europe Facility), TRANSIT and GEANT would achieve the greatest impact. It will propose concrete areas with rationale for their choice. The role of PPPs on cybersecurity will also be assessed.

Type of Output:

- P: Study on priorities for EU research & development in the context of H2020, Q4.

Performance Indicator

- Involving at least 5 representatives from different stakeholders – research, industry, governmental.

3.1.4 Objective 1.4 Response to Article 14 Requests under Expertise Activity

Article 14 requests allow the MS and EU institutions to make direct requests to ENISA seeking assistance or advice on specific activities. Under this Objective, the Agency will address all the requests related to the area of Expertise.

3.1.4.1 Output O.1.4.1 Response to Requests under Expertise Activity

The type of outcome and the performance indicators will be defined during the execution year of the work programme together with the requester. Based on previous experience, from existing Outputs in the area of Expertise, O.1.2.3 and O.1.2.4 are subject of Article 14 requests.

Although, by definition, it is not possible to accurately estimate the exact number or the output and outcome of these requests for 2017, the allocated resources are indicated in the Summary Section at the end.

3.2 Activity 2 – Policy. Promote network and information security as an EU policy priority

In this activity ENISA supports the EU policy development and EU policy implementation in a number of important areas.

3.2.1 Objective 2.1. Supporting EU policy development.

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

In the policy development area the Agency will co-operate with public and private stakeholders to develop insights, consolidate views and provide recommendations in areas where the EU take action to further develop its policy. Examples include eHealth, Smart Grids, Certification, DSM, finance and transport.

3.2.1.1 Output O.2.1.1 – Contribute to EU policy in the area of eHealth

ENISA, using its knowledge and expertise in this area, will provide recommendations to the EU Commission and EU MS on how eHealth cyber security be better dealt with and will bring public and private sector to share lessons learned from past experiences.

In this context the Agency will liaise with the Commission and all relevant EU Member States to identify and analyse consistent eHealth cyber security approaches or strategies. Through discussion with the competent experts from public and private sector the Agency will identify the key elements of such a national approach and issue recommendations for developing such a scheme. ENISA will validate its findings via a workshop with all competent authorities.

Type of Output

- P: Recommendations on national eHealth NIS frameworks, Q4
- E: 1 workshops with stakeholders, Q2-Q4

Performance Indicator

- By 2017 more than 15 private eHealth providers and 10 EU MS take part in the activity

3.2.1.2 Output O.2.1.2 – Contribute to EU policy in the area of Smart Grids and ICS-SCADA

ENISA will liaise with the Commission, the Member States and the private sector in the implementation of the EU's Smart Grids strategy and ICS-SCADA actions.

The Agency, building on its existing knowledge and expertise, will support the Commission and Energy regulators on EU's Cyber Security Strategy for the Energy Sector. It will continue its co-operation with Smart Grids and ICS-SCADA asset owners on several topics such as ICS-SCADA certification, internet interdependencies and cyber security skills of the sector.

ENISA will engage with all relevant stakeholders, provide contributions to the Commission on policy initiatives (e.g. EECCS, DG ENER's EG 2 and EECSP, CEN/CENELEC's M490, EuroSCSiE) and make sure that these efforts properly align with EU's overall Smart Grid Policy.

Type of Output

- E: 2 workshops with stakeholders, Q2-Q4

Performance Indicator

- By 2017 more than 15 private smart grid and ICS-SCADA providers and 10 National Energy Regulators take part in this activity

3.2.1.3 Output O.2.1.3 – Support the policy discussions in the area of IT security certification

The Agency will continue to support the Commission and the Member States in identifying a certification framework for the ICT security products and services which on one hand will boost competition and on the other promote mutual recognition or harmonisation of certification practices up to a certain level. Any planned activity in the area of IT security certification will respect existing national efforts and interests.

ENISA will bring together standardisation organisations (ETSI, IEC, etc.), ICT certification stakeholders (test labs, certification and accreditation bodies, SOG-IS, CCRA, etc.) as well as ICT security product users (ESMIG, Eurosmart, etc.) as a means to enhance the dialogue around security certification and build upon existing results these initiatives have developed in the past.

Issues to be considered mapping the existing European situation in certification, possible steps to take at EU level, how to speed up the development of secure European ICT infrastructures and services and the policy impact of certification.

Type of Output

- E: 1 workshop with stakeholders, Q2-Q4

Performance Indicator

- By 2017 more than 10 private companies and 10 EU MS take part in the activity.

3.2.1.4 Output O.2.1.4 – Restricted. Towards a Digital Single Market for high quality NIS products and services

ENISA will continue supporting the Commission in the development of the Digital Single Market (DSM) in Europe from the NIS perspective.

The Agency, building upon its previous work on DSM (WP 2016) and on Commission's studies on the matter, will identify two market segments (e.g. cloud computing, network infrastructures) where the EU has significant NIS advantages vis-à-vis other continents and analyse the main reasons for it.

To achieve this the Agency will liaise with the Commission, EU MS, and relevant public and private sector organisations that will provide critical input and insights on the matter. The analysis will reveal lessons learned, success stories and good practices to be used for other sectors in the context of DSM.

The report will include strategic recommendations to the stakeholders and it is envisaged to be used for inspiration by other sectors. In this endeavour, ENISA will engage appropriate public and private stakeholders in the analysis and validation of the results.

ENISA will also contribute to the European Cloud Initiative of the Commission. In that respect the Agency will provide technical insights and good practices in the Free Flow Data Initiative and cloud certification actions foreseen under this initiative.

Type of Output

- P: Recommendations on DSM up take, Q4
- E: One workshops with stakeholders, Q2-Q4

Performance Indicator

- By 2017 more than 10 leading private companies from 2 sectors take part in the study

3.2.1.5 Output O.2.1.5 – Contribute to EU policy in the area of Finance

ENISA will continue its efforts in the area of NIS for the finance sector by collaborating with Commission (DG FISMA), EBA and ECB, national Financial Supervisory Authorities, FI-ISAC group and numerous private financial institutions.

More specifically the Agency will continue its co-operation with the Finance Supervisory Authorities on the proper deployment of cloud services by the finance sector. In that respect ENISA will co-operate with all relevant stakeholders on the take up of its existing report (WP 2016) on the secure deployment of cloud by the finance sector.

In addition the Agency will continue contributing to the Secure Pay Consortium. ENISA will focus its contribution to the incident reporting WG, the secure communication channels WG and the authentication WG. In that context ENISA will provide its expertise to Finance Competent Authorities on the most effective implementation of an incident reporting mechanism.

Furthermore ENISA will also continue its co-operation with EBA and ECB to develop good security practices for the proper implementation of the third party payments mechanisms envisaged in the Payment Service Directive II. In that context ENISA will also develop insights and evaluate existing good practices on other payments mechanisms including mobile payments.

Type of Output

- P: Good practices on mobile payments (position paper), Q4
- E: One workshops with stakeholders, Q2-Q4

Performance Indicator

- By 2017 engage 15 financial institutions and 10 NSAs in this activity

3.2.1.6 Output O.2.1.6 – Contribute to EU policy in the area of Smart Transportation

ENISA will continue its efforts in the area of smart cities and especially smart transport.

The Agency will liaise with the Commission and MS's competent authorities on the implementation of EU's Smart Transportation Strategy by addressing topics related to security, resilience and data protection.

In that context ENISA will co-operate with private sector on the take up of its good practices (WP 2015) in this area. More specifically the Agency will co-operate with cities and multi modal transport operators to promote good practices related to NIS governance and controls measures (e.g. risks assessment, incident reporting, etc.).

The Agency will contribute to relevant EU and national initiatives including standardisation ones.

Type of Output

- E: 2 workshops with stakeholders, Q2-Q4

Performance Indicator

- By 2017 more than 10 transport operators and 10 EU competent authorities take in the activity

3.2.2 Objective 2.2 Supporting EU policy implementation

Objective 2.2 covering policy implementation is structured on 4 main topics:

- Contribute to EU policy in the area of e Communications
- Support for the implementation of the eIDAS regulation.
- Support addressing the area of privacy and data protection linked to upcoming data protection regulation.
- Support the implementation guidelines for the Implementation of Mandatory Incident Reporting in the context of the NIS Directive

In the policy implementation area the Agency will co-operate with competent authorities and private stakeholders to implement existing policies of the EU. Emphasis is given on harmonisation and soft-law outcomes that would allow public and private sector to efficiently implement the EU policies. Examples include NIS Directive, Telecom Package, eIDAS, Privacy and Data Protection.

3.2.2.1 Output O.2.2.1 – Contribute to EU policy in the area of electronic communications sector

The Agency will continue its co-operation with the eCommunication sector developed over the years (WP 2010-2016).

The Agency will liaise with NRAs for the harmonised implementation of article 13a (incident reporting, baseline security requirements, root causes, trusted information sharing) in line with the DSM Strategy. It will also collaborate with BEREC and Commission on the new NIS provisions to be considered in the update of the new Telecom Package Directive as well as the Universal Services Directive. It will also consult with eCom providers and internet infrastructure providers on lessons learnt from incidents, sharing of experiences and good practices and on policy implementation matters.

ENISA will also liaise with the 5G PPP Working Group on Network Management and Security and will jointly organise a workshop to identify common areas of interest and further develop the area of 5G and SDN/NFV security matters. Cooperation will also be sought with the NFV Industry Specification of ETSI which is also active in network virtualisation security and it has recently established a relevant Working Group (NFV ISG Security Working Group).

Type of Output

- E: 2 workshops with eCommunication providers, Q2-Q4

Performance Indicator

- By 2017 engage 20 private eCommunication providers and 20 NRAs in the activity

3.2.2.2 Output O.2.2.2 – Develop guidelines for the implementation of mandatory incident reporting

ENISA, building on its experience on mandatory incident reporting schemes and the work done by the Cooperation Group and the CSIRT network being established by the NIS directive, will develop guidelines on implementing mandatory incident reporting mechanisms. This outcome can be also useful in the context of the NIS Directive.

This activity aims at helping EU Member States, relevant private sector and EU Commission to properly implement the incident reporting obligation defined in the NIS Directive. This work builds on ENISA's work

on the matters in the area of eCommunication providers (WP 2012-WP 2016), in the area of Trust Service Providers (WP 2015-WP2016) and in the area of NIS Directive (WP 2016).

ENISA will identify experts from all relevant public and private sectors and engage them in the process in order to develop and validate the appropriate guidelines. Using its experience and knowledge in incident reporting in different contexts ENISA will develop a simple and practical framework for reporting incidents in these sectors (e.g. who reports, what is reported, how it is reported, when it is reported, etc.).

The proposed approach will extensively be validated with numerous relevant stakeholders. ENISA will do its utmost to achieve consistency and harmonisation among the different implementation approaches across sectors. Emphasis will be given on applying similar approaches, concepts, frameworks, good practices, recommendations, parameters and/or thresholds per sector. By doing this ENISA will develop an easy, consistent and affordable implementation scheme to be deployed by different sectors. Such schemes would allow the proper analysis of reported incidents and pave the way for a consistent analysis across sectors.

Type of Output

- P: Guidelines for the Implementation of Mandatory Incident Reporting in the context of the NIS Directive, Q4
- E: 2 workshops with relevant stakeholders, Q2-Q4

Performance Indicator

- By 2017 more than 15 private stakeholders and more than 15 public stakeholders take part in the study

3.2.2.3 Output O.2.2.3 – Engaging eIDAS Competent Authorities and the private sector in the implementation of article 19

ENISA will continue liaising with national Supervisory Bodies (SBs) on the implementation of eIDAs article 19.2 (e.g. reporting framework, parameters and thresholds, reporting tool, baseline security measures, etc.).

In the context of the forum launched in 2015, he Agency will pursue collaboration with the Commission (eIDAS Task Force), national SBs and Trust Service Providers on lessons learned from incidents, sharing of experiences and good practices, and on policy implementation. Also ENISA will continue its co-operation with other relevant initiatives like FESA and ETSI. In 2017, the Forum will be organised twice in order to share practices about the operational implementation of the Regulation and contribute to the work carried out by the EU eIDAS Observatory.

Furthermore, ENISA will engage SBs and Trust Service Providers on a strategic discussion about the use of existing baseline security measures and the proper use of existing standards (e.g. ETSI work in the context of M/460) and will support stakeholders in the adoption of them.

Type of Output

- E: 2 workshops with relevant stakeholders, Q2-Q4

Performance Indicator

- By 2017 engage more than 12 national competent authorities in the activity

3.2.2.4 Output O.2.2.4 - Recommendations for technical implementations of the eIDAS Regulation (Q4, 2017)

ENISA will continue its work on supporting public and private bodies in implementing the eIDAS Regulation by addressing technological aspects and building blocks for trust services. The aspects to be covered will be agreed with the EC and MS through the eIDAS experts group. Based on 2016 report on appropriate technological protection measures to preserve privacy and trust, the implementation guidelines will address specific technological measures and approaches and will be validated through coordinating eIDAS technical subgroups.

Upon request by EU MS and/or the Commission and within a given context, ENISA will update previously published reports in this area of work depending on the progress of the state-of-the-art.

Type of Output:

- P, Recommendations to support the technical implementation of the eIDAS Regulation, Q4.

Performance Indicator:

- Involving at least 5 representatives from different bodies/MS.

3.2.2.5 Output O.2.2.5 - Recommendations for technical implementations of the General Data Protection Regulation

This study will provide best practises and specific recommendations for the technical implementation of aspects related to the protection of personal data in the context of the provisions of General Data Protection Regulation. It will provide a set of recommendations that will provide data controllers and data processors support on selecting and implementing applicable methodological procedures for implementing aspects such as consent, right to erasure, data portability, data breaches, accountability, anonymization vs pseudonymization, etc.

Upon request by EU MS and/or the Commission and within a given context, ENISA will perform studies relevant to the implementation of the GDPR at EU MS level.

Type of output:

- P: Recommendations for technical implementations of the general data protection regulation, Q4.

Performance indicator:

- Involving at least 5 representatives from different bodies/MS.

3.2.2.6 Output O.2.2.6 – Privacy enhancing technologies

This activity aims to continue the Agency's work in the field of privacy. More specifically, ENISA will continue on practical guidelines to implement privacy and data protection by design and default. While in 2014 the work focused on a definition of the terms, beyond the mere statement of properties towards a practical definition which comes with a guide to construct such systems, and in 2015 and 2016 the focus was in providing the methodology to access the maturity of the current available techniques. Together with the Agency's partners in 2017 the Agency will continue this work by a community building effort that aims to create and maintain a repository of best available techniques for Privacy Enhancing Technologies (PETs). The Agency will contribute to tools and techniques that allow to evaluate new techniques and keep lists of best available techniques up to date.

The Annual Privacy Forum (APF) will be used to gather the key communities and to disseminate the work in this area to the respective communities in industry and policy making.

Type of output:

- P: Q4 Updated report on privacy-by-design describing the community approach; this report should be accompanied with a prototype of a PETs maturity assessment tool.
- E: Q2, APF' 2017

Performance indicators:

- The results of the PbD report should be evaluated by the scientific community, part of the results should aim to be presented at relevant workshops; distinguished experts in the field shall be asked for their evaluation. Both should be used to jump start an online community.
- APF should have 100 participants from the relevant communities; its scientific track should have an acceptance rate well below 50%; proceedings should be published under a well-known label.
- Both parts of the activities should support the aims of O.2.2.5.

3.2.2.7 Output O.2.2.7 – Guidelines for data controllers on securing the automated processing of personal data

The outcome of this project will be guidelines for the security of personal data in different sectors and taking into account the overall risk involved in the processing, as well as the impact to the involved personal data. Special attention will be given to emerging technologies and trends in certain fields of online processing of personal data, e.g. in the context of the internet of things and big data. In the course of this exercise, training material for the security of personal data will also be developed for data controllers and processors.

Type of Output:

- P: Guidelines for data controllers on securing the automated processing of personal data, Q4.

Performance Indicator:

- Involving at least 5 representatives from different bodies/MS during the preparation and validation of the guidelines.

3.2.2.8 Output O.2.2.8 – Supporting the Implementation of the NIS Directive

ENISA will support the Commission, Member States and the private sector in the implementation of the NIS Directive. This output mainly covers reporting obligations for MS and implementation of cybersecurity strategies, while the cooperation aspects are covered in Output O.3.1.5 and O.4.2.3.

More specifically ENISA will assist the designated national competent authorities to develop an appropriate framework for reporting incidents of significant impact. The Agency will assist the stakeholders to define the scope of reported incidents, the parameters and thresholds used as well as the required procedure to follow. The Agency will leverage its expertise and knowledge in this area (article 13 a, article 19) to achieve its objectives.

ENISA will also contribute to the establishment of the Co-operation Network and provide suggestions on its functioning. The Agency, upon request, can analyse specific issues identified by the co-operation group and develop recommendations and suggestions that would allow Commission and Member States to take informed decision on NIS matters.

The Agency will leverage its expertise and good practices, among others, on Critical Information Infrastructures, National Cyber Security Strategies, baseline security requirements in numerous sectors (energy, transport, finance etc.), standardisation, ICT certification to contribute to the work of two groups. That would be by reusing and customising existing results or by developing new, specific results meeting the needs and requirements of the two groups.

Type of Output:

- E: Several workshops and contributions in the context of the Co-operation Group
- P: Recommendations related to the establishment of the Co-operation Group
- P: Numerous Contributions (technical and strategic) related to harmonised implementation of the NIS Directive

Performance Indicator:

- Involving at least 15 MS and 15 private stakeholders in the implementation of the NIS Directive

3.2.3 Objective 2.3. Response to Article 14 Requests under Policy Activity

Article 14 requests allow the MS and EU institutions to make direct requests to ENISA seeking assistance or advice on specific activities. Under this Objective, the Agency will address all the requests related to the area of policy development and policy implementation.

3.2.3.1 Output O.2.3.1. Response to Requests under Policy Activity

The type of outcome and the performance indicators will be defined during the execution year of the work programme together with the requester. Based on previous experience, from existing Outputs in the area of Policy, O.2.1.1 to O.2.1.6 and O.2.2.1 to O.2.2.5 are subject of Article 14 requests.

Although, by definition, it is not possible to accurately estimate the exact number or the output and outcome of these requests for 2017, the allocated resources are indicated in the Summary Section at the end.

3.3 Activity 3 – Capacity. Support Europe maintaining state-of-the-art network and information security capacities

ENISA will provide assistance to MSs and EU institutions and bodies, as well as the private sector by supporting enhancement of NIS capacity building through the EU. ENISA will work together with Member States and EU institutions to assist them in capacity building across the EU. For instance, ENISA will continue promoting capacity building activities also in support of the rolling-out and uptake of electronic identification and trust services under the eIDAS Regulation. In particular, the Agency will work together with all relevant stakeholders to ensure that the approach is coherent across the EU.

3.3.1 Objective 3.1. Assist Member States' capacity building.

One of the main goals of this objective is to develop and improve activities related to the operational security capacity-support program. In 2017, ENISA will build upon its work in operational security area, and will update and continue providing technical training material for CSIRTs to concisely support improvement of technical skills across Europe and support MS through a dialogue with relevant stakeholders in order to adjust our focus to technical challenges for the coming years. Another main goal of this objective 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.

3.3.1.1 Output O.3.1.1 – Status report on Cyber security skills

This work will take into account existing research and initiatives of the EC and ENISA and build upon to create a baseline matching features matrix with the job market requirements. Another objective is to consolidate the NIS education map piloted in 2014 and enhanced during the following years. It can be consulted here https://cybersecuritymonth.eu/references/universities .

Type of output:

- A report and a consolidated NIS education map with courses , P, Q4

Performance indicator:

- Involving at least 14 representatives from different bodies/MS.

3.3.1.2 Output O.3.1.2 – Support national and governmental CSIRTs capabilities

In 2017 ENISA will provide a continuous monitoring and update on CSIRT capabilities' maturity and progress in Europe. The agency will support the development of Member States' national incident response capabilities by providing recommendations on key dimensions of NIS capacity building with a focus on the development and efficient functioning of national and governmental CSIRTs. ENISA will as well offer, upon their request, direct support to single Member States to assess and improve their CSIRT capabilities.

The main objectives of this output in 2017 is to help MS and another ENISA stakeholders, such as the EU institutions, bodies and agencies, to develop and extend their incident response capabilities and services in order to meet the ever growing challenges to secure their networks. Another objective of this output is to further develop and apply ENISA recommendations for national and governmental CSIRT Baseline Capabilities. As a continuous effort ENISA will maintain and regularly update its online European CSIRT Inventory.

Type of output:

- P: Q4: Update on CSIRT Baseline capabilities report
- P: Q2 and Q4: CSIRT online Inventory update – European interactive map of CSIRTs
- E: Q2: Annual ENISA technical CSIRT workshop for national and governmental CSIRTs ' (12th workshop 'CSIRTs in Europe')
- P: Q4: Good practice guide on how to improve CSIRT capabilities (work in progress from 2015, 2016)

Performance Indicator:

- Support provided at least for two MSs to enhance their 'national and governmental CSIRT baseline capabilities'
- Support provided at least for two EU institutions, bodies or agencies in development or enhancement of their incident response capabilities
- Twice a year (Q2, Q4) updated overview of existing CSIRTs and their constituencies in Europe for different type of stakeholders (e.g. business sector)
- Minimum of fifteen MSs participating in the technical CSIRT workshop.

3.3.1.3 Output O.3.1.3 – Update and provide technical trainings for MS and EU bodies

In 2017 most of activities in this area target at maintaining and extending the collection of good practice guidelines and trainings for CSIRT and other operational personnel. The Agency will support the development of Member States' national incident response preparedness by providing good practice guidance on key elements of NIS capacity building with a focus on CSIRT trainings and services in order to improve skills of CSIRT teams and their personnel. ENISA will further build upon successful work in the area of 'training methodologies and impact assessment'.

In detail, the Agency will provide an update of training material in high demand and provide new set of a training material based on emerging technologies in order to reinforce MS CSIRTs skills and capacities to efficiently manage cyber security events. A special emphasis in this output is laid on supporting MS CISRTs and EU bodies by a concrete advice (like good practice material) and concrete action (like CSIRT training). ENISA will as well offer, upon their request, direct support to single Member States to provide technical trainings and advisories.

Type of output:

- P: Q4: New set of technical training material on incident handling for emerging technologies like IoT and time critical systems (e.g. hospitals, national PKI)
- P: Q4: Update of existing operational training material (details on operational category can be found on ENISA training website)
- P: Q4: Good practice guide on CSIRT services (exact topic will be chosen in Q4/2016 to capture the emerging and up-to-date challenges in this area)

Performance indicator:

- Continued CSIRT services training will be provided to a minimum of 20 participants of different organisations in 5 MS (new training material).
- Improved operational practices of CSIRTs in at least 15 MS (ongoing support with best practices development and updated training material).

3.3.1.4 Output O.3.1.4 – Support EU MS in the development and assessment of NCSS

ENISA will continue assisting EU MS to develop their capabilities in the area of National Cyber Security Strategies (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 of 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 private sector with varying degrees of experience to discuss and exchange good practices, share lessons learnt and identify challenges and possible solutions. Through this interaction with MS ENISA will validate and update its existing NCSS good practice guide and evaluation/assessment framework of NCSS.

Finally ENISA will continue updating ENISA's EU map of NCSS as well as with enhancing this map with information in other ENISA's reports with relevant scope such as CIIP governance and ICS-SCADA security maturity models.

Type of Output

- P: Updated - EU's map on NCSS
- E: 2 workshops with EU MS on NCSS development, Q2-Q4

Performance Indicator

- By 2017 engage 15 EU MS in this activity

3.3.1.5 Output O.3.1.5 – EU CSIRT network secretariat

ENISA will support the Commission and Member States in the implementation of the NIS Directive.

More specifically ENISA will provide the secretariat of the CSIRT network and actively support the co-operation among them.

Type of Output

- S: Rules of procedures of the CSIRT network (art 8b (5))
- S: Q1-Q4: Provide EU CSIRT network secretariat (e.g. logistics, organisation of the meeting, agenda management, meeting minutes)
- S: Facilitate CSIRTs regular participation in the EU CSIRT network events
- E: Several workshops and contributions in the context of the CSIRT network

Performance Indicator

- Involving all 28 MS designated CSIRTs in the implementation of the NIS Directive

3.3.2 Objective 3.2. Support EU institutions' capacity building.

ENISA will advise on key orientations and, upon request, on actions to be implemented in order to achieve a high level of NIS across all European Union. ENISA will, as well, produce information notes on threats, risks and incidents with a view of making European's networks more secured.

3.3.2.1 Output O.3.2.1 – Restricted and public Info notes on NIS

In case of NIS issues and occurrences that reach a certain level of public and media attention it is crucial, that the Agency continue to provide a more balanced set of information about the issues and occurrences.

ENISA's intention is to continue providing Info Notes as a reliable and continuous service to its stakeholders in a timely manner. The overall goal for each Info Note is to highlight fundamental facts and shortcomings behind specific NIS.

In 2017 ENISA will continue providing timely information in the form of Info Notes to key stakeholders on NIS incidents and significant developments in the cyber security field. ENISA will further assess the distribution methodology in relation to emerging technologies and assess the impact of Info Notes among key stakeholders as well as the delivery platform development.

Type of output:

- P: Q1-Q4: Restricted Info Notes on NIS for key stakeholders
- P: Q1-Q4: Public Info Notes on NIS
- P: Q4 Development of Info Notes delivery process

Performance indicator:

- in 2017 at least 1 additional key stakeholder group (e.g. ENISA MB members or PSG) receives restricted Info Notes on regular basis
- In 2018 Public Info Notes are published on weekly basis on ENISA website.

3.3.2.2 Output O.3.2.2 – Restricted. Upon request, support the assessment of existing policies/procedures/practices on NIS within EU institutions

At the request and/or in agreement with the Commission ENISA will assess the impact of specific policies, procedures and practices on NIS within EU institutions and compare those against national and/or other international experiences. ENISA will then engage the key players in a dialog to discuss its findings and propose recommendations and good practices in a form of a small position paper.

Type of Output

- P: Position Paper on a given topic, Q4
- E: 2 workshops with relevant stakeholders, Q2-Q4

Performance Indicator

- By 2017 at least 3 EU institutions and 5 MS take part in the activity

3.3.2.3 [Output O.3.2.3 - Study on the applications of encryption and other technologies as enabler of the European Digital Single market]

[The Agency will investigate the use of encryption and other privacy enhancing technologies as means to establish online trust in the Digital Single Market.

Upon request by EU MS and/or the Commission and within a given context, ENISA will perform analysis for specific business areas (e.g. eID).

Type of Output

- P: Report, Q4

Performance Indicator

- By 2017 at least 3 EU MS take part and contribute to this activity]

3.3.3 Objective 3.3. Assist private sector capacity building.

The private sector is a highly relevant sector where the Agency supports capacity building. During 2017 the aim is to extend the work on cybersecurity culture, cyber hygiene and to start an action related to liability and insurance.

3.3.3.1 Output O.3.3.1 – Cybersecurity culture: from identifying the issues to providing working scenarios for management level

The management level is an essential environment for most decisions with impact in NIS- Network and Information Security. The understanding of the issues at stake by senior managers impact the mitigation actions to be approved, or allocations of budgets, or development of new business sectors etc. With this output we propose to give practical advice in terms of identifying the most common issues to what the real life scenario may look like for the management level.

Type of Output:

- P: Study on cybersecurity culture, Q4

Performance indicator:

- Involving at least 5 representatives from different bodies/MS.

3.3.3.2 Output O.3.3.2 – Handbooks on cyber-hygiene when processing customer data for different scale companies

This study will build on 2016 work on security measures and existing best practises to protect customer data and to transform them into practical handbooks. Through the compilation of concise reference guidebooks, different size companies from diverse sectors (e.g. in retail, health, e-commerce, etc.) will be provided with tailored practical techniques and tools on how to be proactive and adopt well acknowledged information security and data protection best practises.

Type of Output:

- P: Handbook on cyber-hygiene, Q4.

Performance indicator:

- Involving at least 5 representatives from different bodies/MS.

3.3.3.3 Output O.3.3.3 – Good Practices and Recommendations on Cyber Insurance

Cyber insurance might prove a good incentive for businesses to invest in information security. To investigate its potential, ENISA will take stock of existing approaches to cyber insurance at national, EU and non EU states (e.g. US, Asia, etc.) level and then survey private and public sector as well as insurance companies on the lessons learned and the good practices in use from the deployment of cyber insurances (e.g. liability issues, proper policy calculation, asset cost, cost of breaches). In this task the deliverables produced by other, well appreciated institutions (e.g OECD, European FI-ISAC) should be taken into account.

ENISA will analyse the findings, identify good practices and issue recommendations for targeted stakeholders. In this context, the Agency will create and maintain a small expert group that would provide guideline and validate the results of the study together with other relevant stakeholders from the public and private sector.

This work will build upon ENISA's previous work on cyber insurance (WP 2012).

Type of Output

- P: Good Practices and Recommendations on Cyber Insurances , Q4
- E: 1 workshop with relevant stakeholders, Q2-Q4

Performance Indicator

- By 2017 at least 7 insurance companies and 10 companies take part in the activity.

3.3.3.4 Output O.3.3.4 – Security Recommendations for digital Service Providers and Users of Trust Services

The objective of this item is to develop a set of recommendations for the trust service providers and their customers. The choice of specific areas to be covered will be agreed with the relevant stakeholders, such as the TSPs, conformity assessment bodies and supervisory authorities. These recommendations will complement the existing knowledge base that ENISA created for the trust service providers.

Type of Output:

- P: Security recommendations for digital service providers and users of trust services, Q4.

Performance Indicator

- Review and acceptance by at least 10 stakeholders (trust service providers, conformity assessment bodies, and supervisory authorities).

3.3.4 Objective 3.4. Assist in improving general awareness

In close collaboration with Member States, ENISA will help EU citizens to gain essential cyber security knowledge and skills to help protect their digital lives. This will include promoting an annual European Cyber Security month and working with the Member States delivering projects like the Cyber Security Challenges as well as national initiatives, upon request from Member States.

3.3.4.1 Output O.3.4.1 – Cyber Security Challenges

In order to promote capacity building and awareness in NIS among emerging young generation of cyber security experts in EU MS, in 2017 ENISA will continue to promote and advise EU MS on running national 'Cyber Security Challenge' competitions. The agency will also continue its European Cyber Security Challenge 2017 annual activity. Its support to the national and European activities will aim at university students from technical schools and young talents and also at security practitioners from the industry. The goal will be to increase the interest and future opportunities in NIS for these communities by promoting excellence in the form of competitions, as well as to gather feedback on the areas of interest from these stakeholders. In order to do so, ENISA will try to achieve large participation among individuals from EU MS for the final European competition.

Type of output:

- S: Q1-Q4: European Cyber Security Challenge 2017
- S: Q2-Q3: 'Award workshop' for winners of the European Cyber Security Challenge 2016 (ENISA promotes best of the best)
- S: Q4: European Cyber Security Challenge 2018 planning support

Performance indicator:

- At least two additional EU MS organise its national cyber security challenge in 2018
- In 2018 at least two additional EU MS participate in the European Cyber Security Challenge
- Promote collaboration between academia and industry in order to improve future opportunities in NIS for young talents.

3.3.4.2 Output O.3.4.2 – European Cyber Security Month deployment

The metrics built into the ECSM- European Cyber Security Month have shown an increased number of participants, and a better engagement level from year to year. This is an achievement that was possible with the support of an active community. In 2017 we intend to explore ways of making more use of sector briefs for cybersecurity professionals. The previously proposed pillars remain: support a multi-stakeholder governance approach; encourage common public-private activities; assess the impact of activities, optimising and adapting to new challenges as appropriate.

Type of Output:

- P: Q4, An evaluation report, Specialised material: October's 5 weeks with 5 sector briefs at EU level e.g. finance, education, health, IoT, telecommunications;

- P: Q4, A survey on national campaigns impact and metrics; This survey will complement ECSM, it will be used as a basis to improve it in order to outreach to more EU citizens and will focus on methodology impact assessment;

Performance indicator:

- Involving all 28 EU MSs, other partners and representatives from different bodies/MS.

3.3.4.3 Output O.3.4.3 –Online privacy portal

ENISA will provide guidance on the use of privacy enhancing tools for online privacy (e.g. anti-tracking and application encryption tools), targeting different players in the field (end users, data controllers, developers of PETs, Data Protection Authorities) and aiming at bringing more certainty and trust in the field.

Type of Output:

- P: Guidelines on the use of privacy enhancing tools for online privacy, Q4.

Performance Indicator:

- Involving at least 5 representatives from different bodies/MS.

3.3.5 Objective 3.5. Response to Article 14 Requests under Capacity Activity

Article 14 requests allow the MS and EU institutions to make direct requests to ENISA seeking assistance or advice on specific activities. Under this Objective, the Agency will address all the requests related to the area of capacity building.

3.3.5.1 Output O.3.5.1. Response to Requests under Capacity Activity

The type of outcome and the performance indicators will be defined during the execution year of the work programme together with the requester. Based on previous experience, from existing Outputs in the area of capacity, O.3.1.2, O.3.1.3, O.3.1.4 and O.3.2.2, O.3.2.3 and O.3.4.1 are subject of Article 14 requests.

Although, by definition, it is not possible to accurately estimate the exact number or the output and outcome of these requests for 2017, the allocated resources are indicated in the Summary Section at the end.

3.4 Activity 4 – Community. Foster the emerging European network and information security community

In order to achieve this scope, ENISA will enhance cooperation at EU level among Member States, Union institutions and related NIS stakeholders, including private sector and will focus on two main objectives: Cyber Crisis cooperation and CSIRT and other NIS community building.

3.4.1 Objective 4.1. Cyber crisis cooperation

ENISA will continue to support the operational communities and CSIRTs in their cyber crisis cooperation development activities. The organisation and evaluation of pan European cyber exercises will continue to have a central role in this support. In addition ENISA will monitor closely the implementation of action points from previous exercises. In this context the Cyber Exercise Platform (CEP) will be maintained and enhanced with more content to help the exercising of operational security communities. CEP will be

offered by the Agency upon request to interested stakeholders as a cyber exercise cloud service. The training portfolio of the Agency in cyber crisis management will be expanded and made available online in CEP.

Furthermore, ENISA will continue to support the development of standard cooperation procedures for the EU-level operational security networks and take on any responsibilities assigned to it in relation to the core service platform (CSP) developed in the context of the Connecting Europe Facilities (CEF) programme.

3.4.1.1 Output O.4.1.1 – Evaluation of Cyber Europe 2016

In 2016 ENISA organised the fourth pan European cyber crisis exercise, Cyber Europe 2016 (CE2016)..

In early 2017, ENISA will perform an in depth analysis of the evaluation data gathered from the exercise. This will result in a detailed After Action Report (AAR) that will be shared only with the participating countries. The report will include a dedicated section for any explicit comments received from the participating countries in order to increase transparency. ENISA will also prepare a public version of the report according to the public affairs strategy of the exercise

Type of output:

- P: Evaluation report for CE2016 (public and restricted versions), Q3

Performance Indicator

- At least 80% of the countries actively involved in the exercise contribute to the evaluation and quality assurance processes of the report

3.4.1.2 Output O.4.1.2 – Report on Exercise after Action Activities from 2014-16

The pan European exercises organised by ENISA are producing a number of very important recommendations and actions for all involved stakeholders. It is extremely important to ensure the follow up and monitor the progress of all these actions. Otherwise the value of the exercise lessons learned is deteriorated.

In 2017, and the follow on years, ENISA would like to analyse thoroughly and monitoring the implementation of actions from previous exercises. This activity will result in a report on the status of after action activities from previous exercises.

Type of output:

- P: Report on after action activities (restricted), Q4

Performance Indicator:

- At least 80% of the countries actively involved in exercises agree with the conclusions of the report

3.4.1.3 Output O.4.1.3 – Planning of Cyber Europe 2018

In 2018, ENISA will organise the fifth pan-European cyber exercise, Cyber Europe 2018 (CE2018). This exercise will closely follow up and build upon the lessons learned and actions from previous exercises, such as CE2014 and CE2016.

CE2018 will be a program of trainings and exercises 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-time 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 built-up will be realistic and focused in order to capture better how incidents are managed and cooperation happens in real-life. The exercise will include explicit scenarios for the CSIRT Network set up under the NIS Directive.

The high-level exercise program brief will include the strategic dimensions of the exercise will be prepared based on the lessons learned from CE2016, to drive the whole planning process. The exercise brief will be given for comments and approval to the MS Cooperation Group set up under the NIS Directive.. Following this ENISA will assemble group of planners from the participating countries to work closely towards developing a detailed exercise plan (ExPlan) by the end of 2017. ENISA will involve the group of planners in all relevant planning steps and take into account their input towards a consented plan. The exercise planning will set in early enough to avoid overlaps with other major related activities.

ENISA will consult MS and seek agreement of the Cooperation Group set up under the NIS Directive on a possible joint EU-NATO cyber exercise within the framework of Cyber Europe.

Type of output:

- P: Exercise plan (restricted), Q4.

Performance Indicator:

- At least 24 EU/ EFTA Member States and countries confirm their support for Cyber Europe 2018.

3.4.1.4 Output O.4.1.4 – Trainings on Cyber Exercise Planning and Cyber Crisis Management

In 2017, ENISA will further enhance its methodology, seminars and trainings on: a) cyber crisis management and b) the organisation and management of exercises. This activity will include the development of material and infrastructure for onsite and online trainings on these subjects. In addition this activity will cover the delivery of these trainings upon request.

Type of output:

- S: Trainings on CEP and CCM, Q4.

Performance Indicator:

- At least 70% of participants in trainings (online or onsite) evaluate the experience positive or very positive

3.4.1.5 Output O.4.1.5 – Cyber Exercise Platform (CEP) Development and Content Management

Since 2014 ENISA started the development of the Cyber Exercise Platform (CEP). CEP hosts number of services that ENISA offers to the Member States and EU Institutions, such as: exercise organisation and management, exercise playground with technical incidents, map of exercises and hosting the exercise development community. With this activity ENISA would like to maintain and enhance the experience offered by CEP, including user support.

In addition, new content and exercise incident challenges and material will be developed in order to keep up the interest of the stakeholders and make CEP a central tool in cyber security exercising for all stakeholders.

Type of output:

- S: Support for CEP, Q4.

Performance Indicator:

- At least 70% of CEP users evaluate it positively

3.4.1.6 Output O.4.1.6 – Design of Cyber Security Games in CEP

The CEP platform opens new opportunities for ENISA to enlarge the user base and thus offer to the operational cyber security communities opportunities to exercise and gain experience and knowledge. One way to enlarge the user base, and thus increase the impact of ENISA, is to offer new and interesting functionalities that will attract new registrations to CEP. One such project is to reuse the exercise material and virtual infrastructures of CEP to design cyber security games. The first step in this process is the design of the concept of cyber security games (re)using CEP. Following this, ENISA will organise a small pilot with a selected group of stakeholders to test and improve the concept.

Type of output:

- E: Design of conduct of cybersecurity games in CEP, Q4.

Performance Indicator:

- At least 70% of the pilot phase participants score the concept positively

3.4.1.7 Output O.4.1.7 – Cyber Exercises Support to MS and EU Institutions

CEP offers a flexible way of organising simultaneously multiple exercises in an isolated way. In addition, CEP offers the opportunity to reuse exercise material and infrastructures. This functionality can be offered by ENISA to EU Member States and Institutions as a cloud exercise service (CloudEx). ENISA would be able to set up an initial exercise space for anyone interested and pass over the management of this space fully.

Based on this functionality as well as on the expertise ENISA has on organising exercises, this activity will support the organisation of cyber security exercises for MS and EU Institutions upon request. In addition to offering CEP, ENISA will be able to offer support cyber incident scenario development as well as trainings and seminars on exercise organisation.

Type of output:

- S: Cyber Exercises support, Q4.

Performance Indicator:

- at least 80% of requests received by ENISA evaluate the service positively

3.4.1.8 Output O.4.1.8 – EU-level Cyber Crisis and Incident Management Procedures and Infrastructures

Since 2015, ENISA offers the secretariat to the MS developing EU-level standard cooperation procedures at operational and technical levels. The upcoming policy framework, NIS Directive, is expected to strengthen this by making this supporting role more formal as the secretariat for the cooperation of the EU operational cyber security network (CSIRTs). In this context, ENISA will offer support for the network, helping further the development of EU-level cooperation with standard operation procedures at both levels, including the point of contact management.

In this context also alert exercises and communication checks will be organised based on the defined procedures.

Type of output:

- S: support for the Cyber SOPs editorial team of the cooperation of cyber security network of CSIRTs, Q4.

Performance Indicator:

- At least 90% of the participating MS agree to the developed operational procedures.

3.4.1.9 Output 0.4.1.9 – Support the Connecting Europe Facility (CEF) Cybersecurity Digital Service Infrastructure (DSI)

In 2017 ENISA will have to prepare to manage and operate the centralised components of the Common Service Platform (CSP) of the Cybersecurity DSI to be implemented during 2016-2019 under CEF WP2015, subject to the agreement of the Government Board of the Cybersecurity DSI. As of 2017 ENISA will have to follow the CSP development very closely and build the capability to gradually take over the parts of the infrastructure as implemented. By 2019 ENISA must be ready to fully assume the responsibility for the management, maintenance and further development of the CSP.

As a result of this, the Agency will engage with the contractor developing and deploying the CSP in order to coordinate all activities that are in relation with the above tasks. ENISA will also investigate how we can extend our already excellent collaboration with GEANT.

The exact deliverables will include:

- 1) P: Q2: Roadmap for the implementation at the Agency's premises of management and operations of the centralised components of the Common Service Platform (report, Q2, 2017).
- 2) P: Q3: Detailed implementation plan of the management and operations of the centralised components of the Common Service Platform by the Agency (report, Q3, 2017).
- 3) S: Q4: Successful deployment of the management and operations of the centralised components of the Common Service Platform at the Agency (Operation of the CSP, report on the deployment, Q3 and Q4, 2017).
- 4) S: Q4: Cooperation with the CSP contractor(s) and contribution to the activities of the Cybersecurity DSI Governance Board (service, Q4, 2017).

Performance indicators:

- All personnel that will be involved in the operation, management, maintenance and enhancement of CSP is recruited and trained on time to assume their tasks
- The parts of the infrastructure which are delivered by the contractor are all successfully deployed at ENISA before the end of 2017
- Over 80% of the countries in the Governance Board approve the implementation and deployment plan

3.4.2 Objective 4.2. CSIRT and other NIS community building.

ENISA will continue to support the cooperation among CSIRTs, within an EU Member States CSIRTs network. As part of this activity, ENISA will provide the secretariat of the network of CSIRTs foreseen by the proposed NIS Directive and actively support its functioning by suggesting ways to improve cooperation

among CSIRTs and supporting this cooperation, including by developing and providing guidance on best practices and trainings in the area of operational community efforts, such as on information exchange.

Furthermore, the Agency will contribute to the dialogue among NIS related communities, including between CSIRTs and law enforcement and data privacy communities, in order to support consistent EU-wide approach to NIS.

3.4.2.1 Output O.4.2.1 Technical training community support for MS and EU bodies

ENISA will continue through its train the trainer program to collaborate with other EU institutions, bodies, agencies and international organisations (e.g. EUROPOL, CERT-EU, EUROJUST, FIRST, GEANT, CCDCOE) to perform a sustainable dialog, development and improvement of CSIRT good practices and training material for stakeholders from different industry areas. Specifically, in 2017 ENISA will provide an overview on SOC tasks and outputs for the implementation (technical) level. It will also provide comparison on different implementation methods and its and pros and cons. ENISA will continue to support a successful TRANSITS training program for CSIRT start up to enlarge the training community in Europe.

Furthermore, ENISA will continue to improve its training methodology for technical CSIRT trainings with a focus on cutting edge training methods and environment to enhance training community performance, scope and impact for the EU MS and CSIRT community as a whole.

Type of output:

- E: Q3, Annual Train the Trainer Workshop (TTT)
- S: Q1-Q4, Trainer Engagement Support Program (TESP)
- P: Q4, Study on Design and methodology for online training support (e.g. Webinars)
- S: Q1, Q3, Q4, TRANSITS training program support
-

Performance indicator:

- Support provided at least for two TRANSITS I trainings and one TRANSITS II training.
- Extend training program capacity and community in Europe for different types of stakeholders in the area of incident management by introducing two new external trainers and collaborate with at least two organisations or institutions on training material update or good practice development.

3.4.2.2 Output O.4.2.2 – Support the fight against cybercrime and collaboration between CSIRTs and LEA

In 2017, the key goal is to build upon the progress ENISA has made in supporting different operational communities (e.g. CSIRT, law enforcement, European FI-ISAC) to enhance mutually satisfactory ways to collaborate and support good practices among different stakeholders in operational communities in Europe. In detail, ENISA will continue its effort to support our common EU wide objective on fight against cybercrime with different stakeholders.

Type of output:

- P: Q4, Further improvement of communication between CSIRTs and LEA (based on 2011 report 'Flair for Sharing')
- P: Q4, Provide guidelines on emerging trends, tools and methodologies to support LEA and CSIRT co-operations

- E: Q3, continue annual ENISA/EC3 workshop for national and governmental CSIRTs and their LEA counterparts
- S: Q1-Q4, continue activities and involvement in CSIRT and other operational communities structures (e.g. FIRST, TF-CSIRT)

Performance indicator:

- At least 15 MS participate at ENISA/EC3 annual workshop
- Work of ENISA successfully reflected by existing communities when appropriate (European FI-ISAC, TF-CSIRT, etc.)

3.4.2.3 Output O.4.2.3 – Support EU CSIRT network community building

ENISA will support the cooperation among CSIRTs, within an EU Member States CSIRTs network. As part of this activity, ENISA will provide the secretariat of the network of CSIRTs and actively support its functioning by suggesting ways to improve cooperation among CSIRTs and supporting this cooperation, including by developing and providing guidance and good practices in the area of operational community efforts, such as on information exchange. In addition, ENISA will take an active role to support EU CSIRT network in activities relevant to the CEF work programme. ENISA will also manage EU CSIRT network infrastructure assigned to ENISA (if applicable - CEF annual work program to support CSIRTs in the area of community building and information sharing (Connecting Europe Facilities (CEF) program for CSIRTs).

Type of output:

- P: Q1-Q4, EU CSIRT network support (NIS Directive in place)
- P: Q1-Q4, Expanding ENISA CSIRT Inventory service for EU national and governmental CSIRTs - new functionalities such as CSIRT services, operations mode and capabilities (NIS Directive art 8b (3) a) (build upon ENISA online CSIRT Inventory tool)

Performance indicator:

Work of ENISA successfully reflected by existing CSIRT communities when appropriate (FIRST, TF-CSIRT, EU CSIRT network). In 2018 improved cooperation and information sharing among CSIRTs in Europe

3.4.3 Objective 4.3 Response to Article 14 Requests under Community Activity

Article 14 requests allow the MS and EU institutions to make direct requests to ENISA seeking assistance or advice on specific activities. Under this Objective, the Agency will address all the requests related to the area of Community building, exercises and CSIRTs cooperation.

3.4.3.1 Output O.4.3.1 Response to Requests under Community Building Activity

The type of outcome and the performance indicators will be defined during the execution year of the work programme together with the requester. Based on previous experience, from existing Outputs in the area of community building, O.4.1.4 O.4.1.7 and O.4.2.2 are subject of Article 14 requests.

Although, by definition, it is not possible to accurately estimate the exact number or the output and outcome of these requests for 2017, the allocated resources are indicated in the Summary Section at the end.

3.5 Activity 5 – Enabling. Reinforce ENISA's impact

Activity 5 covers three main objectives:

- Management
- Engagement with stakeholders
- International activities

3.5.1 Objective 5.1. Management

Under this activity several tasks are carried out and they are coordinated by the Executive Director.

Executive Director's Office

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

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

Management Board, Executive Board and PSG Secretariat

In 2017, ENISA will continue to support its formal bodies, the Management Board (MB) and the Permanent Stakeholders Group (PSG) as well as Executive Board in their functions by providing secretariat functions.

For the MB, one ordinary meeting will be organised during 2017 and informal meetings will be held as necessary. The existing electronic newsletter will be continued throughout 2017, as will support for the MB Portal. For the PSG also, two formal meetings will be organised.

For the Executive Board, a formal meeting will be organised once per quarter.

ENISA will continue to explore additional ways of supporting the Agency's statutory bodies in the most effective way, including the possible use of technology means.

The Management Board, Executive Board & PSG Secretariat reports to the Executive Director.

3.5.2 Objective 5.2. Engagement with stakeholders

Under this objective are grouped some of the tasks and activities of the agencies carried out in collaboration with stakeholders:

- National Liaison Officer Network coordination
- EU relations coordination
- Spokesperson, Stakeholders Communication and Dissemination Activities
- Core activities quality control and project office

National Liaison Officer Network

ENISA has kicked off various activities aiming at strengthening the cooperation with its National Liaison Officers' (NLO) Network. NLOs are key actors for the Agency's daily work and they warrant the interaction

with select public sector entities in the MS while they provide assurance in terms of outreach effective liaison with the MS and dissemination of ENISA deliverables.

In 2017, ENISA will build upon these efforts and improve its cooperation with the NLO Network, as the First Point of Contact for ENISA in the MS, with emphasis on:

- An NLO meeting to discuss possible improvements in the collaboration with ENISA. Improvements aim at leveraging on the NLO network for the dissemination of ENISA deliverables.
- Information to 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 where the Agency contributes to (for example co-organiser, etc.).
- The Agency maintaining and sharing with the NLO network information on all relevant ENISA projects and activities (e.g. unit responsible for the project, relevant tender results, etc.) while maintaining and expanding as appropriate online resources available.

EU Relations

As in previous years, the Agency will carry out the bulk of its EU relations work with statutory stakeholders including the Commission, EU Parliament, Council (working groups) and MS, by relying on its senior management (Executive Director (ED) and Heads of Department (HOD)) to develop relations. This approach will take due account of the management structure of the Agency so that the level of participation in any particular meeting remains at an appropriate level. A similar approach is taken for speaking engagements.

In 2017 the focus of these activities will be to continue to develop contacts within the EU institutions and with industry to prepare the renewed mandate for the Agency in the post 2020 period. It follows that contacts at the highest policy and possibly at the political level will be managed by the ED with the HoD of as backups depending on the subject to be discussed.

Spokesperson, Stakeholders Communication and Dissemination Activities

In 2017, ENISA will seek to improve its focus on key activities and to provide regular information to the press and media regarding these activities.

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

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

Operational Quality Control and Project Office

The operational quality control (OQ) function of the Agency aims at responding to a mix of regulatory, compliance and stakeholder requirements addressed to operations in an effort to improve organisational performance and compliance. Clearly the expertise built in this area can be leveraged upon by other services of the Agency. 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 OQ 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 that has been duly documented in a dedicated SOP and applied accordingly. OQ

addresses such areas as performance management including key performance indicators, the project management methodology, quality reviews of deliverables etc.

The project office seeks to better coordinate in cross cutting activities and themes that involve several operational areas. Such activities include the preparation of briefings, coordinating select policy recommendations across the Department, drafting formal contributions and documents etc.

In 2017 ENISA seeks to develop further the management of information security risks and controls under the authority of the Agency's management. In terms of developing the Information Security Management Systems and against a risk assessment and assets inventory the documented policy framework will be tested against implemented practices.

3.5.3 Objective 5.3. International relations

Under the ED's guidance and initiative, ENISA will seek to strengthen contacts at international level.

3.6 Activity 6 – Compliance and support

The ENISA Administration and Resources Department (ARD) strives to operate a cost-efficient, customer-oriented service department.

ENISA ARD has contributed to the ENISA strategy both internally and externally seeking the optimal solutions for delivering on the mandate of ENISA.

The ARD seeks to enhance the functionality of the administrative procedures of the Agency, to provide administration related services and strategical support and orientation for the Agency recourses strategy.

ARD oversees a variety of programs, projects and services relating to personnel, finance, purchasing, technology, facilities management, health, safety, security, and much more.

3.6.1 Objective 6.1. IT Objectives

In 2015 ENISA set out to define its ICT strategy for the years 2015 - 2018. The main thrust of this strategy is to consolidate systems and applications on a maximum of 2 platforms, maximise data sharing, make applications available in a secure way on the most widely used mobile devices, and, to progressively move the Agency's IT infrastructure to the Cloud. To this end the Agency will join with other EU agencies in launching in 2016 a joint tender covering Cloud services.

After the signing of the joint-Agencies tender for Cloud services (expected in 2016), the Agency will start planning and procuring Cloud services. Some of these services may be shared with other Agencies, e.g. Agency Community Cloud.

By mid-2017 it is expected that most business applications will be securely available on the most widely used mobile devices. By this timeframe the platform consolidation should be close to complete, making data (information) more readily available for reporting and monitoring purposes.

Task	Objective	Level of completion 2015	Level of completion 2016	Level of completion 2017
Consolidate systems and applications on a maximum of 2 platforms	Efficiency	20%	60%	90%
Maximise data sharing	Efficiency	30%	60%	90%
Move the Agency's IT infrastructure progressively to the Cloud	Efficiency	30%	50%	90%
Business applications will be securely available on the most widely used mobile devices.	Availability	10%	70%	90%
Continuous Operations	Availability	98%	98,5%	99%

3.6.2 Objective 6.2. Finance, Accounting and Procurement Objectives

The key objective here is to ensure the compliance of the financial resources management with the applicable rules, and in particular with the sound financial management, efficiency and economy principles as set down in the Financial Regulation. As the Agency resources are derived from the Union Budget, management is required to comply with a set of regulations, rules and standards set down by the Union competent institutions. The Unit is responsible for high quality reporting (annual accounts) and contribution to the audit and discharge procedures.

In 2017, the Agency expects to benefit from the deployment of tools used to simplify and automate its work, automated applications (Budget Management, Budget Reporting, Procurement planning), e-Prior (EU Commission platform for the management of the procurement lifecycle, from pre-award to post-award of a contract), as well as the integration of systems (staff missions, project management and budget management).

The deployment of tools coupled by outsourcing of certain activities of low value, is expected to improve the overall resources management and reporting capacity of the Agency.

The aim is to contribute to the Agency annual and multi annual programming from inception to execution. The financial resources are allocated according to the expressed needs of the organisational Units according to the priorities set by the Agency management.

Key objectives for the year 2017 include high budget commitment and payment rates, low number of budget transfers during the year, planned and justified carry overs, and reduced average payment delay.

Task	Objective	Level of completion 2015	Level of completion 2016	Level of completion 2017
Deployment of new financial information systems	Efficiency, better reporting, information quickly provided	10%	70%	100%
Budget Implementation (Committed appropriations of the year)	Efficiency and Sound Financial Management	100%	100%	100%
Payments against appropriations of the year (C1 funds)	Efficiency and Sound Financial Management	85%	87%	90%

Payments against appropriations carried over from year N-1 (C8 funds)	Efficiency and Sound Financial Management	90%	95%	95%
Payments made within Financial Regulation timeframe	Efficiency and Sound Financial Management	85%	87%	90%

3.6.3 Objective 6.3. Human Resources Objectives

In 2017, ENISA will recruit additional personnel in line with the Agency's Establishment Plan. Some of these recruitments relate to staff turnover at the Agency. Recruitment is carried out in an efficient and timely manner.

In 2017, the annual performance appraisal exercise will be carried out taking into account the new staff regulations and applicable rules. HR is also responsible for training and arranges for both mandatory and professional development training. These training exercises are conducted to ensure that staff members retain and improve their skills and competencies.

Task	Objective	Level of completion 2015	Level of completion 2016	Level of completion 2017
Posts on the Agency establishment plan filled	Minimum 95 % of the recruitment target reached	95%	97%	99%
Respect the recruitment procedure time framework. Recruitment is defined as the time between placing the advert and identifying a successful candidate.	Average length of recruitment procedure: 4 months (including the 1-month period of publication of the Vacancy Notice)	4 months	3 months	2 months
Turnover of staff	Reduce the turnover of TA's to less than 10%	<10%	<8%	<7%

3.6.4 Objective 6.4. Compliance, communication, information security and control coordination

3.6.4.1 Objective 6.4.1. Internal Communication

Internal communication activities aim to keep all those working within the Agency informed and to enable both management and staff to fulfil their responsibilities effectively and efficiently. Staff members must be regularly informed of policy decisions taken by the Management Board and ENISA Senior Management, enabling them to better understand their role and to acquire broader knowledge of the Agency's mission and activities. This should contribute to a common corporate culture, improve staff engagement and ultimately also improve the operations implementation of the work program. It is proposed that the completion of the internal communications strategy will be completed in 2016. Thereafter it is envisaged to do an annual review of this Strategy to ensure that it is kept up to date and appropriate for the Agency.

Task	Objective	Level of completion 2015	Level of completion 2016	Level of completion 2017
Increase the level of awareness of ENISA's	Develop Internal Communication Strategy	10%	50%	80%

work and recent developments related to the Agency.				
Increase the staff motivation.	Bring all staff members and offices closer for a better and fruitful cooperation	20%	60%	85%

3.6.4.2 Objective 6.4.2. Legal Affairs

In 2017, Legal Affairs will continue supporting the legal aspects associated with the operation of the Agency. This includes dealing with matters such as contracts, procurement, employment related matters, data protection and corporate governance matters. The Legal Affairs function also includes dealing with complaints submitted pursuant to Article 90 of the Staff Regulations and complaints to the European Ombudsman and representing the Agency before the European Court of Justice, General Court or Civil Service Tribunal.

3.6.4.3 Objective 6.4.3. Data Protection Compliance tasks and Data protection Office

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

- Inform and advise ENISA of its obligations pursuant to Regulation 45/2001/EC and 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 EDPS.
- Monitor the documentation, notification and communication of personal data in the context of ENISA's operations.
- Act as ENISA's contact point for EDPS on issues related to the processing of personal data; co-operate and consult with EPDS whenever needed.

3.6.4.4 Objective 6.4.4. Information Security coordination

The Information Security Officer (ISO) coordinates the Information Security Management System on behalf of the Authorising Officer. In particular the ISO advises the ICT Unit alongside the Quality and Data Management Unit to develop and implement information security policies, standards, guidelines and baselines that seek to secure the confidentiality, integrity and authentication of the information systems of the Agency. The ISO is instrumental in incident handling and incident response and security event monitoring. The ISO also leads the security training for the Agency's staff and he provides security guidance on all IT projects, including the evaluation and recommendation of technical controls. In 2017 the ISO will contribute to such goals as:

- Improving the security posture of ENISA by planning penetration tests and vulnerability assessments
- Advising on security policies and updating existing ones in line with the evolution of threats and risks
- Improving the internal security training for ENISA staff
- Implementing new systems and tools that can support improvements on IT Security.

3.6.4.5 Objective 6.4.5. Internal Control Coordination

Internal Control reviews and evaluates risk management, governance and internal control processes of the Agency, in order to provide, to the Senior Management, Executive Director and the Management Board,

independent and objective assurance and consulting services designed to add value and improve the Agency's operations.

3.7 Summary tables

3.7.1 List of Outputs work programme 2017

Activity 1 – Expertise. Anticipate and support Europe in facing emerging network and information security challenges
Objective 1.1. Improving the expertise related to Critical Information Infrastructures
Output O.1.1.1 – Baseline Security Recommendations for the Energy Sector
Output O.1.1.2 – Baseline Security Recommendations for the Transport Sector in the context of Smart Cities
Output O.1.1.3 – Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures
Output O.1.1.4 – Baseline Security Recommendations for the eHealth Sector
Objective 1.2. NIS Threats Landscape and Analysis
Output O.1.2.1 – Annual ENISA Threat Landscape
Output O.1.2.2 – Thematic Threat Landscape reports
Output O.1.2.3 – Annual Incident Analysis Report for the Telecom Sector (article 13 a)
Output O.1.2.4 – Annual Incident Analysis Report for Trust Service Providers (article 19)
Objective 1.3. Research & Development, Innovation
Output O.1.3.1 – Guidelines for the European standardisation in the field of ICT security
Output O.1.3.2 – Priorities for EU Research & Development in the context of H2020
Objective 1.4. Response to Article 14 Requests under Expertise Activity
Output O.1.4.1. Response to Requests under Expertise Activity
Activity 2 – Policy. Promote network and information security as an EU policy priority
Objective 2.1. Supporting EU policy development.
Output O.2.1.1 – Contribute to EU policy in the area of eHealth
Output O.2.1.2 – Contribute to EU policy in the area of Smart Grids and ICS-SCADA
Output O.2.1.3 – Support the policy discussions in the area of IT security certification
Output O.2.1.4 – Restricted. Towards a Digital Single Market for high quality NIS products and services
Output O.2.1.5 – Contribute to EU policy in the area of Finance
Output O.2.1.6 – Contribute to EU policy in the area of Smart Transportation
Objective 2.2. Supporting EU policy implementation
Output O.2.2.1 – Contribute to EU policy in the area of electronic communications sector
Output O.2.2.2 – Develop guidelines for the implementation of mandatory incident reporting
Output O.2.2.3 – Engaging eIDAS Competent Authorities and the private sector in the implementation of article 19
Output O.2.2.4 - Recommendations for technical implementations of the eIDAS Regulation (Q4, 2017)
Output O.2.2.5 - Recommendations for technical implementations of the General Data Protection Regulation
Output O.2.2.6 – Privacy enhancing technologies
Output O.2.2.7 – Guidelines for data controllers on securing the automated processing of personal data
Output O.2.2.8 – Supporting the Implementation of the NIS Directive
Objective 2.3. Response to Article 14 Requests under Policy Activity
Output O.2.3.1. Response to Requests under Policy Activity
Activity 3 – Capacity. Support Europe maintaining state-of-the-art network and information security capacities

Objective 3.1. Assist Member States' capacity building.
Output O.3.1.1 – Status report on Cyber security skills
Output O.3.1.2 – Support national and governmental CSIRTs capabilities
Output O.3.1.3 – Update and provide technical trainings for MS and EU bodies
Output O.3.1.4 – Support EU MS in the development and assessment of NCSS
Output O.3.1.5 – EU CSIRT network secretariat
Objective 3.2. Support EU institutions' capacity building.
Output O.3.2.1 – Restricted and public Info notes on NIS
Output O.3.2.2 – Restricted. Upon request, support the assessment of existing policies/procedures/practices on NIS within EU institutions
[Output O.3.2.3 - Study on the applications of encryption and other technologies as enabler of the European Digital Single market]
Objective 3.3. Assist private sector capacity building.
Output O.3.3.1 – Cybersecurity culture: from identifying the issues to providing working scenarios for management level
Output O.3.3.2 – Handbooks on cyber-hygiene when processing customer data for different scale companies
Output O.3.3.3 – Good Practices and Recommendations on Cyber Insurance
Output O.3.3.4 – Security Recommendations for digital Service Providers and Users of Trust Services
Objective 3.4. Assist in improving general awareness
Output O.3.4.1 – Cyber Security Challenges
Output O.3.4.2 – European Cyber Security Month deployment
Output O.3.4.3 –Online privacy portal
Objective 3.5. Response to Article 14 Requests under Capacity Activity
Output O.3.5.1. Response to Requests under Capacity Activity
Activity 4 – Community. Foster the emerging European network and information security community
Objective 4.1. Cyber crisis cooperation
Output O.4.1.1 – Evaluation of Cyber Europe 2016
Output O.4.1.2 – Report on Exercise After Action Activities from 2014-16
Output O.4.1.3 – Planning of Cyber Europe 2018
Output O.4.1.4 – Trainings on Cyber Exercise Planning and Cyber Crisis Management
Output O.4.1.5 – Cyber Exercise Platform (CEP) Development and Content Management
Output O.4.1.6 – Design of Cyber Security Games in CEP
Output O.4.1.7 – Cyber Exercises Support to MS and EU Institutions
Output O.4.1.8 – EU-level Cyber Crisis and Incident Management Procedures and Infrastructures
Output 0.4.1.9 – Support the Connecting Europe Facility (CEF) Cybersecurity Digital Service Infrastructure (DSI)
Objective 4.2. CSIRT and other NIS community building.
Output O.4.2.1 Technical training community support for MS and EU bodies
Output O.4.2.2 – Support the fight against cybercrime and collaboration between CSIRTs and LEA
Output O.4.2.3 – Support EU CSIRT network community building
Objective 4.3. Response to Article 14 Requests under Community Activity
Output O.4.3.1. Response to Requests under Community Building Activity
Activity 5 – Enabling. Reinforce ENISA's impact
Objective 5.1. Management

Objective 5.2. Engagement with stakeholders
Objective 5.3. International relations
Activity 6 – Compliance and support
Objective 6.1. IT Objectives
Objective 6.2. Finance, Accounting and Procurement Objectives
Objective 6.3. Human Resources Objectives
Objective 6.4. Compliance, communication, information security and control coordination
Objective 6.4.1. Internal Communication
Objective 6.4.2. Legal Affairs
Objective 6.4.3. Data Protection Compliance tasks and Data protection Office
Objective 6.4.4. Information Security coordination
Objective 6.4.5. Internal Control Coordination

3.7.2 Overview of activities budget and resources

The budget and posts distribution is based on the Activity Based Budgeting (ABB) methodology of the Agency, which is line with the Activity Based Management (ABM) principle. ABB focuses on integrated budgeting and financial management, based on activities linked to the Agency's priorities and objectives.

Based on the ABB methodology, direct and indirect costs are distributed to Activities, according to the following assumptions:

- Direct FTE: FTEs allocated to Core Activities (A1 to A4) and Enabling activity (A5)
- Indirect FTE: FTEs from Activity 6 (compliance and resourcing) are re-distributed according to the ratio of FTEs allocated to Core Activities - A1 to A4, and Enabling activity – A5, to the total FTEs.
- Total posts (FTEs) are the sum of Direct and Indirect FTEs
- Direct Budget:
  - The cost estimate of each activity (A1 to A4 and A5) in terms of goods and services procured
  - The cost estimate of salaries of Direct FTEs attributed, based on an average salary calculation.
  - The cost estimate of missions of Direct FTEs attributed.
  - Overhead costs (A6 activity costs) distributed to Direct FTEs.
- Indirect Budget:
  - The cost estimate of salaries of Indirect FTEs attributed, based on an average salary calculation.
  - The cost estimate of missions of Indirect FTEs attributed.
  - Overhead costs (A6 activity costs) distributed to Indirect FTEs.
- Total Budget is the sum of the Direct and Indirect Budget.

The budget appropriations, within the summary tables include the total budget request of the Agency, including the new tasks and their requirements for additional financial and human resources. A separate Annex, Annex B details the resources and budget appropriations required for the new tasks.

The table below presents the allocation of financial and human resources to Activities of the Agency based on the ABB methodology.

Activity / Objective	Total budget, including new tasks (€)	Total posts, including new tasks (FTEs)
Activity 1 – Expertise. Anticipate and support Europe in facing emerging network and information security challenges	**1.894.201,35**	**12,50**
Objective 1.1. Improving the expertise related to Critical Information Infrastructures	925.650,70	6,00
Objective 1.2. NIS Threats Landscape and Analysis	574.794,53	3,53
Objective 1.3. Research & Development, Innovation	285.243,40	1,96
Objective 1.4. Response to Article 14 Requests under Expertise Activity	108.512,72	1,01
Activity 2 – Policy. Promote network and information security as an EU policy priority	**4.313.453,60**	**29,04**
Objective 2.1. Supporting EU policy development.	1.164.430,06	7,34
Objective 2.2. Supporting EU policy implementation	2.850.613,55	18,92
Objective 2.3. Response to Article 14 Requests under Policy Activity	298.409,99	2,78
Activity 3 – Capacity. Support Europe maintaining up state-of-the-art network and information security capacities	**2.676.980,23**	**18,76**
Objective 3.1. Assist Member States' capacity building.	813.089,30	4,60
Objective 3.2. Support EU institutions' capacity building.	384.379,17	3,31
Objective 3.3. Assist private sector capacity building.	638.407,30	4,05
Objective 3.4. Assist in improving general awareness	434.181,76	3,01
Objective 3.5. Response to Article 14 Requests under Capacity Activity	406.922,71	3,78
Activity 4 – Community. Foster the emerging European network and information security community	**3.930.648,79**	**25,68**
Objective 4.1. Cyber crisis cooperation	2.748.336,64	18,77
Objective 4.2. CSIRT and other NIS community building.	1.060.235,34	5,78
Objective 4.3. Response to Article 14 Requests under Community Activity	122.076,81	1,14
Activity 5 – Enabling. Reinforce ENISA's impact	**2.805.564,95**	**18,17**
Objective 5.1. Management	1.259.622,40	8,11
Objective 5.2. Engagement with stakeholders	1.497.281,18	9,63
Objective 5.3. International relations	48.661,37	0,42
Activity 6 – Compliance and support	**675.451,07**	**4,85**
Objective 6.1. IT Objectives	206.206,64	1,48
Objective 6.2. Finance, Accounting and Procurement Objectives	235.664,73	1,69
Objective 6.3. Human Resources Objectives	138.453,03	0,99
Objective 6.4. Compliance, communication, information security and control coordination	95.126,67	0,70
Total budget and resources, including new tasks	**16.296.300,00**	**109,00**

Annexes A

A.1 Annex I: Resource allocation per Activity 2017 – 2019

Section 2.2 of the document presents in a pie chart the distribution of resources proposed for 2017.

The Agency identified new tasks which would require extra budget and resources and more details are presented in Annex B.

A.2 Annex II: Human and Financial Resources 2017-2019

Table 1 – Expenditure

Expenditure	2016		2017	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1	6.334.000	6.334.000	8.963.800	8.963.800
Title 2	1.600.000	1.600.000	2.179.000	2.179.000
Title 3	3.126.564	3.126.564	5.153.500	5.153.500
Total expenditure	**11.060.564**	**11.060.564**	**16.296.300**	**16.296.300**

EXPENDITURE	Commitment appropriations						
	Executed Budget 2015	Budget 2016	Draft Budget 2017		VAR 2017 / 2016	Envisaged in 2018	Envisaged 2019
			Agency request	Budget Forecast			
Title 1 Staff Expenditure	**5.923.926**	**6.334.000**	**8.963.800**	**8.963.800**	**41,52%**	**8.370.736**	**8.530.351**
11 Staff in active employment	4.515.300	5.267.000	6.893.800	6.893.800	30,89%	7.015.736	7.153.351
- of which establishment plan posts							
- of which external personnel							
12 Recruitment expenditure	356.509	195.000	995.000	995.000	410,26%	250.000	254.000
13 Socio-medical services and training	140.980	218.000	260.000	260.000	19,27%	270.000	277.000
14 Temporary assistance	911.137	654.000	815.000	815.000	24,62%	835.000	846.000
Title 2 Building, equipment and miscellaneous expenditure	**1.427.497**	**1.600.000**	**2.179.000**	**2.179.000**	**36,19%**	**2.072.000**	**2.084.000**
20 Buildings and associated costs[7]	923.342	1.041.000	1.206.000	1.206.000	15,85%	1.207.000	1.210.000

[7] Including possible repayment of interest; detailed information as regards building policy provided in Table in Annex III

21 Movable property and associated costs	22.551	62.000	232.000	232.000	274,19%	157.000	159.000
22 Current administrative expenditure	56.951	51.000	86.000	86.000	68,63%	88.000	91.000
23 ICT	424.653	446.000	655.000	655.000	46,86%	620.000	624.000
Title 3 Operational expenditure	**2.712.851**	**3.126.564**	**5.153.500**	**5.153.500**	**64,83%**	**5.237.750**	**5.269.365**
30 Activities related to meetings and missions	836.823	734.000	940.500	940.500	28,13%	964.750	989.365
32 Horizontal operational activities	408.267	392.564	643.000	643.000	63,79%	643.000	650.000
36 Core operational activities	1.467.761	2.000.000	3.570.000	3.570.000	78,50%	3.630.000	3.630.000
TOTAL EXPENDITURE	**10.064.274**	**11.060.564**	**16.296.300**	**16.296.300**	**47,34%**	**15.680.486**	**15.883.716**

Table 2 – Revenue

Revenues	2016	2017
	Revenues estimated by the agency	Budget Forecast
EU contribution	10.120.000	15.240.000
Other revenue	940.564	1.056.300
Total revenues	**11.060.564**	**16.296.300**

REVENUES	2015	2016	2017		VAR 2017 /2016	Envisaged 2018	Envisaged 2019
	Executed Budget	Revenues estimated by the agency	As requested by the agency	Budget Forecast			
1 REVENUE FROM FEES AND CHARGES							
2. EU CONTRIBUTION	9.155.661	10.120.000	15.240.000		50,59%	14.636.486	14.834.716
of which Administrative (Title 1 and Title 2)							
of which Operational (Title 3)							
of which assigned revenues deriving from previous years' surpluses							
3 THIRD COUNTRIES CONTRIBUTION (incl. EFTA and candidate countries)	270.288	300.564	416.300		38,51%	404.000	409.000
of which EFTA	270.288	300.564	416.300		38,51%	404.000	409.000

of which Candidate Countries							
4 OTHER CONTRIBUTIONS	616.379	640.000	640.000		0,00%	640.000	640.000
of which delegation agreement, ad hoc grants							
5 ADMINISTRATIVE OPERATIONS	21.946						
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT							
7 CORRECTION OF BUDGETARY IMBALANCES							
TOTAL REVENUES	**10.064.274**	**11.060.564**	**16.296.300**		**47,34%**	**15.680.486**	**15.883.716**

Table 3 – Budget outturn and cancellation of appropriations

Calculation budget outturn

Budget outturn	2013	2014	2015
Revenue actually received (+)	9.370.250	10.019.554	10.069.280
Payments made (-)	-8.147.389	-8.710.278	-9.395.559
Carry-over of appropriations (-)	-1.222.860	-1.333.221	-674.521
Cancellation of appropriations carried over (+)	55.320	74.505	80.675
Adjustment for carry over of assigned revenue appropriations from previous year (+)			800
Exchange rate differences (+/-)	-270	-291	-278
Adjustment for negative balance from previous year (-)			
Total	55.050	50.260	80.397

Budget Outturn

The Budget Outturn 2015 demonstrates a commitment rate of 100,00 % of total appropriations of the year at year end (31/12). The high commitment rate shows the already proven capacity of the Agency to fully implement its annual appropriations. The same commitment rate achieved in 2010, 2011, 2012, 2013 and 2014, is maintained for a sixth year in a row. The payment rate reached 92,89 % (85,61% in 2014) and the amount carried forward to 2015 was EUR 671.393,26 (EUR 1 308 475,80 in 2014) representing 7,11% of total C1 appropriations 2015 (from 14,39% in 2014).

Cancellation of appropriations

- Commitment Appropriations

No commitment appropriations were cancelled.

The appropriations of 2015 were fully utilised, i.e. the commitment rate reached 100,00%.

- Payment Appropriations

No payment appropriations were cancelled.

The appropriations of 2014 carried over to 2015 were utilised at a rate of 93,95 % (automatic and non-automatic carry-overs) which indicates a satisfactory capability of estimation of needs. From the amount of EUR 1 332 420,80 carried forward, only the amount of EUR 80 675,08 was cancelled, due to the fact that the estimated expenditure deviated from the actual.

A.3 Annex III: Human Resources - Quantitative

Table 1 – Staff population and its evolution; Overview of all categories of staff

Staff population		Actually filled as of 31.12 2014	Authorised under EU budget 2015	Actually filled as of 31 12.2015	Authorised under EU budget for year 2016	Actually filled as of 31.12.2016	n draft budget for year 2017	Envisaged in 2018	Envisaged in 2019
Officials	AD								
	AST								
	AST/SC								
TA	AD	30	32	30	34	34	59	59	59
	AST	16	16	15	14	14	14	13	13
	AST/SC								
Total		**46**	**48**	**45**	**48**	**48**	**73**	**72**	**72**
CA GFIV			7	9	30	30	30	30	30
CA GF III		12	15	11	5	5	5	5	5
CA GF II		1	1	1	0	0	0	0	0
CA GFI		1	1	1	0	0	0	0	0
Total CA		**14**	**24**	**22**	**35**	**35**	**35**	**35**	**35**
SNE		**2**	**3**	**2**	**1**	**1**	**1**	**1**	**1**
Structural service providers									
TOTAL		**62**	**75**	**69**	**84**	**84**	**109**	**108**	**108**
External staff for occasional replacement									

Table 2 – Multi -annual staff policy plan year 2017 – 2019

Category and grade	Establishment plan in EU Budget 2015		Filled as of 31/12/2015		Modifications in year 2015 in application of flexibility rule		Establishment plan in voted EU Budget 2016		Modifications in year 2016 in application of flexibility rule		Establishment plan in Draft EU Budget 2017		Establishment plan 2018		Establishment plan 2019	
	officials	TA	officials	TA	officials	TA	officials	TA	officials	TA	officials	TA	officials	TA	officials	TA
AD 16																
AD 15		1		1				1				1		1		1
AD 14																
AD 13																
AD 12		3		2				3				3		3		3
AD 11				1												
AD 10		5		3				5				5		5		5
AD 9		9		3				10				10		10		10
AD 8		7		4				15				19		19		19
AD 7		6		1												
AD 6				14								21		21		21
AD 5		1		1												
Total AD	**0**	**32**		**30**				**34**				**59**		**59**		**59**
AST 11																
AST 10																
AST 9																
AST 8																
AST 7								2				2		2		2
AST 6		2		1				5				5		5		5
AST 5		6		3				5				5		5		5
AST 4		3		3				2				2		1		1
AST 3		3		7												
AST 2		2		1												
AST 1																
Total AST	**0**	**16**		**15**				**14**				**14**		**13**		**13**
AST/SC1																
AST/SC2																
AST/SC3																
AST/SC4																
AST/SC5																
AST/SC6																

Total AST/SC																
TOTAL		**48**		**45**				**48**				**73**		**72**		**72**

A.4 Annex IV: Human Resources - qualitative

A.4.1 A. Recruitment policy

A recruitment policy and guidelines are published on the ENISA's website.

The policy guidelines, identifies the relevant legislation pertaining to the recruitment of staff. In addition, the composition and appointment process for the selection committee along with their duties and responsibilities are detailed. The policy also includes the duties of the Human Resources Section and the production of the selection committee report. A section is also dedicated to appeals by candidates and data protection.

A.4.2 B. Appraisal of performance and reclassification/promotions

Table 1 - Reclassification of temporary staff/promotion of officials

Category and grade	**Staff in activity at 1.01.Year 2014**		**How many staff members were promoted / reclassified in Year 2015**		**Average number of years in grade of reclassified/promoted staff members**
	officials	TA	officials	TA	
AD 16	0	0			
AD 15	0	0			
AD 14	0	1			
AD 13	0	0			
AD 12	0	2			
AD 11	0	1			
AD 10	0	4			
AD 9	0	3			
AD 8	0	3			
AD 7	0	4		**1**	**3**
AD 6	0	8		**1**	**3**
AD 5	0	0			
Total AD	**0**	**26**			
AST 11	0	0			
AST 10	0	0			
AST 9	0	0			
AST 8	0	0			
AST 7	0	0			
AST 6	0	1			
AST 5	0	3			
AST 4	0	3			

AST 3	0	6			
AST 2	0	3		**2**	**3**
AST 1	0	0			
Total AST	**0**	**16**			
AST/SC1					
AST/SC2					
AST/SC3					
AST/SC4					
AST/SC5					
AST/SC6					
Total AST/SC					
Total	**0**	**42**		**4**	

Table 2 - Reclassification of contract staff

Function Group	Grade	Staff in activity at 1.01.Year 2014	How many staff members were reclassified in Year 2015	Average number of years in grade of reclassified staff members
CA IV	18	0	0	
	17	0	0	
	16	0	0	
	15	0	0	
	14	0	0	
	13	0	0	
CA III	12	0	0	
	11	0	0	
	10	0	0	
	9	4	0	
	8	6	0	
CA II	7	0	0	
	6	1	0	
	5	1	0	
	4	0	0	
CA I	3	0	0	
	2	1	0	
	1	0	0	
Total		**13**	**0**	

ENISA has in place Management Board Decisions on the appraisal of Temporary Agents and Contract Agents which give effect to the Commission implementing Rules.

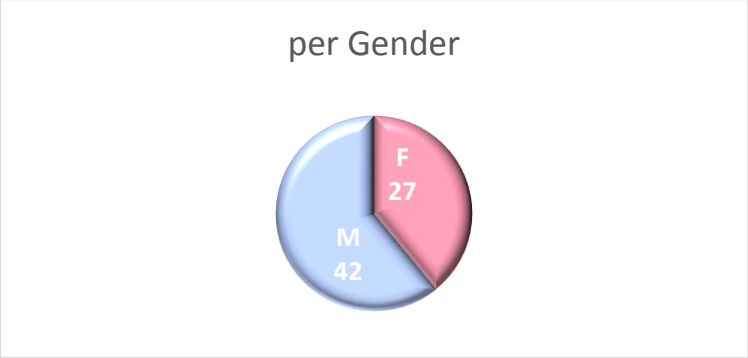
In relation to reclassification ENISA is in receipt of new implementing rules adopted by the Commission as of December 2015. ENISA is in the process of reviewing these implementing rules with a view to adopting by way of Management Board Decisions in 2016.

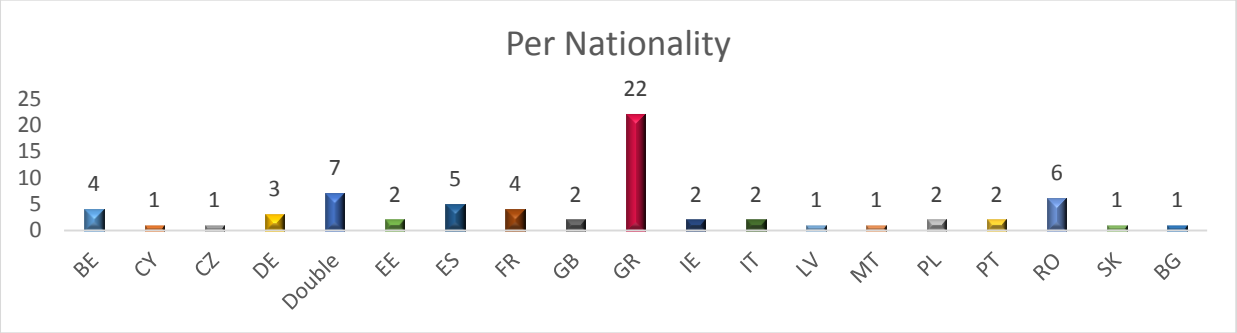
A.4.3 C. Mobility policy

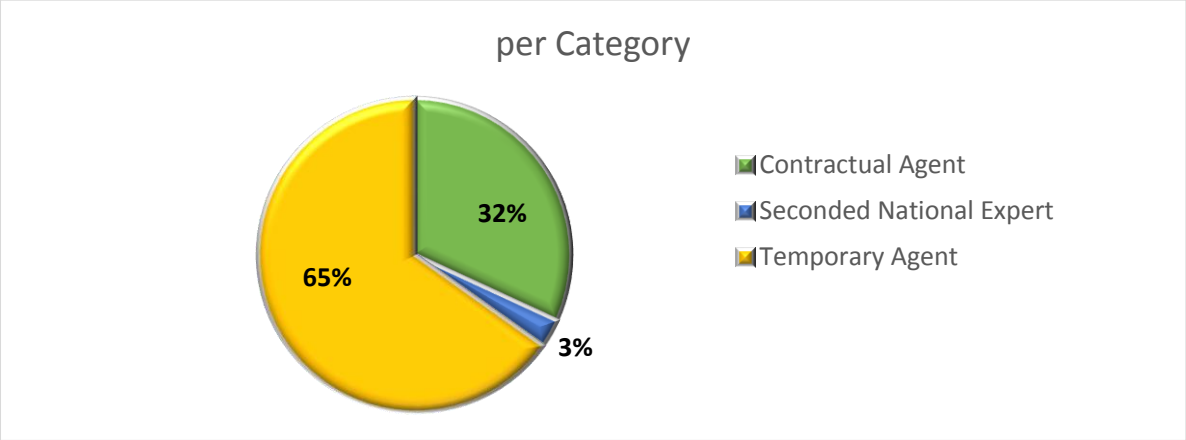
ENISA is currently preparing the adoption and implementation of the Commission Implementing rule on the policy covering mobility which will be adapted for our use. It is expected that this policy will be in place in Q1 of 2016.

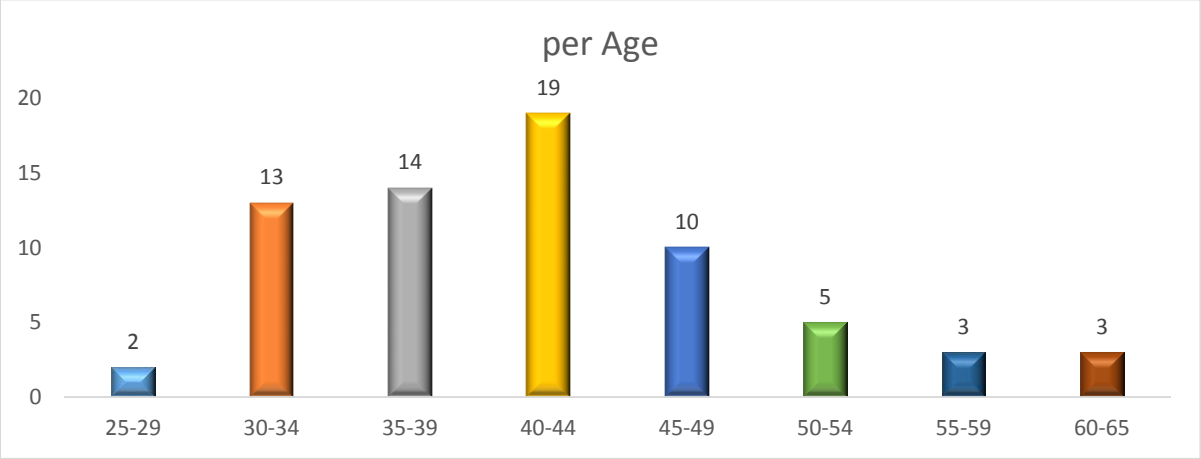
A.4.4 D. Gender and geographical balance

Please see the attached charts illustrating gender, geographical balance and category/grade in the Agency. Total number of Staff as of 31/12/2015: 69 (45 TA's: 30 AD's + 15 AST's + 22 CA's + 2 SNE's)









A.4.5 E. Schooling

A European School is located in Heraklion and is used by Staff members of ENISA.

No European School exists in Athens. To facilitate the schooling requirements of the Staff in Athens service level agreements have been concluded with a number of international schools that are attended by the children of the Staff.

A.5 Annex V: Buildings (table)

Current building(s)

	Name, location and type of building	Other Comment
Information to be provided per building:	Heraklion, Office building	The Greek Government subsidises the rent of the office in full.

	Athens, Office building	New office is occupied as of 01/03/2013 in Marousi, Athens, hosting the Core Operational activities of ENISA. The Greek Government subsidises the rent of the office in full.
Surface area (in square metres) Of which office space Of which non-office space	Heraklion : 2.042 m2, Athens: 2.036,38 m2	
Annual rent (in EUR)	Heraklion: 299 934,60 EUR Athens: 316 444,08 EUR	
Type and duration of rental contract	Heraklion, annual lease agreement, renewable Athens, lease agreement extended until February 2018	
Host country grant or support	The Greek Government subsidises the rent of the offices in full.	
Present value of the building	Not applicable	

Building projects in planning phase

Not applicable as the rent of the buildings are funded by the Greek Government.

A.6 Annex VI: Privileges and immunities

Agency privileges	Privileges granted to staff	
	Protocol of privileges and immunities / diplomatic status	**Education / day care**
In accordance with Art. 23 of Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013, the protocol No 7 on the privileges and immunities of the European Union annexed to the TEU and the TFEU applies to the Agency and its staff.	In accordance with Article 23 of Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013, the protocol No 7 on the privileges and immunities of the European Union annexed to the TEU and the TFEU applies to the Agency and its staff. The Greek Government and ENISA signed a Seat Agreement in April 2005, which was ratified by Greek Law 3572/2007 and is applicable to ENISA and its staff.	A public School of European Education, Type 2, was founded in 2005 by the Greek government in Heraklion – Crete for the children of the staff of ENISA. There is no European School operating in Athens.

A.7 Annex VII: Evaluations

An external evaluation of the Agency was delivered in October 2015 by an external consultant. The report presents the findings and conclusions from the external evaluation of ENISA's core operational activities in 2014. The overall objective of the evaluation was to evaluate the effectiveness, efficiency, added value, utility, coordination and coherence of the activities carried out by ENISA, thereby providing ENISA with an evaluation of its performance and an assessment of the possible options for change/improvement.

This evaluation is the first in a series of annual evaluations (up until 2018). Much of the data collection was carried out during the summer holiday period in 2015, which required an adaptation of the evaluation framework. More on the methodology, including strengths and weaknesses of the chosen approach. In subsequent years, the methodology will be further refined and adapted, while still enabling the tracking of performance.

The assessment of relevance relies on analysing the linkages between core operational activities and ENISA's legal mandate, and if there has been a balance in addressing different tasks. Furthermore it is based on stakeholder's opinions of whether activities are responding to needs in the EU and Member States, and on the extent to which the actual outputs have been useful (utility).

Regarding the relevance of ENISA's activities, the core operational activities carried out under the Work Programme 2014 have a clear connection to the legal mandate of ENISA. There were no instances of activities falling outside of the mandate identified and thus it can be concluded that ENISA carried out its activities as foreseen in the regulation.

The evaluation findings also show that ENISA clearly responds to a need in the European NIS landscape; a conclusion which is supported by the 2011 study conducted by the European Parliament on "The role of ENISA in contributing to a coherent and enhanced structure of network and information security in the EU and internationally" which acknowledged that ENISA's function was, at the time, increasingly seen as valuable and necessary, and that its effective mission had steadily grown over the years.

The scope and objectives of ENISA's work is seen as relevant to respond to the needs, but at the same time stakeholders see limits in ENISA's mandate and outreach. In particular, private stakeholders and industry appear to strive towards a more operational role for ENISA, going beyond the advisory and facilitating mandate of the Agency, in order to effectively achieve the overall objectives of NIS and cyber security. Such views were also expressed in the European Parliament's study, where experts noted that in the future ENISA might consider taking a limited operational role in combating cyber threats (e.g. taking on 24 x 7 responsibilities), instead of just facilitating these activities.

There are no detailed recommendations to be distilled from the evaluation in relation to relevance, but it can be noted that ENISA carries out a high number of core operational activities (in light of limited resources). A recurring comment from stakeholders was that ENISA's ambitious objectives were difficult to achieve given the small size of the agency. This was echoed in Ramboll Management Consulting and Euréval's 2009 evaluation of 26 decentralised EU agencies which noted that the small size of ENISA makes it questionable whether it has the critical mass to produce impacts in a meaningful way or whether ENISA's "good quality products" could achieve the expected results. It may be important in the future to focus on activities where there is a strong demand from the NIS communities to ensure that ENISA's deliverables achieve a real impact.

Regarding the effectiveness of ENISA's activities, the evaluation findings are positive and on most indicators ENISA's Work Programme 2014 has achieved the intended outcomes, results and impacts, as per

the judgment norm agreed for the evaluation. There is a clear pattern in terms of progress, where targets under ENISA's control (such a high quality, community building, good practice dissemination) are largely achieved. The progress towards more long term objectives looks more uncertain (preparedness to respond to crisis, increase in capacity etc.), as this is highly dependent on contextual factors as well as public and private stakeholders' engagement and investment. Still, a majority of consulted stakeholders were of the opinion that ENISA clearly contributes to ensuring a high level NIS in the EU, which should be seen as a strong achievement.

In terms of organisation and ENISA's internal functioning, the Agency seems to be largely well functioning. There are current and forecasted issues with staff shortages and difficulties in recruiting, which according to interviews could have an impact on the Agency's capacity going forward. In order to maintain a high level of expertise, the Agency must be able to attract and retain the right people, and this is currently proving difficult. There were few indications in the evaluation that ENISA did not have the right competences or sufficient capacity during 2014, but this should be followed up carefully in coming evaluations.

The division of the Agency between Heraklion and Athens sometimes leads to cumbersome work processes and lack of communication and cooperation, but it seems like ENISA staff and managements have found ways to cope with the situation and minimise negative impact. While it would certainly be more effective and efficient to have only one location. It should be noted that the evaluators did not visit Heraklion for the current evaluation; this should be taken into account when planning for the evaluation of 2015 core operational activities.

Project management and work processes are well in place, although the project management tool Matrix does not serve the purpose of day to day management. Initiatives were under way during the evaluation period to implement common "spread sheet" models across departments for day to day management of projects, this would be a good development.

Overall, the effectiveness of ENISA's activities in 2014 is assessed as good. A general observation can be made regarding the broad scope of the activities and high number of deliverables in 2014. In light of limited resources and the inherent difficulty reaching more long term impact, it could be considered to narrow the scope and number of activities, and to concentrate efforts in order to maximise chances of reaching impact. In the current evaluation the findings did not provide any direction in particular as to what activities were most effective. However, in the evaluators' opinion the findings are not sufficiently robust to draw firm conclusions, due to the limited stakeholder group consulted. This should be addressed in subsequent evaluations.

Regarding the efficiency of ENISA's activities, the operational budget of ENISA is limited, and the main expenditure relates to staff costs. In the light of the resources available (staff and expenditures), ENISA manages to produce quite a high number of deliverables which also have generated considerable outreach in terms of downloads. No indication of low efficiency was identified in the evaluation period, though specific cost saving measures could not be established.

The tasks of the ENISA and the physical location of the Agency require extensive travel by all operational staff. A more central location (in Europe) of the Agency would have been more efficient and could save travel expenses and staff resources. While relocation is not feasible under the current mandate, it should be considered when reviewing ENISA's mandate in 2018.

It should be noted that efficiency is difficult to assess without a baseline or comparison to relate to. In future evaluations, tracking of costs over years will be conducted. It could also be envisaged to compare

ENISA's costs to other (comparable) EU Agencies, on indicators such as administrative costs, travel costs, etc.

Regarding the coordination and coherence of ENISA, it can be concluded that ENISA's effectively cooperates and engages with its main stakeholders as stipulated in its mandate. The support provided by ENISA is seen as a complement to that of other public interventions, and no adverse effects were identified.

A.8 Annex VIII: Risks Year 2017

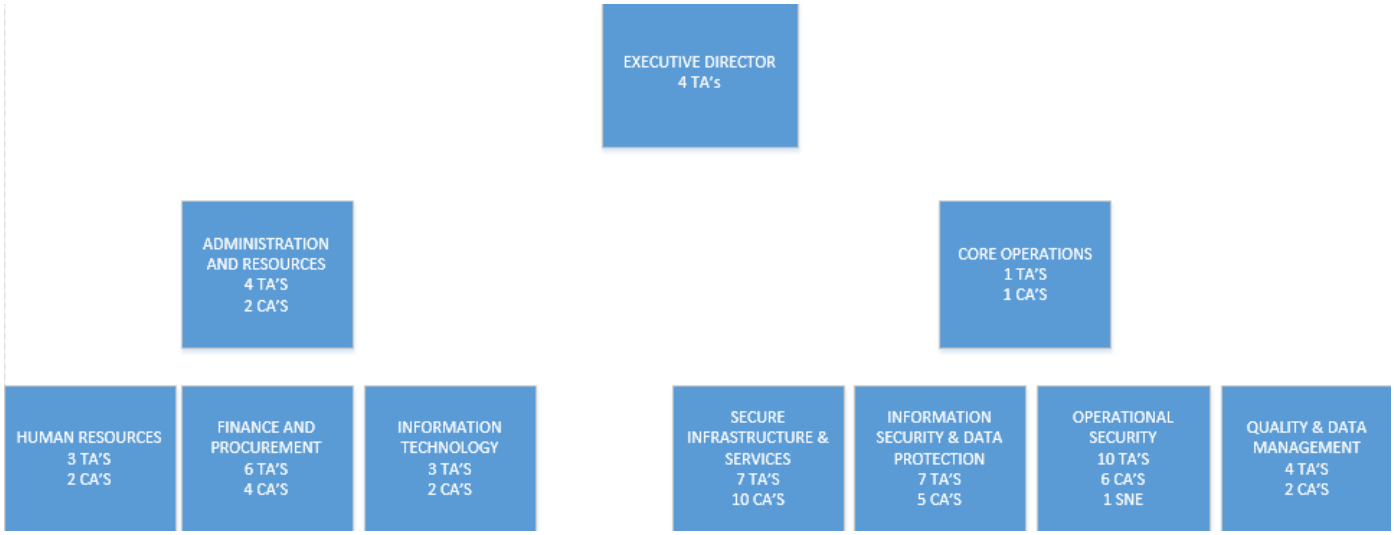
The Self Risk Assessment is on-going and the final results are not available yet.

A.9 Annex IX: Procurement plan Year 2017

Procurement planning will be provided in next versions.

A.10 Annex X: Organisation chart

Organisation chart of the Agency reflecting the situation of January 2016 is included below.



Annex B: Justification for the extra resources and budget linked to new tasks in WP17

This Annex identifies new tasks that have been included in the 2017 work programme and provides a justification for the resources necessary to carry out these tasks. This Annex seeks to present the views of the Agency with regard to its new tasks and required resources to demands therefrom.

The new tasks likely to be assigned to the Agency under the new legal framework are related to the NIS Directive including the CSIRT Secretariat, the new Telecoms Package implementation, the cPPP for Cyber Security and the implementation, maintenance and operation of the CEF (Connecting Europe Facility) SMART Digital Service Infrastructure (DSI) Core Service Platform in WP2017. Further additions are foreseen in terms of NCSS (National Cyber Security Strategies), incident reporting, certification and standards.

Pursuant to EU Regulation (526/2013) ENISA has been assigned to develop and maintain a high level of expertise in the areas of Network and Information Security (NIS) for the purpose of assisting the Union institutions, bodies, offices and agencies in developing and implementing policy.

The Agency is also required to assist Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents and stimulate broad cooperation between actors from the public and private sectors.

Recent EU initiatives in this area include the **Network and Information Security (NIS) Directive**, the Data Protection Regulation and the Digital Single Market Strategy (DSM) adopted in May 2015 that includes a public-private partnership on cybersecurity.

The EU Commission envisages that the DSM could boost the EU economy by almost €415 billion per year and create hundreds of thousands of new jobs.

ENISA recognizes the importance of cybersecurity and this proposal describes the resources requested by ENISA to fully support the EU initiatives outlined above and in particular the NIS Directive.

Resources for New Tasks[8] required:

Year	2017	2018	2019	2020
Extra posts (FTEs)	25	25	25	25
Total budget (Euro)	5.054.300,00	4.179.300,00	4.119.300,00	4.079.300,00

In case additional resources are not made available to the Agency, to the levels described above, further support rendered by ENISA for the implementation of important policy developments such as the NIS

[8] According to Article 33.9 of the Framework Financial Regulation[8], when entrusting new tasks to the Agency, the Commission shall, without prejudice to the legislative procedures for the modification of the constituent act, submit to the European Parliament and the Council the necessary information to assess the impact of the new tasks on the resources of the Agency so as to review where necessary its financing.

Directive, the Digital Single Market initiative and the General Data Protection Regulation is likely to become questionable.

Current staffing levels of the Agency point to a situation of relatively unchanged TA rates since launch (in 2004) and an increase in CA posts (mostly following mandate renewal in 2013). Adding new important policy tasks to the Agency's mandate, requires developing these new policy areas with new Experts who actually have the skills to support the new areas of policy development. These Experts need to be engaged at the appropriate level to ensure continuity and a suitable degree of performance.

The significant increase in cyber threats over the past few years, which have been thoroughly documented by the associated ENISA Threat Landscape reports leaves no doubt that better preparation in the EU requires significant increase in resources to meet cyber-security challenges and the requirements of the shifting policy framework alike.

Summary of extra posts and budget linked to new tasks for the interval 2017-2020

In this section we provide the justifications regarding the resources needs foreseen in a 4 year interval 2017-2020.

	2017	2018	2019	2020
Extra posts (FTEs)	**25,00**	**25,00**	**25,00**	**25,00**
Project Costs	1.570.000,00	1.570.000,00	1.510.000,00	1.470.000,00
Operational Costs (salaries, running costs, etc.)	3.484.300,00	2.661.486,00	2.714.715,72	2.769.010,03
Total budget (euro)	**5.054.300,00**	**4.231.486,00**	**4.224.715,72**	**4.239.010,03**

Description, direct costs and staff allocation for activities in 2017

I. Activities linked to NIS directive implementation.

There are two main activities associated with the NIS Directive that will impact the work of the Agency in 2017, namely,

- Technical measures such as NCSS, incident reporting;
- Additionally community related measures such as the CSIRT Secretariat.

The required resources presented in this sub-section only address the direct project costs increase that is necessary in order to accomplish all associated tasks meeting the requirements of the Member States and of the EU Institutions that the Agency supports. While varying degrees of involvement of the Agency can be foreseen, this document supports the view that reinforcing current resources to the required level is essential to meet the emerging regulatory requirements.

I.1. Implementation aspects covering technical measures (excluding community tasks)

The tasks identified below will be developed under Activity A2 – policy, more exactly policy implementation as WP2017 is currently structured.

Total resources needed for implementing NIS Directive: 10 FTEs and €520.000 euros.

Details are given hereinafter on a per action basis.

1	Activities	Explanation (Under A2, linked to O.2.2.)	FTEs	Project budget
1	**National Cyber Security Strategies**		**1,5**	**90k**
	1.1.	Assist MS to Develop and evaluate NCSS	0,5	30 k
	1.2.	Assist MS to develop certain capabilities at national level (e.g. define the characteristics of the competent authority)	0,5	30 k
	1.3.	Assist MS identify critical operators in sectors defined in the NIS Directive	0,5	30k
2	**Co-operation Network (except the CSIRT secretariat)**		**1**	**80k**
	2.1	Contribute to the work of the co-operation network	0,5	30 k
	2.2	Develop position papers on items asked by the co-operation network	0,5	50 k
3	**Security Requirements**		**4**	**200k**
	3.1.	Assist MS define appropriate technical and organisational measures to manage the security risks to networks and information systems for the following sectors o Energy: electricity, oil and gas o Transport: air, rail, water and road o Banking: credit institutions o Financial market infrastructures: trading venues, central counterparties o Health: healthcare providers o Water: drinking water supply and distribution o Digital infrastructure: internet exchange points (which enable interconnection between the internet's individual networks), domain name system service providers, top level domain name registries o Online marketplaces (which allow businesses to set up shops on the marketplace in order to make their products and services available online) o Cloud computing services o Search engines	3	150 k
	3.2.	Assist MS and COM to identify standards or develop new standards in the sectors defined above	0,5	25 k
	3.3.	Assist MS and COM to deploy certification in managing security risks to networks and information system for the above mentioned sectors	0,5	25 k
4	**Incident Reporting**		**3,5**	**150k**
	4.1	Assist MS to develop a harmonised framework for reporting incidents for the sectors mentioned below o Energy: electricity, oil and gas o Transport: air, rail, water and road o Banking: credit institutions o Financial market infrastructures: trading venues, central counterparties o Health: healthcare providers o Water: drinking water supply and distribution o Digital infrastructure: internet exchange points (which enable interconnection between the internet's individual networks), domain name system service providers, top level domain name registries o Online marketplaces (which allow businesses to set up shops on the marketplace in order to make their products and services available online) o Cloud computing services o Search engines	3,5	150 k
	TOTAL		**10**	**520k**

I.2. NIS directive and community related activities under Activity A3 (capacity building)

These tasks will be carried out under Activity A3 – capacity building.

	Activities	Explanation	FTEs	Project budget

5	**EU CSIRT network secretariat (under A3, linked to O.3.1.5)**	**1**	**50k**
5.1.	Provide EU CSIRT network secretariat (e.g. logistics for meetings, workshops, reporting; drafting minutes)	1	50 k

I.3. NIS directive and community related activities under Activity A4 (community)

These tasks will be carried out under Activity A4 – community.

	Activities	Explanation	FTEs	Project budget
6	**Support EU-CSIRT network community building (under A4, linked to O.4.2.3)**		**2**	**300k**
	6.1.	EU CSIRT network support • CSIRT network capabilities: Handbook with CSIRT policies templates in main EU languages and Guidelines on how to implement core CSIRT services and tools (one tender, budget €70.000,00) • CSIRT maturity: Update on CSIRT assessment parameters for EU national CSIRTs (one tender, budget €30.000,00)	0,9	100 k
	6.2.	Expanding ENISA CSIRT Inventory service for EU national and governmental CSIRTs (build upon ENISA CSIRT Inventory tool) - new functionalities such as CSIRT services, operations mode and capabilities (NIS Directive art 8b (3) a)	0,1	0 k
	6.3.	Annual EU CSIRT network meetings; under CSIRT community building: Facilitate teams' participation in the regular EU CSIRT network meetings; budget €200.000,00	1	200k

II. Connecting Europe Facility (CEF) related activities

This section covers the new tasks linked to *Connecting Europe Facility* (CEF) Cybersecurity Digital Service Infrastructure (DSI). These tasks are going to be located under Activity 4, Community.

(All tasks for staff are continuous, as we talk about continuous operation and improvement of a live platform; on top of operation and development all staff is also involved in the tender procedures: Budget is spent mainly in dedicated tenders for implementation and improvement of implementation.)

	Activities	Explanation	FTEs	Project budget
7	**Connecting Europe Facility (CEF)[9] (under A4, linked to O.4.1.9)**		**10**	**500k**
	7.1.	• Project manager responsible for the development and platform enhancements • Project manager responsible for operations covering also transition and service procurement	2	
	7.2.	Support, development, maintenance and operation • Developers / support for project manager (will support the initial implementation and the continuous update of the platform and its services. Larger development chunks are outsourced, see below) • Operators (responsible for communication with stakeholders, adjustment of requirements and consequences for the implementation and operating	8	500k

[9] Budget increase for CEF represents an increase for ENISA, and not for the Union budget, as this activity is already authorised and managed as an ongoing project.

	the information exchange in shifts. This is planned for office hours' operation only, not 24/7!) Budget: 100K = adjustment of requirements (1 tender) 4x25k = 4 events for stakeholders (quarterly; with potential for reimbursement on request) 100K = plan for hand-over and initial transformation/adjustment of platform operation (1 tender) 5x25K = quarterly rounds of implementation and changes (monthly updates; purchase orders)

III. Supporting the implementation and operation of a common EU ICT security certification framework

The tasks identified hereinafter will be developed under Activity A2 – policy, more exactly, Objective 2.1, policy implementation, as WP2017 is currently structured.

The description of this activity will be extended in WP 2017 (linked to Output O.2.1.3 – Support the policy discussions in the area of IT security certification) to match the scope of the activity described below.

Total resources needed for implementing EU ICT security product certification framework: 2 FTEs and €200.000.

Details are given hereinafter on a per action basis.

	Activities	Explanation	FTEs	Project budget
8	**Supporting the implementation and operation of a common EU ICT security certification framework (under A2, extension of O.2.1.3)**		**2**	**200k**
	8.1.	Coordination and logistical support of Member States representatives and experts' groups meetings to agree and develop a common EU ICT security certification framework (estimated six meetings)	0.25	50K
	8.2.	Preparation of reference documents for the implementation and operation of the common EU ICT security certification framework	1	100K
	8.3	Organization of open workshops to collect input from all stakeholders in the ICT security product field (estimated two workshops)	0.25	25K
	8.4	Creation of a centralized online catalogue of certified products and updated online information on the scheme	0.25	25K
	8.5	Support to the EU Commission in legislative initiatives involving ICT security certification	0.25	0K

Summary of costs for 2017 and following years

Summary of direct costs per Objective/Activity

	Location in WP2017	Explanation	Type of posts	FTEs	Project budget
1	**Activity 2, Objective 2.2**	**Policy implementation (NIS directive)**	8 AD6s and 2 AD8	**10**	**520k**
2	**Activity 3, Objective 3.1**	**Capacity building – community (NIS directive)**	1 AD6s	**1**	**50k**
3	**Activity 4, Objective 4.2**	**Community – NIS directive**	2 AD6s	**2**	**300k**
4	**Activity 4, Objective 4.1**	**Community - CEF**	8 AD6s and 2 AD8	**10**	**500k**
5	**Activity 2, Objective 2.1**	**Policy Implementation (ICT security certification framework)**	2 AD6s	**2**	**200K**

Total	Direct costs	25	1570k

Detailed project costs and operational costs for 2017-2020

Extra Posts and Costs / Year	2017	2018	2019	2020
Extra posts (FTEs)	25	25	25	25
Extra project budget	**1.570.000,00**	**1.570.000,00**	**1.510.000,00**	**1.470.000,00**
Annual salary cost	1.696.800,00	1.730.736,00	1.765.350,72	1.800.657,73
Investments costs (2017)	875.000,00	0	0	0
Running costs (missions, building, indirect costs)	912.500,00	930.750,00	949.365,00	968.352,30
Total operational budget	**3.484.300,00**	**2.661.486,00**	**2.714.715,72**	**2.769.010,03**
Total extra budget (euro)	**5.054.300,00**	**4.231.486,00**	**4.224.715,72**	**4.239.010,03**

Foreseen evolution in the new tasks for the period 2017-2020

In comparison with the detail presented for 2017, this sub-section presents the foreseen trends and possible variations on resources:

- Policy implementation (NIS directive)
  - After the initial set up of the community in 2016 and 2017 ENISA needs to sustain all its operations with regards to this work item.
- Capacity building – community (NIS directive)
  - The CSIRT network secretariat tasks will remain unchanged.
- Community – NIS directive
  - After the initial set up of the community in 2016 and 2017 ENISA needs to sustain all its operations with regards to this work item. However, we expect MSs to gradually integrate some of these tasks. ENISA will still support MSs that will not achieve this integration.
- Community – CEF
  - The CEF Digital Service Infrastructure (DSI) will be handed over to be fully operational by ENISA after the initial contract with a private company issued by the European Commission ends in 2018. The staff needed to be recruited, trained and prepared to fully operate, maintain and further develop the Infrastructure as well as build the community around it by 2018. Therefore no fluctuations in requirements are foreseen.
- Policy implementation (ICT security certification framework)
  - After the initial set up of the community in 2016 and 2017 ENISA needs to sustain all its operations with regards to this work item.

.

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 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu