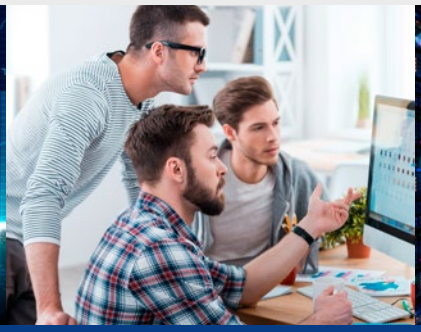
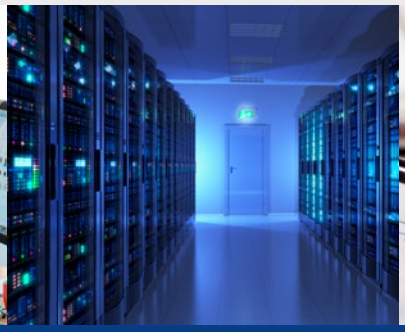
ENISA PROGRAMMING DOCUMENT


The EU Cyber Security Agency

ENISA.EUROPA.EU

2017–2019

ABOUT ENISA

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

CONTACT

For contacting ENISA or for general enquiries please use the following details:
info@enisa.europa.eu
www.enisa.europa.eu

LEGAL NOTICE

This publication presents the ENISA Programing Document 2017-2019 as approved by Management Board in Decision No MB/2016/13. The Management Board may amend Work Programme 2017 at any time.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

Catalogue number: TP-AH-16-001-EN-N
ISSN: 2467-4176
ISBN 978-92-95032-43-9
DOI: 10.2824/132933

ENISA PROGRAMMING DOCUMENT

2017–2019

Including Multiannual planning, Work programme 2017 and Multiannual staff planning

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 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 and during 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 Programming Document 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 programming documents provided in the context of Framework Financial Regulation.

The budget and resources allocations within the summary tables and Annexes are in line with the COM Multiannual Financial Framework (MAFF) 2014-2020.

LIST OF ACRONYMS

ABB: Activity Based Budgeting
APF: Annual Privacy Forum
BEREC: Body of European Regulators of Electronic Communications
cPPP: Cyber Security Public-Private Partnership
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
ECSO: European Cyber Security Organisation
ED: Executive Director
EDO: Executive Directors Office
EDPS: European Data Protection Supervisor
eID: electronic Identity
eIDAS: Regulation on electronic identification and trusted services for electronic transactions in the internal market
ENISA: European Union Agency for Network and Information Security
ETSI: European Telecommunications Standards Institute
EU: European Union
FAP: Finance, Accounting and 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
NAPARC: National Public Authority Representatives Committee
NCSS: National Cyber Security Strategies
NIS: Network and Information Security
NISD: NIS directive
NLO: National Liaison Officer
NRA: National Regulatory Authority
O: Output
OES: Operators of Essential Services
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
SB: Supervisory Body
SCADA: Supervisory Control and Data Acquisition
SDO: Standard Developing Organization
SME: Small and Medium Enterprise
SO: Strategic Objectives
SOP: Standard Operating Procedure
SRAD: Stakeholder Relations and Administration Department
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

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.

Reference	Policy/legislation reference. Complete title and link
2016	
The NIS directive	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1-30, available at: ELI: http://data.europa.eu/eli/dir/2016/1148/oj
COM communication 0410/2016 on cPPP	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0410
COM decision C(2016)4400 on cPPP	COMMISSION DECISION of 5.7.2016 on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation, Brussels, 5.7.2016, C(2016) 4400 final, available at (including link to the Annex): https://ec.europa.eu/digital-single-market/en/news/commission-decision-establish-contractual-public-private-partnership-cybersecurity-cppp
Joint Communication on countering hybrid threats	JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats a European Union response, JOIN/2016/018 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018
General Data Protection Regulation (GDPR)	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1-88, available at: http://data.europa.eu/eli/reg/2016/679/oj
LEA DP directive	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89-131, available at: http://data.europa.eu/eli/dir/2016/680/oj
PNR directive	Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132-149, available at: ELI: http://data.europa.eu/eli/dir/2016/681/oj
2015	
Digital Single Market Strategy for Europe (DSM)	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe, COM/2015/0192 final, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX:52015DC0192

Reference	Policy/legislation reference. Complete title and link
Payment Services directive	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), OJ L 337, 23.12.2015, p. 35-127, available at: http://data.europa.eu/eli/dir/2015/2366/oj
The European Agenda on Security	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, The European Agenda on Security, COM/2015/0185 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2015:0185:FIN
2014	
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 and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73-114, available at: http://data.europa.eu/eli/reg/2014/910/oj
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
2013	
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
Cybersecurity Strategy of the EU	JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667
ENISA Regulation	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, OJ L 165, 18.6.2013, p. 41-58, available at: http://data.europa.eu/eli/reg/2013/526/oj
Directive on attacks against information systems	Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14.8.2013, p. 8-14, available at: http://data.europa.eu/eli/dir/2013/40/oj
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, OJ L 328, 7.12.2013, p. 42-68, http://data.europa.eu/eli/reg_del/2013/1271/oj
COM Regulation 611/2013 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, OJ L 173, 26.6.2013, p. 2-8, available at: http://data.europa.eu/eli/reg/2013/611/oj
2012	
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
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
EP resolution on CIIP	European Parliament resolution of 12 June 2012 on critical information infrastructure protection — achievements and next steps: towards global cyber-security (2011/2284(INI)), available at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167
2011	
Council conclusions on CIIP	Council conclusions on Critical Information Infrastructure Protection 'Achievements and next steps:
COM Communication on CIIP	towards global cyber-security' (CIIP), 2011, Adoption of Council conclusions, available at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010299%202011%20INIT
(old — focus up to 2013)	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection, 'Achievements and next steps: towards global cyber-security', Brussels, 31.3.2011, COM(2011) 163 final available at: http://ec.europa.eu/transparency/regdoc/rep/1/2011/EN/1-2011-163-EN-F1-1.Pdf
EU LISA regulation	Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 286, 1.11.2011, p. 1-17, Version consolidated, after amendments, available here: http://data.europa.eu/eli/reg/2011/1077/2015-07-20
Single Market Act	Single Market Act — Twelve levers to boost growth and strengthen confidence 'Working Together To Create New Growth', COM(2011) 206 final
Telecom Ministerial Conference on CIIP	Telecom Ministerial Conference on CIIP organised by the Presidency in Balatonfüred, Hungary, 14-15 April 2011
2010	
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
Digital Agenda	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe, COM/2010/0245 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010DC0245&from=EN
2009	
COM communication on IoT	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions — Internet of Things: an action plan for Europe, COM/2009/0278 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2009:0278:FIN
Council Resolution of December 2009 on NIS	Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security, OJ C 321, 29.12.2009, p. 1-4, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex %3A32009G1229(01)
2002	
Framework Directive 2002/21/EC as amended	Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.4.2002, p. 33-50, consolidated version, after amendments, available at: http://data.europa.eu/eli/dir/2002/21/2009-12-19
ePrivacy Directive 2002/58/EC as amended	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002 P. 0037-0047, Consolidated version, after amendments, available at: http://data.europa.eu/eli/dir/2002/58/2009-12-19

MISSION STATEMENT

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 and 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 policymakers 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. By concentrating on implementation measures, the Agency will complement the significant work that has gone into defining the legal framework.

BRIDGING PUBLIC AND 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.

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 weaponisation 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, policymakers 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 'Consumerisation of cyber-crime', that is, making malicious tools available to everybody.

Threat intelligence collection, management and sharing should become an inherent part of the national cybersecurity capabilities.

II.

SECTION II.

MULTI-ANNUAL PROGRAMMING 2017 – 2019

2.1 MULTI-ANNUAL OBJECTIVES

The multiannual objectives of the Agencies are derived from the ENISA regulation and are part of ENISA strategy. The objectives of the Agency are structured around five 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.

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 Management Board 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.

1 Annual and multiannual work programmes (Article 5 §2 of ENISA regulation).

2 In order to achieve the 5 year strategic objectives laid out in this document, the multiannual work programme will provide prioritised 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.

- **#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.
- **#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.

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 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, standardisation, IT Security certification and other relevant industrial practices.

This activity has four 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 and 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 directorate-generals 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 established under the NIS directive, 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 three 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.

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

3 This objective should not be confused with ENISA's support provided to single Member States requesting assistance pursuant to Article 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.

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

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 organisations as well as in the general public.

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

Objective 3.1. Assist Member States' capacity building

- 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 organisation 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, ENISA will enhance cooperation at EU level among Member States, Union institutions and related NIS stakeholders, including the 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 organisation 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 two 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 5 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 Core Operations 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.

Objective 5.4. Compliance and support

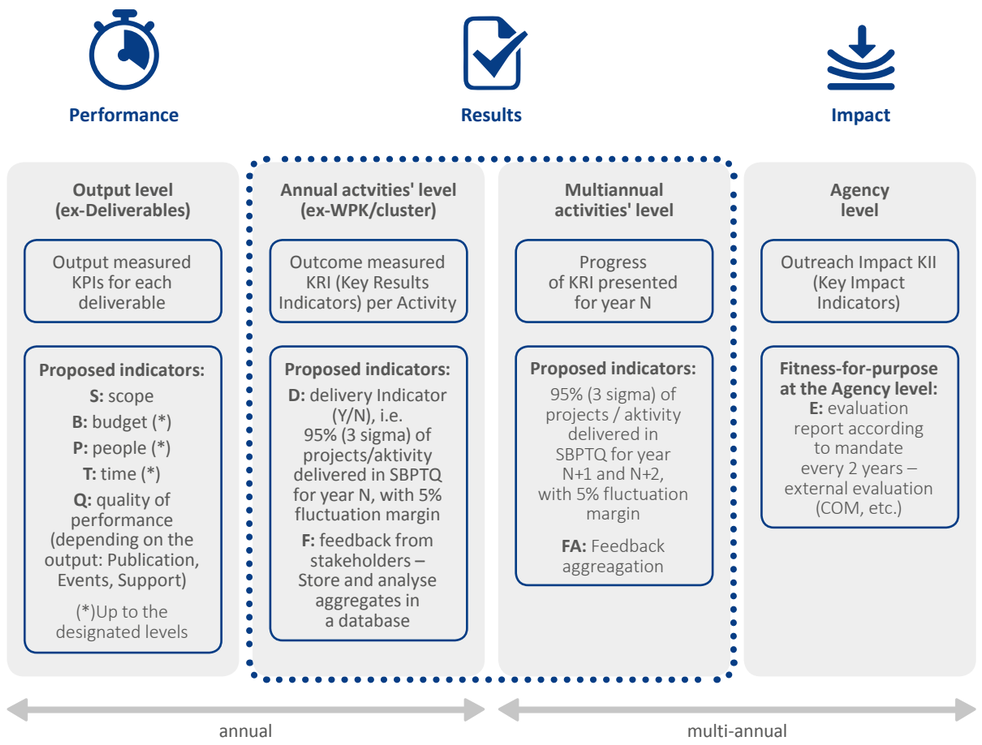
- The Agency will seek to comply with legal and financial requirements and provide Human resources, Budget, IT infrastructure, etc. in line with the operational objectives.

2.3 MONITORING THE PROGRESS AND THE ACHIEVEMENTS OF THE AGENCY. SUMMARISING 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 programme, 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:

- adherence to the scope of the deliverable or project;
- budget (or financial resources) available to the output or project, remaining within prescribed levels with a ± 5 % margin;
- people (or human resources) available to the output or project, remaining within prescribed levels with a ± 5 % margin;
- time available to carry out the output or project remaining within prescribed levels with a ± 5 % margin;
- quality of performance depending on the type of output, according to the classification of output in the work programme (being, publication, event, support).

Results that are a concern at the annual and at multi-annual activities' level. The indicators used are as follows:

- delivery indicator aiming at delivery of at least 95 % against work programme 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;
- 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.

The key indicators broken down at the output level, the activities level and the agency level, are presented hereunder. (Table 1)

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 programme.

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 utilises 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.

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						
Quality (e.g. citations, downloads, MS participation etc.)	Q	Integer: quan-titative target						

* Feedback via e.g. survey associated with deliverables on website
** Aggregations of deliverables or categories thereof

Table 1.

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 website 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.

It is envisaged that the deliverables part of the website will be leveraged to channel targeted feedback against each deliverable downloaded.

#	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

Table 2.

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	**Scope in start remains identical to scope in the end**	**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 re-sponses 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

Table 3.

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 A5 is presented in the chart hereunder. The budget and resources for each activity are presented in section 3.7.2. in the summary table. The budget and posts distribution is based on the Activity Based Budgeting (ABB) methodology of the Agency detailed in 3.6.2. of this document.

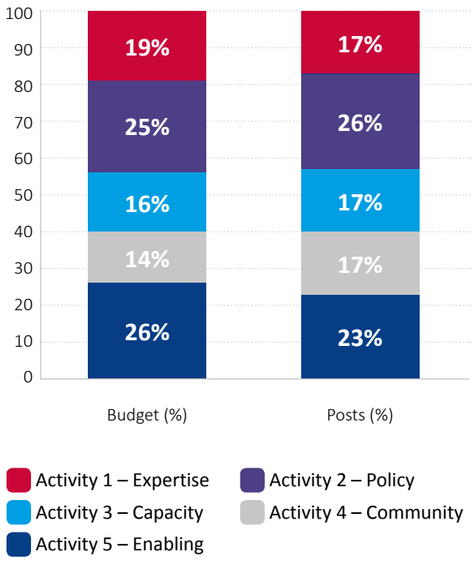
Following the publication of the NIS directive (NISD), the Agency is re-allocating budget and resources to the new tasks/activities provisioned for the Agency in the directive. Another area which will probably require more budget/resources is the Cybersecurity Public Private partnership (cPPP). However, the impact on the ENISA work programme has not yet been identified. This will be updated in future versions.

In addition, this version of the work programme takes account of the prioritisation exercise carried out during the March meeting of the Ad Hoc group, although it is recognised that this prioritisation will need to be fine-tuned by the full Management Board.

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 more resources than capacity building.

The budget and resources allocations within the summary table and Annexes are in line with the COM Multiannual Financial Framework (MAFF) 2014-2020.

Budget and posts distribution (ABB)



III.

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 for 2017 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.

For each Output, the following are included in this document:

- A description of the specific actions and outcome which are expected to contribute to the achievement of the objective,
- The type of output (in summary table at the end of each Activity):
  - **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 (in summary table at the end of each Activity).
- 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.

This objective will look at common requirements as well as focusing on sector specific areas of NIS directive such as energy, health, transport, etc. as well as on baseline security recommendations for IoT in the context of Critical Information Infrastructures.

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

3.1.1.1 Output O.1.1.1 — Baseline Security Recommendations for the OES Sectors

ENISA will work closely with representatives from the Member States to identify a set of baseline security requirements that are applicable to all Operators of Essential Services (OES) as defined in the NIS directive.

The Agency will identify and analyse existing security practices (e.g. BSI's requirements) and standards (e.g. ISO 27001, NIST's CIIP Framework [6]) and compare them so as to identify the baseline security recommendations.

In deriving such a set of 'common' baseline requirements, no account will be taken of sector-specific needs as these are likely to introduce conflicting priorities (for example, the relative importance of availability and integrity is likely to be different in the energy sector to the banking sector, where different risks prevail).

However, the Agency will take note of such specific requirements as and when they are identified during the analysis phase and will then map them to the needs and requirements of Operators of Essential Services. This information can then be used a starting point for creating sector-specific baselines at a later date.

The Agency will also compare and validate the results with other relevant approaches in the area of Operators of Essential Services (e.g. EE-ISAC and ENTSO-E cyber security subgroup) and interact with all important stakeholders from public as well as 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.

3.1.1.2 Output O.1.1.2 — 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 (the NIS directive, the Internet of Things — An action plan for Europe, The Alliance for the Internet of Things (AIOTI) [7], the 5G Infrastructure Pubic Private Partnership (5G PPP) [8]).

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 Directorate-General for Communications Networks, Content and Technology, 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).

6 https://www.nist.gov/cyberframework

7 The Alliance for Internet of Things Innovation (AIOTI), more info available at: https://ec.europa.eu/digital-single-market/en/alliance-internet-things-innovation-aioti

8 The 5G Infrastructure Pubic Private Partnership (5G PPP), more info available at: https://5g-ppp.eu/

3.1.2 Objective 1.2. NIS Threat 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

The ENISA Threat Landscape (ETL) 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 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.

The ENISA Threat Landscape (ETL) report enjoys major attention both within Member States, Commission, as well as expert and lay communities.

In carrying out this work, 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.

In 2017, the ENISA Threat Landscape will be accompanied by an End-User application (web) that will provide available information online. In this manner, ETL users will be in the position to access ENISA threat information on a permanent basis. This platform may be used for integration of additional relevant information.

In 2017, ENISA will continue the cooperation with CERT-EU in the area of Threat Landscaping. This effort will be carried out by means of information exchanges, use of CERT-EU services and organisation of common meetings/events.

Annual Incident Analysis Reports

ENISA is mandated by 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 assesses root causes. Furthermore, the reports provide a consistent and factual aggregate analysis of incidents for policymakers, the public and the industry, describing overall frequency and impact of ICT security incidents across the EU.

3.1.2.2 Output O.1.2.2 — Annual Incident Analysis Report for the Telecom sector (article 13a)

This report provides an aggregated analysis of the major cyber security and network integrity incidents affecting the 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.

3.1.2.3 Output O.1.2.3 — 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.

3.1.3 Objective 1.3. Research and 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. The 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 an assessment of the situation of European standardisation in the area of ICT security, taking into account the new requirements and priorities associated with the NIS directive (and potentially the Commission's communication on cPPP). 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.

In carrying out this work, ENISA will consult with industry and standards organisations (e.g. ETSI, CEN, CENELEC) as appropriate.

3.1.3.2 Output O.1.3.2 — Priorities for EU Research and Development

This study will provide an analysis of areas covered by the NIS directive, the General Data Protection Regulation and the COM decision on cPPP and will aim to show where R & D activities funded in the context of H2020, CEF (Connecting Europe Facility), TRANSITS and GEANT would achieve the greatest impact.

ENISA will work closely with ECSO (European Cyber Security Organisation) and cPPP on cybersecurity in order to align the work being carried with the ENISA Work Programme. In addition, the agency will offer support to NAPARC (National Public Authority Representatives Committee) by offering a secretariat function.

ENISA will look into adapting the current best practices and guidelines for protecting EU systems and networks according to the evolving threats. As well as building specific used cases that can be adopted by the IT Security community.

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.

The type of outcome and the performance indicators will be defined during the execution year of the work programme together with the requester.

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.

3.1.4.1 Output O.1.4.1 — Response to Requests under Expertise Activity

3.1.5 Type of Outputs and performance indicators for each Outputs of Activity 1 Expertise

Summary of Outputs in Activity 1 — Expertise. Anticipate and support Europe in facing emerging network and information security challenges		
Outputs	**Type of output (P=publication, E=Event, S=Support)**	**Performance indicator**
Objective 1.1. Improving the expertise related to Critical Information Infrastructures		
Output O.1.1.1 — Baseline Security Requirements for the OES sectors	**P:** Baseline Security Requirements for OES **P:** Mapping of OES Security Requirements to Specific Sectors, Q4 **E:** two workshops with stakeholders from OES sectors, Q2-Q4	Engage 20 MS in the development of baseline security requirements for OES Engage 15 private sector stakeholders in the development of baseline security requirements for OES More than 10 MS and 15 OES participate in the workshops
Output O.1.1.2 — Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures	**P:** Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, Q4	Engage five leading IoT developers and five leading CII operators from five EU MS in the preparation of the study
Objective 1.2. NIS Threats Landscape and Analysis		
Output O.1.2.1 — Annual ENISA Threat Landscape	**P:** Report and online information offering; report in Q4, information offering during the year	Involvement of at least five representatives from different bodies/MS in the stakeholder group supporting the preparation of annual ETL
Output O.1.2.2 — Annual Incident Analysis Report for the Telecom sector (article 13a)	**P:** Annual Incident Analysis Report for the Telecom sector, Q4	More than 20 NRAs/EU MS contribute in preparation of the report
Output O.1.2.3 — Annual Incident Analysis Report for Trust Service Providers (article 19)	**P:** Annual Incident Analysis Report for the Trust Service Providers, Q4	More than 10 SBs/EU MS contribute in preparation of the report
Objective 1.2. NIS Threats Landscape and Analysis		
Output O.1.3.1 — Guidelines for the European standardisation in the field of ICT security	**P:** Guidelines for the European standardisation in the field of ICT, Q4	Participation in drafting and review of the guidelines of at least five representatives of European Standard Developing Organizations (SDOs) and relevant services of the European Commission
Output O.1.3.2 — Priorities for EU Research and Development in the context of H2020	**P:** Study on priorities for EU research and development in the context of H2020, Q4	Involving at least five representatives from different stakeholders — research, industry, governmental
Objective 1.2. NIS Threats Landscape and Analysis		
Output O.1.4.1 — Response to Requests under Expertise Activity	**S:** Answers to requests	

Table 4.

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 policymaking having an EU dimension.

In the policy development area the Agency will cooperate 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 Certification and DSM.

ENISA, using its knowledge and expertise in this area, will liaise with the Commission and all relevant EU Member States to identify and analyse current eHealth cyber security challenges. Through discussion with the competent experts from public and private sector the Agency will identify the key elements of comprehensive national approach to eHealth cyber security in order to meet the requirements of Article 7 of the NIS directive, whilst still allowing the sector to make appropriate use of new technologies. ENISA will validate its findings via a workshop with all competent authorities.

3.2.1.1 Output O.2.1.1 — Support the policy discussions in the area of IT security certification

Taking due account of recent legislative and policy developments, such as the adoption of the NIS directive and the publication of the Commission position on the cPPP, the Agency will continue to support the Commission and the Member States in identifying a certification framework for 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.

3.2.1.2 Output O.2.1.2 — 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.

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

The Agency, building upon its previous work on DSM (WP 2016) and on Commission's studies on the matter, will identify two market segments where the EU could potentially develop a significant cybersecurity commercial approach. This will be supported by an analysis of why the EU is well positioned to develop these areas and recommendations for further development.

To achieve this the Agency will liaise with the Commission, EU MS, and relevant public and private sector organisations in order to collect 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.

3.2.2 Objective 2.2. Supporting EU policy implementation

Objective 2.2 covering policy implementation is structured around four 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 cooperate 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 cooperation 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). 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 (1)[9]. eCom providers and internet infrastructure providers will be consulted on lessons learnt from incidents, sharing of experiences and good practices and on policy implementation matters.

ENISA will 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).

Following the relevant ENISA's work in 2016, the Agency will continue supporting the European Commission (Directorate-General for Communications Networks, Content and Technology) in the revision and implementation of the Directive 2002/58/EC (ePrivacy directive). In particular, ENISA will act as technical advisor of the EC regarding security of personal data and confidentiality of communications in the electronic communications sector. To this end, ENISA will produce where necessary relevant working papers and technical reports, as well as support the EC in relevant ad hoc initiatives, upon request.

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 assist MS and industry in developing guidelines on implementing mandatory incident reporting mechanisms. This activity will be driven by the context of the NIS directive.

The Agency will assist 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).

9 Universal Service Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services as amended by Directive 2009/136/EC (Citizen rights' Directive) and Regulation (EU) 2015/2120, in consolidated version available at: ELI: http://data.europa.eu/eli/dir/2002/22/2016-04-30

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.

3.2.2.3 Output O.2.2.3 — Recommendations supporting implementation of the eIDAS Regulation

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.

Furthermore, ENISA will 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 according to eIDAS regulation. These recommendations will complement the existing knowledge base that ENISA created for the trust service providers.

3.2.2.4 Output O.2.2.4 — 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 the 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, anonymisation vs pseudonymisation, 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.

3.2.2.5 Output O.2.2.5 — 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. In 2014, the work focused on a definition of the terms 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). In 2016, the Agency developed a community tool that allows to evaluate new techniques and keep lists of best available techniques up to date. In 2017, this tool will undergo a field test. This field test will be used to test the techniques practically and to extend their functionalities. 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 policymaking.

3.2.2.6 Output O.2.2.6 — 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 ENISA's contribution to the cooperation group and especially the development of good practices for identification of OES (criteria). Also, in this output ENISA will also further develop its cooperation with operators of essential services in order to better understand their sectorial needs and requirements.

More specifically ENISA will contribute to the establishment of the Cooperation Group and provide suggestions on its functioning. The Agency, upon request, can analyse specific issues identified by the cooperation 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, CSIRTs, baseline security requirements in numerous sectors (energy, transport, finance etc.), standardisation, ICT certification and others to contribute to the work of the cooperation group. That would be by reusing or customising existing results or by developing new, specific results meeting the needs and requirements of the Cooperation group.

Also, ENISA will take stock of Member States current efforts to define criteria for the identification of OES. Through this stock taking and analysis ENISA will identify common approaches, schemes and good practices. The Agency will then validate them with relevant public and private sector to makes sure that they meet the needs and requirements of both MS and private sector. Such good practices can be used, as much as possible, by MS when defining, at national scheme, their criteria for the identification of OES.

Finally ENISA, using its knowledge and expertise in the area of OES, will liaise with the Commission and all relevant EU Member States to identify and analyse current cyber security challenges, and then develop good practices at sectorial level that could enhance the security of OES. ENISA will focus its efforts mostly on energy, health, finance and transportation. The Agency will validate its findings via a workshop with all competent authorities.

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.

ENISA will support the Commission, Member States and the private sector in the implementation of the NIS directive.

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.

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.

3.2.4 Type of Outputs and performance indicators for each Outputs of Activity 2 Policy

Summary of Outputs in Activity 2 — Policy. Promote network and information security as an EU policy priority		
Outputs	**Type of output (P=publication, E=Event, S=Support)**	**Performance indicator**
Objective 2.1. Supporting EU policy development.		
Output O.2.1.1 — Support the policy discussions in the area of IT security certification	**P:** Characteristics of the common European ICT products security certification framework, Q4 **E:** four workshops with stakeholders, Q2–Q4	More than 10 private companies and 10 EU MS representatives contribute to/participate in the activity
Output O.2.1.2 — Restricted. Towards a Digital Single Market for high quality NIS products and services	**P:** Recommendations on DSM up take, Q4 **E:** one workshop with stakeholders, Q2-Q4	More than 10 leading private companies from two sectors take part in the study
Objective 2.2. Supporting EU policy implementation		
Output O.2.2.1 — Contribute to EU policy in the area of electronic communications sector	**E:** two workshops with relevant stakeholders, Q2-Q4	Engage 20 sector providers and 20 national bodies in the activity
Output O.2.2.2 — Develop guidelines for the implementation of mandatory incident reporting	**P:** Guidelines for the Implementation of Mandatory Incident Reporting in the context of the NIS directive, Q4 **E:** two workshops with relevant stakeholders, Q2–Q4	More than 15 private stakeholders and more than 15 public stakeholders contribute to the study
Output O.2.2.3 — Recommendations for technical implementations of the eIDAS Regulation	**P:** Recommendations to support the technical implementation of the eIDAS Regulation, Q4 **P:** Security recommendations for trust service providers and users of trust services, Q4	Engaging at least five representatives from different bodies/MS in the preparation of the recommendations Review and acceptance by at least 10 stakeholders (trust service providers, conformity assessment bodies, and supervisory authorities) from at least five MS
Output O.2.2.4 — Recommendations for technical implementations of the General Data Protection Regulation	P: Recommendations for technical implementations of the general data protection regulation, Q4	At least five representatives from different bodies/MS participate in the preparation of the recommendations
Output O.2.2.5 — Privacy enhancing technologies	**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	At least five experts in the area to contribute to the report The event should have at least 80 participants from the relevant communities
Output O.2.2.6 — Supporting the Implementation of the NIS directive	**P:** Recommendations and Good Practices on the criteria for choosing OESs **S:** Contribute to the establishment of the Cooperation Group **E:** three workshops related to the tasks of the NISD **S:** Contribute to the activities of MS and private sector in the area of OES	Engaging at least 15 MS and 15 private stakeholders in the ENISA contributions to the implementation of the NIS directive ENISA provides contributions as requested 10 OES participate in the workshops 10 MS participate in the activity
Objective 2.3. Response to Article 14 Requests under Policy		
Output O.2.3.1. — Response to Requests under Policy Activity	**S:** Answers to requests	

Table 5.

3.3 ACTIVITY 3 — CAPACITY. SUPPORT EUROPE MAINTAINING STATE-OF-THE-ART NETWORK AND INFORMATION SECURITY CAPACITIES

ENISA will provide assistance to MS and EU institutions and bodies, as well as the private sector by supporting enhancement of NIS capacity building through the EU. In practice, this will involve promoting capacity building activities and supporting the implementation of key legislative and policy developments such as the NIS directive and the eIDAS Regulation. In particular, the Agency will work together with all relevant stakeholders to ensure that approaches undertaken are 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 programme. In 2017, ENISA will build upon its work in the 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 — Support national and governmental CSIRTs capabilities

In 2017, ENISA will concentrate its efforts on assisting CSIRTs by leveraging its role as secretariat of the CSIRT network as defined in the NIS directive. In close cooperation with this network, 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.

3.3.1.2 Output O.3.1.2 — Update and provide technical trainings for MS and EU bodies

In 2017, most of the 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 the training material, which is in high demand and provide a 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 with 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.

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.

3.3.1.3 Output O.3.1.3 — 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). A priority in this area will be to ensure that NCSS adequately reflect the priorities and requirements of the NIS directive.

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.

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

ENISA provides guidance on important NIS events and developments through Info Notes. Relevant NIS events might cover incidents, significant developments and announcements in the field of cyber security. Info notes are explanatory notes, regarding — for example — events that reach a certain level of public and media attention.

ENISA will provide balanced and neutral information regarding such events, covering issues, points of action, mitigation measures, summaries, related practices, etc.

ENISA's intention is to continue providing Info Notes as a reliable and continuous service to its stakeholders in a timely manner.

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 method. In addition, to the ENISA website, in 2017 Info Notes will be disseminated via the ENISA ETL platform.

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.

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.

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.

3.3.3.2 Output O.3.3.2 — 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 public and private approaches to cyber insurance and identify the lessons learned and good practices in use from the deployment of cyber insurances (e.g. liability issues, proper policy calculation, asset cost, cost of breaches) mostly in the area of pre-policy stage. 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 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).

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 the 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.

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.

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.

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.

3.3.6 Type of Outputs and performance indicators for each Outputs of Activity 3 Capacity

Summary of Outputs in Activity 3 — Capacity. Support Europe maintaining state-of-the-art network and information security capacities		
Outputs	**Type of output (P=publication, E=Event, S=Support)**	**Performance indicator**
Objective 3.1. Assist Member States' capacity building		
Output O.3.1.1 — Support national and governmental CSIRTs capabilities	**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) **S:** Q1-Q4, continue activities and involvement in CSIRT and other operational communities structures (e.g. FIRST, TF-CSIRT)	Updated material of CSIRT Baseline capability report based on input from at least five MS Two updates (Q2, Q4) for the overview of existing CSIRTs and their constituencies in Europe for different type of stakeholders (e.g. business sector) During 2017, support provided at least for two MSs to enhance their 'national and governmental CSIRT baseline capabilities' and for two EU institutions, bodies or agencies in development or enhancement of their incident response capabilities At least 15 MSs participating in the technical CSIRT workshop
Output O.3.1.2 — Update and provide technical trainings for MS and EU bodies	**P:** Q4: Stock taking of Existing Training Schemes in NISD sectors **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) **S:** Trainings on CEP and CCM, Q4	At least 15 MS covered during the survey for the stock taking in NISD training schemes Continued CSIRT services training will be provided to a minimum of 20 participants of different organisations in five MS At least one training material updated to support improved operational practices of CSIRTs in at least 15 MS At least one new (or updated) good practice guide on particular CSIRT service At least 70 % of participants in trainings (online or onsite) evaluate the experience positive or very positive
Output O.3.1.3 — Support EU MS in the development and assessment of NCSS	**P:** Updated — EU's map on NCSS **E:** Workshops with EU MS on NCSS development, Q2-Q4	Engage at least 15 EU MS in this activity/ workshop
Objective 3.2. Support EU institutions' capacity building		
Output O.3.2.1 — Restricted and public Info notes on NIS	**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	In 2017, at least one additional key stakeholder group (e.g. ENISA MB members or PSG) receives restricted Info Notes on regular basis At least six Public Info Notes are published on ENISA website
Output O.3.2.2 — Restricted. Upon request, support the assessment of existing policies/procedures/practices on NIS within EU institutions	**P:** Position Paper on a given topic, Q4 **E:** one workshop with relevant stakeholders, Q2-Q4	At least three EU institutions and five MS take part in the activity
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	**P:** Study on cybersecurity culture, Q4	Involving at least five representatives from different bodies/MS in preparation of this study
Output O.3.3.2 –Recommendations on Cyber Insurance	**P:** Recommendations on Cyber Insurances, Q4	At least seven insurance companies and 10 companies from at least five EU MS take part in the preparation of the recommendations
Objective 3.4. Assist in improving general awareness		
Output O.3.4.1 — Cyber Security Challenges	**S:** Q1-Q4: European Cyber Security Challenge support **E:** Q2-Q3: 'Award workshop' for winners of the European Cyber Security Challenge 2016 (ENISA promotes best of the best)	At least two additional EU MS organise national cyber security challenges in 2017 and participate in the European Cyber Security Challenge
Output O.3.4.2 — European Cyber Security Month deployment	**S:** Q1-Q4: ECSM support **P:** Q4, an evaluation report	All 28 EU MSs and other partners and representatives from different bodies/ MS participate in/support ECSM 2017
Objective 3.5. Response to Article 14 Requests under Capacity Activity		
Output O.3.5.1. — Response to Requests under Capacity Activity	S: Answers to requests	

Table 6.

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 and Report on Exercise after Action Activities from 2014-2016

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

The pan European exercises organised by ENISA are producing a number of significant 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 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 evaluation report according to the public affairs strategy of the exercise.

3.4.1.2 Output O.4.1.2 — 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 programme 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 programme 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.

3.4.1.3 Output O.4.1.3 — Support activities for Cyber Exercise Planning and Cyber Crisis Management

Cyber Exercise Platform (CEP) Development and Content Management

Since 2014, ENISA started the development of the Cyber Exercise Platform (CEP). CEP hosts a 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.

EU-level Cyber Crisis and Incident Management Procedures and Connecting Europe Facility (CEF) Cybersecurity Digital Service Infrastructure (DSI)

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.

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.

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 — 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.

3.4.2.2 Output O.4.2.2 — EU CSIRT network secretariat and support for EU CSIRT network community building

ENISA will support the Commission and Member States in the implementation of the NIS directive, in particular in the area of CSIRTs. 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 particular, the Agency will be proactive in stimulating discussions within the network and will aim to provide content to support discussions on policy and technical initiatives.

In addition, ENISA will take an active role to support the 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 programme to support CSIRTs in the area of community building and information sharing (Connecting Europe Facilities (CEF) programme for CSIRTs).

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.

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.

3.4.4 Type of Outputs and performance indicators for each Outputs of Activity 4 Community

Summary of Outputs in Activity 4 — Community. Foster the emerging European network and information security community		
Outputs	**Type of output (P=publication, E=Event, S=Support)**	**Performance indicator**
Objective 3.1. Assist Member States' capacity building		
Output O.4.1.1 — Evaluation of Cyber Europe 2016. Report on Exercise After Action Activities from 2014-2016	**P:** Evaluation report for CE2016 (public and restricted versions), Q3 **P:** Report on after action activities (restricted), Q4	At least 80 % of the countries actively involved in the exercise contribute to the evaluation and quality assurance processes of the report At least 80 % of the countries actively involved in exercises agree with the conclusions of the report
Output O.4.1.2 — Planning of Cyber Europe 2018	**P:** Exercise plan (restricted), Q4	At least 24 EU/EFTA Member States and countries confirm their support for Cyber Europe 2018
Output O.4.1.3 — Support activities for Cyber Exercise Planning and Cyber Crisis Management	**S:** Support for CEP, Q4 **S:** Support for the Cyber SOPs editorial team of the cooperation of cyber security network of CSIRTs, Q4 **S:** Q1-Q4: Support CEF (including ENISA roadmap for implementation and deployment plan) and contribution to the activities of the Cybersecurity DSI Governance Board (Q4, 2017)	At least 70 % of CEP users evaluate it positively At least 90 % of the participating MS agree to the developed operational procedures Over 80 % of the countries in the Governance Board approve the implementation roadmap and deployment plan
Objective 4.2. CSIRT and other NIS community building		
Output O.4.2.1 — Support the fight against cybercrime and collaboration between CSIRTs and LEA	**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 cooperations **E:** Q3, continue annual ENISA/EC3 workshop for national and governmental CSIRTs and their LEA counterparts	At least five MS CSIRT representatives and five MS LEA representatives participate in the preparation of the report At least five MS CSIRT representatives participate in the preparation of the guidelines At least 15 MS participate at ENISA/EC3 annual workshop
Output O.4.2.2 — EU CSIRT network secretariat and support for EU CSIRT network community building	**S:** Rules of procedures of the CSIRT network (article 12 (5)) **S:** Q1-Q4: Provide EU CSIRT network secretariat (e.g. logistics, organisation of the meeting, agenda management, meeting minutes), facilitate CSIRTs regular participation in the EU CSIRT network events **E:** Up to three workshops of the CSIRT network **S:** Q1-Q4, EU CSIRT network support **P:** Q1-Q4, Update ENISA CSIRT Inventory/ Portal service for EU national and governmental CSIRTs (NIS directive article 12 (3) (a) (build upon ENISA online CSIRT Inventory tool)	Engaging all 28 MS designated CSIRTs in the development of the rules of procedure and in general in the implementation of the NIS directive Positive feedback regarding ENISA support from the majority of the participants in activities Positive feedback from participants in the events/workshops organised by ENISA Work of ENISA successfully reflected by existing CSIRT communities (FIRST, TF-CSIRT, EU CSIRT network) and CSIRT network At least five MS CSIRT representatives participate in the preparation of the updates of the inventory of services design to improved cooperation and information sharing among CSIRTs in Europe
Objective 4.2. CSIRT and other NIS community building		
Output O.4.3.1. — Response to Requests under Community Building Activity	**S:** Answers to requests	

Table 7.

3.5 ACTIVITY 5 — ENABLING. REINFORCE ENISA'S IMPACT

Activity 5 covers four main objectives.

- Management
- Engagement with stakeholders
- International activities
- Compliance and support

3.5.1 Objective 5.1. Management

The Executive Director is responsible for the overall management of the Agency. The Executive Director has a personal assistant.

To support the Executive Director, an Executive Directors Office (EDO) has been set up. The tasks covered by EDO include: Policy advice, Legal advice, Management Board Secretariat, Coordination of the Work Programme and Press Communications.

The policy and legal advice shall extend to all aspects of the work of the agency and includes both advice in relation to the operational and administration Department of the Agency.

The EDO also supports the administration of the Management Board meetings and the administrative correspondence that takes place between meetings.

The EDO manages and supports the relations with the press in order to promote the outreach of the Agency.

In 2017, EDO will continue to support the Management Board (MB) and the Executive Board in their functions by providing secretariat assistance.

In relation to the MB, one ordinary meeting will be organised during 2017 and informal meetings will be held as necessary. The existing electronic MB newsletter will be changed to an ENISA newsletter in 2017. The MB Portal will also be supported. For the Executive Board, a formal meeting will be organised once per quarter and informal meetings when necessary.

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
- Permanent Stakeholders Group
- Stakeholders Communication and Dissemination Activities
- Outreach and Image building activities

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:

- a 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.

Permanent Stakeholders Group (PSG)

In 2017, ENISA will continue and reinforce the contribution of the Permanent Stakeholders Group (PSG) to the ENISA Work Programme.

The PSG is composed of 'nominated members' and members appointed 'ad personam'. The total number of members is 23 and they come from all over Europe. These members constitute a multidisciplinary group deriving from industry, academia, and consumer organisations and are selected upon the basis of their own specific expertise and personal merits. Three (3) 'nominated members' represent national regulatory authorities, data protection and law enforcement authorities.

The PSG is established by the ENISA regulation (EU) No 526/2013. The Management Board, acting on

a proposal by the Executive Director, sets up a PSG for a term of office of 2.5 years.

The Role of the PSG group is to advise the Executive Director on the development of the Agency's work programme, and on ensuring the communication with the relevant stakeholders on all related issues.

Stakeholders Communication and Dissemination Activities

In 2017, ENISA will seek to improve its focus on key activities and engage the higher possible number of stakeholders. This includes the various groups of stakeholders that count with institutional, academia, industry, citizens, etc.

The Agency will continue developing various tools and channels including the website and with strong emphases in social media.

Dissemination activities are the responsibility of the Stakeholders Communication team that will seek the appropriate level of outreach activities to take ENISA's work to all interested and to provide added value to Europe.

Outreach and Image building activities

ENISA´s image of quality and trust is paramount for all stakeholders. It's indubitable the importance that the European Citizens in all areas of our society to trust in ENISA's work. The cyber security challenges are increasing in the world and Europe is not an exception. With this objective ENISA's image needs to be continuously reinforced. The outreach of the Agency work is essential to create the NIS culture across the several actors in Europe. ENISA is consistent of this fact and will work with all interested to reach the Citizens that require information about the work that is developed by the Agency.

Several activities are planned in several Member States that will engender the cyber security awareness across Europe, fulfilling ENISA's mandate, mission and strategy until 2020.

3.5.3 Objective 5.3. International relations

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

3.5.4 Objective 5.4. Compliance and support

The Stakeholder Relations and Administration Department (SRAD) strives to operate a cost-efficient, customer-oriented service department.

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

The SRAD 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.

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

The aim of the SRAD is to provide this assurance and at the same time provide the best level of efficiency and use of the resources that are made available for the Agency. Coordination with the European Commission Internal Audit Service, European Court of Auditors, European Ombudsman, European Commission European Anti-Fraud Office, etc. is one main task of this area. All internal policies related to transparency, anti-fraud policy, whistle-blowers protection, declarations of interests, etc. are addressed within this activity.

Quality Management System and Internal Control Coordination

ENISA is developing the Quality Management System (hereinafter, QMS) of the Agency to support its regulatory and strategic goals by means of a quality management approach. ENISA will follow the ISO 9001:2015 standards as they are designed to help organisations ensure that they meet the needs of customers and other stakeholders while meeting statutory and regulatory requirements. The methodology is based on the Plan-Do-Check-Act (PDCA) cycle that has been duly documented in a dedicated SOP and applied accordingly.

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.

3.5.4.1 IT

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 two 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. Due to the size of the agency and effective resources management, the IT tasks will be outsourced as far as possible to concentrate the available resources in the operational area of the Agency.

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. (Table 8)

Task	Objective	Level of completion 2016	Level of completion 2017	Level of completion 2019
Consolidate systems and applications on a maximum of two 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 %

Table 8.

3.5.4.2 Finance, Accounting and Procurement

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. (Table 9)

Task	Objective	Level of completion 2016	Level of completion 2017	Level of completion 2018
Deployment of new financial information systems	Efficiency, better reporting, information quickly provided	50 %	80 %	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	87 %	89 %	90 %
Payments against appropriations carried over from year n-1 (C8 funds)	Efficiency and Sound Financial Management	95 %	95 %	95 %
Payments made within Financial Regulation timeframe	Efficiency and Sound Financial Management	87 %	90 %	98 %

Table 9.

3.5.4.3 Human Resources

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.

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. (Table 10)

Task	Objective	Level of completion 2016	Level of completion 2017	Level of completion 2018
Posts on the Agency establishment plan filled	Minimum 95 % of the recruitment target reached	90 %	95 %	97 %
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 %	< 16 %	< 12 %	< 10 %

Table 10.

3.5.4.4 Internal communication, legal affairs, data protection and information security coordination

3.5.4.4.1 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 programme. It is proposed that the implementation of the internal communications strategy will be completed and revised in 2017. 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. (Table 11)

Task	Objective	Level of completion 2016	Level of completion 2017	Level of completion 2018
Increase the level of awareness of ENISA's work and recent developments related to the Agency	Develop Internal Communication Strategy	50 %	80 %	90 %
Increase the staff motivation	Bring all staff members and offices closer for a better and fruitful cooperation	60 %	80 %	90 %

Table 11.

3.5.4.4.2 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.

3.5.4.4.3 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; cooperate and consult with EPDS whenever needed.

3.5.4.4.4 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 SUMMARY TABLES

3.6.1 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 OES Sectors
Output O.1.1.2 — Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures
Objective 1.2. NIS Threat Landscape and Analysis
Output O.1.2.1 — Annual ENISA Threat Landscape
Output O.1.2.2 — Annual Incident Analysis Report for the Telecom sector (article 13a)
Output O.1.2.3 — Annual Incident Analysis Report for Trust Service Providers (article 19)
Objective 1.3. — Research and 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 and Development
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 — Support the policy discussions in the area of IT security certification
Output O.2.1.2 — Restricted. Towards a Digital Single Market for high quality NIS products and services
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 — Recommendations supporting implementation of the eIDAS Regulation
Output O.2.2.4 — Recommendations for technical implementations of the General Data Protection Regulation
Output O.2.2.5 — Privacy enhancing technologies
Output O.2.2.6 — 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 — Support national and governmental CSIRTs capabilities
Output O.3.1.2 — Update and provide technical trainings for MS and EU bodies
Output O.3.1.3 — Support EU MS in the development and assessment of NCSS
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
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 — Recommendations on Cyber Insurance
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
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 and Report on Exercise after Action Activities from 2014-2016
Output O.4.1.2 — Planning of Cyber Europe 2018
Output O.4.1.3 — Support activities for Cyber Exercise Planning and Cyber Crisis Management
Objective 4.2. CSIRT and other NIS community building
Output O.4.2.1 — Support the fight against cybercrime and collaboration between CSIRTs and LEA
Output O.4.2.2 — EU CSIRT network secretariat and support for 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

3.6.2 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.

To improve better estimation of resources needed for each ENISA activity, we need to split the budget forecast in Direct and Indirect budget.

The following assumptions are used in the simplified ABB methodology.

- Direct Budget is the cost estimate of each Operational activity (listed in Activities A1 to A5) in terms of goods and services procured.
- Indirect Budget is the cost estimate of salaries, mission costs and overhead costs, attributable to each Operational or Compliance activity. The indirect budget is re-distributed against direct budget in all Activities.
- Compliance posts from Activity A5 Enabling are redistributed to Core Activities — A1 to A4, and operational posts of the Activity A5.
- Total ABB posts (FTEs) are the sum of all the posts from all activities (A1 to A5) after the re-distribution.

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

Title	Total ABB budget (€)	Total ABB posts (FTEs)
Activity 1 - Expertise. Anticipate and support Europe in facing emerging network and information security challenges	2 172 776.62	14.47
Activity 2 - Policy. Make network and information security an EU policy priority	2 737 250.55	21.58
Activity 3 - Capacity. Support Europe in setting up state-of-the-art network and information security capaties	1 809 900.52	14.34
Activity 4 - Community. Make the European network and information security community a reality	1 608 302.69	14.22
Activity 5 - Enabling. Reinforce ENISA's impact	2 916 448.62	19.38
Total	**11 244 679.00**	**84.00**

ANNEXES

ANNEX I.

RESOURCE ALLOCATION PER ACTIVITY 2017–2019

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

ANNEX II.

HUMAN AND FINANCIAL RESOURCES 2017–2019

Expenditure

Expenditure	2016		2017	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1	6 334 000.00	6 334 000.00	6 387 979.00	6 387 979.00
Title 2	1 600 000.00	1 600 000.00	1 770 700.00	1 770 700.00
Title 3	3 126 564.00	3 126 564.00	3 086 000.00	3 086 000.00
Total expenditure	**11 060 564.00**	**11 060 564.00**	**11 244 679.00**	**11 244 679.00**

Expenditure	Commitment appropriations						
	Executed Budget 2015	Budget 2016	Draft Budget 2017		VAR 2017/ 2016	Envisaged in 2018	Envisaged in 2019
			Agency request	Budget Forecast			
Title 1 Staff Expenditure	**5 923 926**	**6 334 000**	**6 387 979**	**6 387 979**	**1%**	**6 386 500**	**6 492 000**
11 Staff in active employment	4 515 300	5 267 000	5 184 279	5 184 279	-2%	5 186 400	5 247 000
– of which establishment plan posts							
– of which external personnel							
12 Recruitment expenditure	356 508	195 000	283 600	283 600	45%	261 100	270 000
13 Socio-medical services and training	140 980	218 000	177 000	177 000	-19%	190 000	195 000
14 Temporary assistance	911 137	654 000	743 100	743 100	14%	749 000	780 000
Title 2 Building, equipment and miscellaneous expenditure	**1 427 497**	**1 600 000**	**1 770 700**	**1 770 700**	**11%**	**1 687 500**	**1 741 000**
20 Building and associated costs	923 342	1 041 000	1 031 500	1 031 500	-1%	1 000 500	1 021 000
21 Movable property and associated costs	22 551	62 000	69 000	69 000	11%	60 000	63 000
22 Current administrative expenditure	56 952	51 000	60 000	60 000	18%	62 000	67 000
23 ICT	424 653	446 000	610 200	610 200	37%	565 000	590 000
Title 3 Operational expenditure	**2 712 851**	**3 126 564**	**3 086 000**	**3 086 000**	**-1%**	**3 375 000**	**3 426 000**
30 Activities related to meetings and missions	836 823	734 000	697 000	697 000	-5%	715 000	736 000
32 Horizontal operational activities	408 267	392 564	530 000	530 000	35%	660 000	690 000
36 Core operational activities	1 467 761	2 000 000	1 859 000	1 859 000	-7%	2 000 000	2 000 000
TOTAL EXPENDITURE	**10 064 274**	**11 060 564**	**11 244 679**	**11 244 679**	**2%**	**11 449 000**	**11 659 000**

Expenditure	Payment appropriations						
	Executed Budget 2015	Budget 2016	Draft Budget 2017		VAR 2017/ 2016	Envisaged in 2018	Envisaged in 2019
			Agency request	Budget Forecast			
Title 1 Staff Expenditure	**5 923 926**	**6 334 000**	**6 387 979**	**6 387 979**	**1%**	**6 386 500**	**6 492 000**
11 Staff in active employment	4 515 300	5 267 000	5 184 279	5 184 279	-2%	5 186 400	5 247 000
– of which establishment plan posts							
– of which external personnel							
12 Recruitment expenditure	356 508	195 000	283 600	283 600	45%	261 100	270 000
13 Socio-medical services and training	140 980	218 000	177 000	177 000	-19%	190 000	195 000
14 Temporary assistance	911 137	654 000	743 100	743 100	14%	749 000	780 000
Title 2 Building, equipment and miscellaneous expenditure	**1 427 497**	**1 600 000**	**1 770 700**	**1 770 700**	**11%**	**1 687 500**	**1 741 000**
20 Building and associated costs	923 342	1 041 000	1 031 500	1 031 500	-1%	1 000 500	1 021 000
21 Movable property and associated costs	22 551	62 000	69 000	69 000	11%	60 000	63 000
22 Current administrative expenditure	56 952	51 000	60 000	60 000	18%	62 000	67 000
23 ICT	424 653	446 000	610 200	610 200	37%	565 000	590 000
Title 3 Operational expenditure	**2 712 851**	**3 126 564**	**3 086 000**	**3 086 000**	**-1%**	**3 375 000**	**3 426 000**
30 Activities related to meetings and missions	836 823	734 000	697 000	697 000	-5%	715 000	736 000
32 Horizontal operational activities	408 267	392 564	530 000	530 000	35%	660 000	690 000
36 Core operational activities	1 467 761	2 000 000	1 859 000	1 859 000	-7%	2 000 000	2 000 000
TOTAL EXPENDITURE	**10 064 274**	**11 060 564**	**11 244 679**	**11 244 679**	**2%**	**11 449 000**	**11 659 000**

Revenue

Revenues	2016	2017
	Revenues estimated by the agency	Budget Forecast
EU contribution	10 120 000	10 322 000
Other revenue	940 564	922 679
Total revenues	**11 060 564**	**11 244 679**

Revenues	2015	2016	2017		VAR 2017/ 2016	Envisaged in 2018	Envisaged in 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**	**10 322 000**		**2.00%**	**10 529 000**	**10 739 000**
of which Administrative (Title 1 and Title 2)							
of which Operational (Title 3)							
of which assigned revenues deriving from previous years' surpluses	55 000	50 000	80 000				
3 THIRD COUNTRIES CONTRIBUTION (incl. EFTA and candidate countries)	**270 288**	**300 564**	**282 679**		**-5.95%**	**280 000**	**280 000**
of which EFTA	270 288	300 564	282 679		-5.95%	280 000	280 000
of which Candidate Countries							
4 OTHER CONTRIBUTIONS	**616 379**	**640 000**	**640 000**		**0.00%**	**640 000.00**	**640 000.00**
of which delegation agreement, ad hoc grants							
5 ADMINISTRATIVE OPERATIONS	**21 946**	**0.00**	**0.00**		**0.00%**	**0.00**	**0.00**
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT							
7 CORRECTION OF BUDGETARY IMBALANCES							
TOTAL REVENUES	**10 064 274**	**11 060 564**	**11 244 679**		**1.66%**	**11 449 000**	**11 659 000**

Budget outturn and cancellation of appropriations

Calculation of 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.

ANNEX III.

HUMAN RESOURCES — QUANTITATIVE

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	Expected to be filled as of 31. 12. 2016	In draft budget for year 2017	Envisaged in 2018	Envisaged in 2019
Officials	AD								
	AST								
	AST/SC								
TA	AD	30	32	30	34	34	34	34	34
	AST	16	16	15	14	14	14	13	13
	AST/SC								
Total		**46**	**48**	**45**	**48**	**48**	**48**	**47**	**47**
CA GFIV			7	9	30	30	28	28	28
CA GF III		12	15	11	5	4	3	2	2
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	34	31	30	30
SNE		2	3	2	1	2	5	6	6
Structural service providers									
Total		**62**	**75**	**69**	**84**	**84**	**84**	**83**	**83**
External staff for occasional replacement									

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	
	OF	TA	OF	TA	OF	TA	OF	TA	OF	TA	OF	TA	OF	TA	OF	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				9				10		10		10
AD 8		7		4				9				15		15		15
AD 7		6		1				7								
AD 6				14												
AD 5		1		1												
Total AD	0	32		30				34				34		34		34
AST 11																
AST 10																
AST 9																
AST 8																
AST 7												2		2		2
AST 6		2		1				3				5		5		5
AST 5		6		3				5				5		5		5
AST 4		3		3				1				2		1		1
AST 3		3		7				3								
AST 2		2		1				2								
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**				**48**		**47**		**47**

OF – officials, TA – Temporary Agents

ANNEX IV.

HUMAN RESOURCES — QUALITATIVE

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.

4.2. B. Appraisal of performance and reclassification/promotions

Reclassification of temporary staff/promotion of officials

Category and grade	Staff in activity at 1.01. Year 2015		How many staff members were promoted/reclassified in Year 2016		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		1	2
AD 7	0	4		1	3
AD 6	0	8		1	2
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		1	4
AST 5	0	3		1	4
AST 4	0	3			
AST 3	0	6		1	6
AST 2	0	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		6	

Reclassification of contract staff

Function Group	Grade	Staff in activity at 1.01.Year 2015	How many staff members were reclassified in Year 2016	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	1	0	
	9	6	0	
	8	4	0	
CA II	7	0	0	
	6	1	0	
	5	0	0	
	4	0	0	
CA I	3	0	0	
	2	1	0	
	1	0	0	
Total		13	0	

There were no reclassifications for CA staff in 2016.

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.

4.3. C. Mobility policy

ENISA is currently preparing the adoption and implementation of the Commission Implementing rule on mobility policy which was adapted to suit agency circumstances by the Standing Working Party of the Agencies. It is expected that this policy will be in place in Q4 of 2016.

4.4. D. Gender and geographical balance

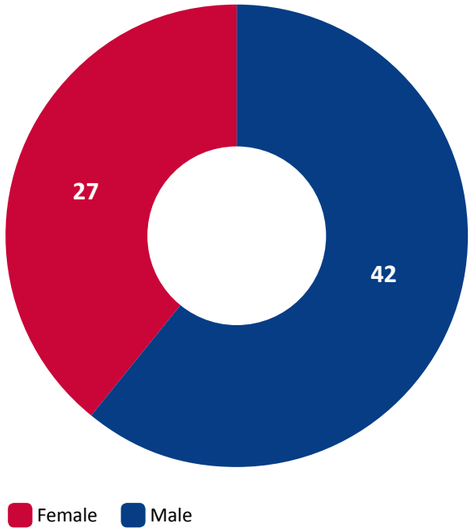
Please see the attached charts illustrating gender, geographical balance and category/grade in the Agency. Total number of Staff as of 31.12.2015: 69 (45 TA's: 30 AD's + 15 AST's + 22 CA's + 2 SNE's).

4.5. E. Schooling

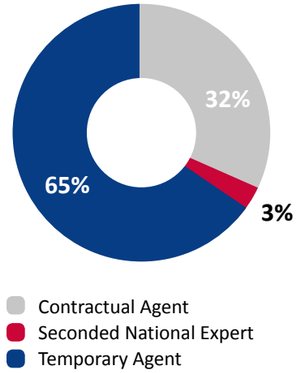
A European School is located in Heraklion and is used by Staff members of ENISA.

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.

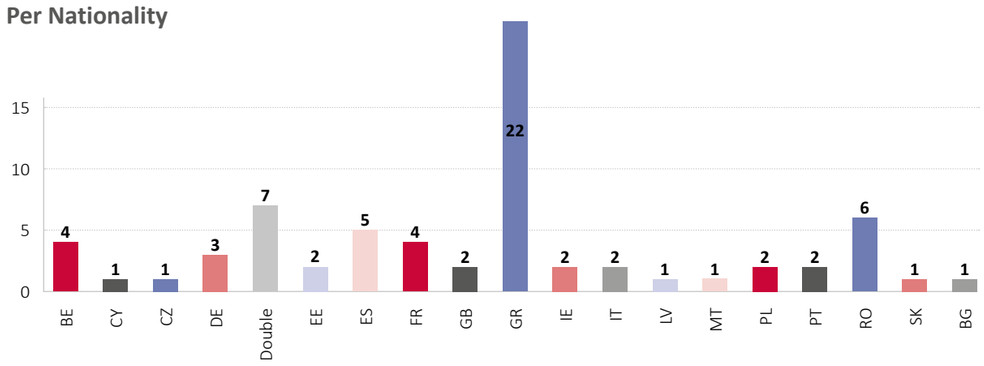
Per Gender



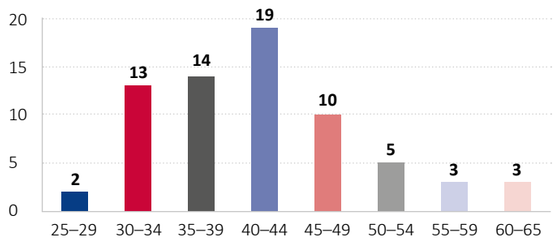
Per Category



Per Nationality



Per Age



ANNEX V.
BUILDINGS

Current building(s):

Function Group	Name, location and type of building	Other Comment
Information to be provided per building:	Heraklion, Office building Athens, Office building	The Greek Government subsidises the rent of the offices in full Office in Marousi, Athens, hosting the Core Operational activities of ENISA
Surface area (in square metres) **Of which office space** **Of which non-office space**	Heraklion: 2 042 m^2 Athens: 2 036.38 m^2	
Annual rent (in EUR)	Heraklion: EUR 299 934.60 Athens: EUR 316 444.08	
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.

ANNEX VI.
PRIVILEGES AND IMMUNITIES

Agency privileges	Privileges granted to staff	
	Protocol of privileges and immunities/ diplomatic status	Education/day care
In accordance with Article23 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

ANNEX VII.
EVALUATIONS

Internal monitoring system MATRIX has been put in place at ENISA and is used for project management by ENISA staff. Regular progress reports are presented at the meetings of the ENISA management team and reviewed at the midterm review meetings.

Also, external consultant has been contracted to carry annual ex post evaluation of core operational activities. The scope of the evaluation focusses on ENISA's core operational activities, with an estimated expenditure above EUR 30 000.00. The overall objective of the annual evaluations is to evaluate the effectiveness, efficiency, added value, utility, coordination and coherence.

The following table summarises the findings per evaluation criteria and outlines actions ENISA's management considered as important. The evaluation of 2014 core operational activities is largely positive and the actions mainly relate to a continuation of the work carried out.

Criteria	Summary findings	Possible Actions
Relevance	Based on the findings, it can be concluded that ENISA clearly responds to a need in the European NIS landscape. The scope and objectives of ENISA's work are seen as relevant to respond to the needs, but at the same time stakeholders see limits to ENISA's mandate and outreach, which affects the ability of the Agency to effectively meet the needs	Continue to explore ways to ensure ENISA's work is addressing real needs in NIS in the EU Map/assess gaps in current NIS landscape, to feed into discussions on future mandate 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
Impact	It appears that, despite ENISA's limited mandate and also fairly small resources, the Agency manages to make a real contribution towards increased NIS in Europe, as perceived by key stakeholders	N/A
Effectiveness — KIIs and downloads	All KIIs were achieved. The evaluation can conclude that some of ENISA's deliverables have generated a high number of downloads in a short period of time (most reports were made available in Q1 2015 and thus downloads had only been available for a few months at the time of writing)	Introduce more ambitious KIIS which enable a tracking of performance
Effectiveness — EU Policy	The evaluation findings show that the work conducted under work stream 1 has been successful in achieving most objectives. In particular, the work undertaken to identify evolving threats, risks and challenges, and the contribution to EU policy initiatives appear to have achieved the intended results. For the work done in supporting the EU in education, research and standardisation, results were more mixed, in particular regarding the link to actual operational issues such as data protection and secure services. These aspects are evidently not under the direct control of ENISA but of national regulators and operators, hence the need for further efforts in coordination and cooperation	Continue efforts to build relations with senior decision-makers at Member State and EU level (public and private)
Effectiveness — Capacity building	ENISA's work to develop capacity in Member States (to coordinate and cooperate during crises, and the support to develop capacities and strategies at Member State level) as part of work stream 2 has been successful in achieving the objectives set out. The contribution to private sector capacities looks more uncertain, based on the responses from the stakeholder survey	Continue to engage with the private sector to improve and increase outreach
Effectiveness — Support cooperation	Findings show that the work stream 3 has largely achieved the objectives set, with stakeholders assessing a clear contribution of ENISA to putting in place effective measures to cope with cyber crises and incidents. In particular, ENISA's support was considered valuable to improve workflow and cooperation among involved stakeholders. That said, as the CE2014 case study concludes, there is still a long road ahead before an EU-level crisis management process is put in place in the cyber security area, with a lack of trust among stakeholders, weaknesses and differences in national capabilities, weak communication structures, insufficient exchanges of information in 'real life' etc., representing hurdles that need to be surmounted over the medium to long term	Continue trust building and cooperation activities as a means to overcome barriers to cooperation during crisis
Efficiency	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	N/A
Coordination and coherence	Overall, it can be concluded that ENISA 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	N/A

Overall, the evaluation of activities foreseen in the Work Programme 2014 conclude that ENISA 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. 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 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 Network Information Security (NIS) and cyber security.

Also, the findings and conclusions from the external evaluation of ENISA's core operational activities in 2015 confirm that ENISA generally functions efficiently; it is characterised by a clear delineation of responsibilities and has cost-saving measures in place, but one case of low efficiency was identified, namely the insufficient dissemination of publications. It was concluded that ENISA significantly enhanced cooperation both between Member States of the EU and between related NIS stakeholders in 2015 by bringing people from different operational communities around the table to share information, ideas and common areas of interest at an operational level. ENISA thereby contributed to a great extent to enhancing community building in Europe and beyond and improved services, workflow and communication among stakeholders to respond to crises. Moreover, the ex post evaluation concluded that ENISA's support to cooperation between stakeholders complemented other public interventions, clearly pointing to a role for ENISA in this regard.

The reports of annual ex post evaluations have been published on ENISA website https://www.enisa.europa.eu/about-enisa/annual-ex-post-evaluation-of-enisa-activities .

ANNEX VIII.
RISKS YEAR 2017

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

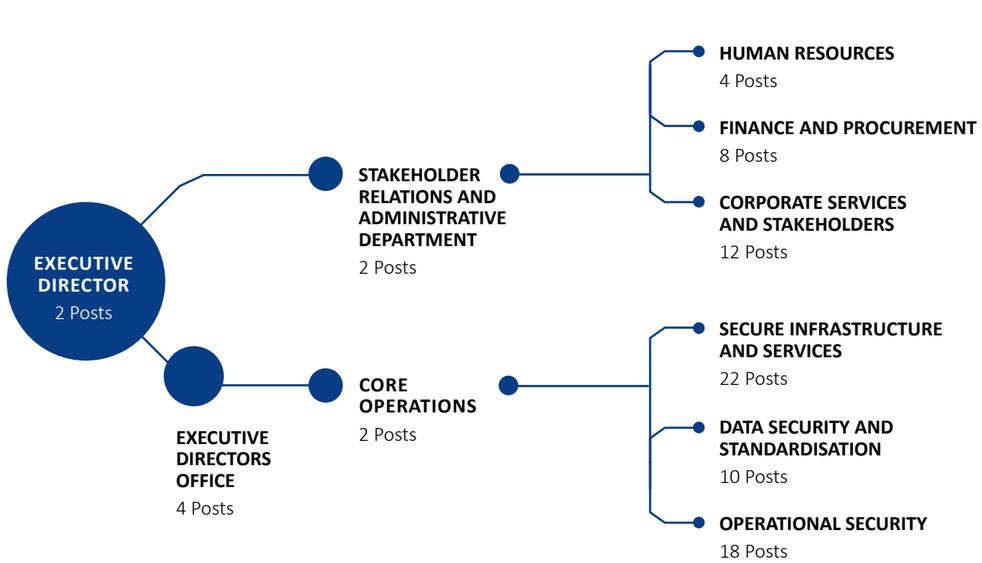
ANNEX IX.
PROCUREMENT PLAN YEAR 2017

2017 WP Procurement Planning – Preliminary budget breakdown	Direct budget (in EUR)	Procurement (tender) procedure required	Launch Q1-Q4?	All other expenditure
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 OES Sectors	195 000.00	180 000.00	Q1	15 000.00
Output O.1.1.2 — Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures	50 000.00	50 000.00	Q1	0.00
Objective 1.2. NIS Threats Landscape and Analysis				
Output O.1.2.1 — Annual ENISA Threat Landscape	105 000.00	50 000.00	Q1-Q2	55 000.00
Output O.1.2.2 — Annual Incident Analysis Report for the Telecom sector (article 13 a)	30 000.00	0.00	Q1	30 000.00
Output O.1.2.3 — Annual Incident Analysis Report for Trust Service Providers (article 19)	30 000.00	0.00	Q1	30 000.00
Objective 1.3. Research and Development, Innovation				
Output O.1.3.1 — Guidelines for the European standardisation in the field of ICT security	45 000.00	40 000.00	Q2	5 000.00
Output O.1.3.2 — Priorities for EU Research and Development	30 000.00	30 000.00	Q1	0.00
Objective 1.4. Response to Article 14 Requests under Expertise Activity				
Output O.1.4.1 — Response to Requests under Expertise Activity	0.00	0.00		0.00
Total Activity 1	**485 000.00**	**350 000.00**		**135 000.00**

2017 WP Procurement Planning – Preliminary budget breakdown	Direct budget (in EUR)	Procurement (tender) procedure required	Launch Q1-Q4?	All other expenditure
Activity 2 — Policy. Make network and information security an EU policy priority				
Objective 2.1. Supporting EU policy development				
Output O.2.1.1 — Support the policy discussions in the area of IT security certification	100 000.00	80 000.00	Q1, Q2	20 000.00
Output O.2.1.2 — Restricted. Towards a Digital Single Market for high quality NIS products and services	40 000.00	35 000.00	Q1	5 000.00
Objective 2.2. Supporting EU policy implementation				
Output O.2.2.1 — Contribute to EU policy in the area of electronic communications sector	45 000.00	0.00	Q1	45 000.00
Output O.2.2.2 — Develop guidelines for the implementation of mandatory incident reporting	60 000.00	50 000.00	Q2	10 000.00
Output O.2.2.3 — Recommendations supporting implementation of the eIDAS Regulation	96 000.00	86 000.00	Q1, Q2	10 000.00
Output O.2.2.4 — Recommendations for technical implementations of the General Data Protection Regulation	50 000.00	25 000.00	Q1, Q2	25 000.00
Output O.2.2.5 — Privacy enhancing technologies	70 000.00	35 000.00	Q1, Q2	35 000.00
Output O.2.2.6 — Supporting the Implementation of the NIS directive	150 000.00	125 000.00	Q1	25 000.00
Objective 2.3. Response to Article 14 Requests under Policy Activity				
Output O.2.3.1 — Response to Requests under Policy Activity	0.00			
Total Activity 2	**611 000.00**	**436 000.00**		**175 000.00**
Activity 3 — Capacity. Support Europe in setting up state-of-the-art network and information security capacities				
Objective 3.1. Assist Member States' capacity building				
Output O.3.1.1 — Support national and governmental CSIRTs capabilities	30 000.00	0.00	Q1	30 000.00
Output O.3.1.2 — Update and provide technical trainings for MS and EU bodies	175 000.00	120 000.00	Q1	55 000.00
Output O.3.1.3 — Support EU MS in the development and assessment of NCSS	40 000.00	0.00	Q1	40 000.00
Objective 3.2. Support EU institutions' capacity building				
Output O.3.2.1 — Restricted and public Info notes on NIS	9 000.00	0.00		9 000.00
Output O.3.2.2 — Restricted. Upon request, support the assessment of existing policies/procedures/ practices on NIS within EU institutions	15 000.00	0.00	Q1	15 000.00
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	50 000.00	45 000.00	Q1	5 000.00
Output O.3.3.2 — Recommendations on Cyber Insurance	25 000.00	0.00		25 000.00
Objective 3.4. Assist in improving general awareness				
Output O.3.4.1 — Cyber Security Challenges	30 000.00	15 000.00		15 000.00
Output O.3.4.2 — European Cyber Security Month deployment	30 000.00	0.00	Q2	30 000.00
Objective 3.5. Response to Article 14 Requests under Capacity Activity				
Output O.3.5.1 — Response to Requests under Capacity Activity	0.00	0.00		0.00
Total Activity 3	404 000.00	180 000.00		224 000.00
Activity 4 — Community. Make the European network and information security community a reality				
Objective 4.1. Cyber crisis cooperation				
Output O.4.1.1 — Evaluation of Cyber Europe 2016 and Report on Exercise after Action Activities from 2014-2016	40 000.00	20 000.00		20 000.00
Output O.4.1.2 — Planning of Cyber Europe 2018	80 000.00	70 000.00	Q1	10 000.00
Output O.4.1.3 — Support activities for Cyber Exercise Planning and Cyber Crisis Management	80 000.00	70 000.00	Q1	10 000.00
Objective 4.2. CSIRT and other NIS community building				
Output O.4.2.1 — Support the fight against cybercrime and collaboration between CSIRTs and LEA	59 000.00	49 000.00	Q2	10 000.00
Output O.4.2.2 — EU CSIRT network secretariat and support for EU CSIRT network community building	100 000.00	50 000.00	Q1	50 000.00
Objective 4.3. Response to Article 14 Requests under Community Activity				
Output O.4.3.1 — Response to Requests under Community Building Activity	0.00	0.00		0.00
Total Activity 4	**359 000.00**	**259 000.00**		**100 000.00**
Total A1-A4	**1 859 000.00**	**1 225 000.00**		**634 000.00**
Activity 5 — Enabling. Reinforce ENISA's impact				
Objective 5.1. Management				
Executive Director and assistant	32 000.00	0.00		32 000.00
Executive Directors Office	80 000.00		Q1	80 000.00
MB and EB	117 000.00		Q1-Q4	117 000.00
Management of Departments	2 000.00	0.00		2 000.00
Objective 5.2. Engagement with stakeholders				
Meetings PSG, NLO, HLE, Industry Event	163 000.00	0.00		163 000.00
Stakeholders Communications	170 000.00	20 000.00		150 000.00
Objective 5.3. International relations				
International relations	0.00	0.00		0.00
Objective 5.4. Compliance and support				
IT	67 000.00	5 000.00		62 000.00
Internal Communications	20 000.00	0.00		20 000.00
Total Activity A5	**651 000.00**	**25 000.00**		**626 000.00**
Total A1-A5	**2 510 000.00**	**1 250 000.00**		**1 260 000.00**

ANNEX X.
ORGANISATION CHART

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



NOTES

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

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Catalogue number: TP-AH-16-001-EN-N
ISSN: 2467-4176
ISBN 978-92-95032-43-9
DOI: 10.2824/132933

enisa.europa.eu