ENISA Programming Document 2018-2020

Including Multiannual planning, Work programme 2018 and Multiannual staff planning

STATUS: DRAFT FOR MB APPROVAL

VERSION: JANUARY, 2017

About ENISA

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

Table of Contents

Foreword

The digital environment and digital economy are essential driving forces for growth in Europe. It is clear however, that the EU will not be able to achieve 'digital growth' in the absence of an approach to cybersecurity that engenders trust in the wider community. It is therefore logical that the roles and responsibilities of the European Union Agency for Network and Information Security (ENISA) have been evolving to support the requirement of a modern and secure digital society. 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 for the overall society.

The exponential increase of needs in NIS represent a major challenge for the Agency. The Agency effectively perform optimization on performance and at the same time needs to prioritize the work program to address the most important issues in the NIS hemisphere. 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 with in the above mentioned stakeholders.

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.
- Communities mobilization

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 2018 to 2020 are presented alongside the detailed planning for 2018. The document follows the structure laid down by the new EC guidelines for programming documents provided in the context of Framework Financial Regulation.

ENISA requested additional resources for Work Programme 2017. Although the European Parliament (EP) supported an increase in budget with two million euro including an additional 6 posts for ENISA, this was not agreed in the Conciliation Committee which includes the Council of the EU and the European Parliament.

For 2018, ENISA requests again additional resources. In summary, this Programing Document presents two scenarios for Work programme 2018. These scenarios are presented, based on a proposed prioritisation of work. In the first scenario, only priority 1 activities are considered where the budget and resources allocations in the summary tables and Annexes are in line with the COM Multiannual Financial Framework (MAFF) 2014-2020. In the second scenario, additional activities proposed by the Management Board and Permanent Stakeholder group, marked Priority 2, with an increase of budget by 2,5 million and additional 6 posts are added.

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
CSSU: Corporate Stakeholders and Services Unit
COD: Core Operational Department
COM: European Commission
CSS: Cyber Security Strategy
DG: EC Directorate-General
DG CONNECT: EC Directorate-General CONNECT
DPA: Data Protection Authorities
DPO: Data Protection Officer
DSM: Digital Single Market
E: Event, type of output i.e. conference, workshop, and seminar
EB: ENISA Executive Board
EC3: European Cybercrime Centre, Europol
ECA: European Court of Auditors
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
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
IAS: Internal Audit Service
ICC & IAC: Internal Control Coordination and Internal Audit Capability
ICS/SCADA: Industrial Control Systems/Supervisory Control and Data Acquisition
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
QMS: Quality Management System
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.

Year	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
	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: 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
	COM Communication on CIIP (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), Official Journal 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

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

Securing Europe's information society

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

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

Adding Value through Complementarity

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

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

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

Achieving Results by Leveraging the Stakeholder Community

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

Creating European Solutions to Enable EU Industry

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

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

Using Security to Strengthen Privacy

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

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

Bridging Public & Private Sectors

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

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

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

1. Section I – General Context

The ENISA Threat Landscape for 2016 made a number of interesting remarks regarding the evolution of the threat environment.

Cyber-threats have undergone significant evolution in terms of sophistications and impact, e.g. extortion/ransom activities and user information stealing. Data breaches have shown enormous growth with hundreds of millions of items of user data flooding the Internet and being covered by front pages of media on almost weekly or monthly basis. Security incidents involving IoT and large volume DDoS attacks complement the threat landscape.

Cyber-threat agents performed a variety of malicious acts greatly increasing the estimates of cyber-crime monetization. The boost of cyber-crime monetization is illustrated in the following particular cases:

- Cyber-Crime Capitalisation in 2016 almost reaches the level of the second most valuable US company.
- Ransomware families are 175% up and average ransom is 100% up (600-700$).
- Data Breaches are as of today 20% over last year.
- The first 1Tbps DDoS attack has happened. It has shown impact DDoS-attacks may have (internet service latencies).
- Cyberspace is a recognised battlefield. This creates a new centre of gravity for the whole cyber-security community.
- In 2016 we have seen the impact and scale of striking power of taking over IoT objects.

In 2016, the race between attackers and defenders continues to suggest that cyber threat agents are always a step ahead defenders. Still, there are some changes in the current state-of-play:

- Defenders have expanded their knowledge on modus operandi by using/implementing cyber-threat intelligence and applying it to their business products and processes in order to enhance their proactive protection strategies.
- Defenders have implemented de-anonymization methods to identify adversaries hiding behind the dark net.
- Defenders have understood that defence is only the one side of the coin and are slowly moving in exploring active/offensive defence capabilities.
- Attackers leveraged vast publicly available intelligence, e.g. published malware source code, to evolve their methods.
- Attackers put quite a lot of effort in investing and supporting their infrastructure as well as marketing their products and services to maintain their lucrative business.

The above points lead to some additional remarks. Adversaries have increased cyber-crime “capitalization” to a new all-time record. The cooperation between law enforcement agencies and private sector organisations were key in identifying malicious activities and infrastructure takedowns. Finally, despite defenders having raised their entry level engagements the time to detect a breach increased further this year, which means that defenders detect incidents at lower speed as they are caused and need to reverse this in the future.

Concluding, on top of a quite active cyber-crime scene, ETL has indicated that high profile (state-sponsored) attackers have taken further action with their involvement in highly sophisticated and stealthy

cyber-attacks, cyber espionage, cyber-sabotage acts, and multi-layer attacks that even managed to influence political developments. Their active presence suggests that cyber-space operations might eventually sketch the term cyber-warfare and requires the attention of everyone as the future of the cyber-space is increasingly threatened every year.

2. Section II Multi-annual programming 2018 – 2020

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 5 activities, presented in more detail in section 2.2, and referred throughout the document with the following suggestive names: expertise, policy, capacity, community and enabling.

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.
#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.

[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 prioritized mid-term operational objectives to be achieved by ENISA within a period of 3 years. Annual concrete activities (outputs) will be identified in the annual work programmes, according to a recursive approach in order to achieve the mid-term operational objectives and in the long term the strategic objectives.

In the sections that follow, priorities, guidelines and an appreciation of the added value have been summarised by activity. Note however, that these descriptions do not cover objectives related to 'Article 14 Requests' as such requests are made on an ad hoc basis and ENISA cannot predict their content in advance. A summary table of the WP2018 Outputs is presented in Section 3.6.1. In this table priorities are also indicated.

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 investigate their implications for 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 and NIS competent authorities 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 the specific security challenges that those technologies and services pose on critical infrastructures, businesses at large and citizen's private data.

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

This activity has 3 main objectives which are described from a multiannual perspective in the next sub-sections and a separate Objective dedicated to Article 14 requests. Each objective is presented providing priorities for 2018-2020, the guidelines on how to achieve the objectives and the added-value provided by ENISA.

2.2.1.1 Multiannual priorities (2018-2020) for Objective 1.1. Improving the expertise related to NIS

Priorities

- undertake regular stocktaking of existing expertise within the EU on NIS challenges related to existing or future services and technologies, and make that information available to the EU NIS community;
- among these challenges, focus on key issues to offer analyses and general recommendations;
- seek to explore in particular issues related to software (e.g. mobile), ICS/SCADA, smart infrastructures and Internet of Things;

Guidelines

- collate and analyse in priority available expertise provided by national NIS competent authorities, closely liaise with them to support its stocktaking activity and when drawing analyses and

recommendations offer the opportunity to voluntary experts from these authorities as well as from other relevant stakeholders to take part to its work;
- focus on challenges of significant added-value for the EU NIS community and on aspects to the impact that they may have on the functioning of critical economic and societal functions with the EU, as foreseen in the NIS directive (e.g. expertise relevant to Operators of Essential Services);
- take a holistic approach encompassing the technical, organizational, regulatory, policy dimensions of NIS as well as different relevant approaches, including the user's perspective and work whenever possible on a multiannual basis to deepen understanding of identified issues;

Added-value

- provide European-wide visibility to existing NIS expertise, in particular developed at national level;
- foster convergent understanding of NIS challenges across the EU NIS community as well as best practices to address them, by offering tailored, high quality and up-to-date analysis and recommendations;
- raise awareness of operators, European institutions and national public authorities on rising security challenges that should be taken into account at technical and policy levels;
- support its work under Activity 2 (Policy), 3 (Capacity) and 4 (Community) by advising on challenges that may influence EU NIS policy developments and implementation, national and European capacity building as well as crisis and CSIRT cooperation.

2.2.1.2 Multiannual priorities (2018-2020) for Objective 1.2. NIS threat landscape and analysis

Priorities

- produce annual analyses of national incident reports within the framework of the implementation of the Telecom package, eIDAS and the NIS directive;
- carry an annual EU threat landscape offering a general technical assessment of existing and anticipated threats and their root causes;
- in addition to the general threat assessment, focus as well on a specific dimension (e.g. sector or cross-sector threats in the context of the NIS directive, or threats to existing technologies whose usage is increasing e.g. IPV6 and threats today underestimated which may increase in the future);

Guidelines

- seek synergies among national incident reports in its analyses mentioned above;
- ensure that the EU threat landscape benefit from these analyses as well as from other relevant sources of information, in particular existing national threat assessments as well as information stemming from the CSIRT network subject to its approval;
- seek to enhance visibility of these results to the EU NIS community;

Added-value

- offer an EU-wide independent synthesis on technical threats of general interest for the EU, in particular in the context of the implementation of the NIS directive (operators of essential services, digital service providers);
- improve general awareness on threats of national and European public and private entities and bodies and foster mutual understanding by National Competent Authorities on current and future threats;

- support its work under other Activities by advising on threats that may influence EU NIS policy developments and implementation (Activity 2), by encouraging Member States' to develop national threat assessments and advising the Union institutions, bodies and agencies (hereinafter: "Union institutions") on threats to their security (Activity 3) as well as creating synergies with crisis and CSIRT cooperation such as by supporting cooperation on the development of threats taxonomies (e.g. incident taxonomies) (Activity 4);

2.2.1.3 Multiannual priorities (2018-2020) for Objective 1.3. Research & development, Innovation

Priorities

- support Member States and the European Commission define EU priorities in the field of R&D within the context of the European contractual Public and Private Partnership (ECSO);

Guidelines

- provide the secretariat of the National Public Authorities committee of ECSO (NAPAC);
- support cooperation among National Public Authorities on issues related to the definition of R&D and when relevant liaise with other stakeholders' represented within ECSO;
- participate, whenever possible and upon request, in chosen ECSO Working Groups

Added-value

- contribute to the smooth functioning and impact of the cPPP and seek to avoiding duplication of efforts of Union institutions and Member States on R&D and innovation;
- become a reference point of contact for Member States on R&D related issues;
- contribute to reduce the gap between research and implementation;
- support its work under Activity 2 by ensuring synergy between its advising role on R&D within the context of ECSO and is advising role on other EU NIS policy issues addressed within and outside the context of ECSO, in particular related to the establishment of a functioning Digital Single Market;

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

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

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

- Developing European NIS related policies and laws. To this end, ENISA will proactively engage with Union institutions, and in particular all relevant DGs of the European Commission, in order to provide input, including preparatory work, advice and analyses related to the development and update of Union NIS policy and law.
  In cooperation with the Member States, especially 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 appropriate EU policy levers. ENISA will, in particular, promote the integration of NIS aspects within policies with a – direct or indirect – digital focus. 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. Although ENISA is primarily focusing on the implementation of the NIS Directive, it will also support cooperation among Member States regarding other EU policies and regulations with a NIS scope 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 2 main objectives described in the following sub-sections and a separate objective covering Article 14 requests.

2.2.2.1 Multiannual priorities (2018-2020) for Objective 2.1. Supporting EU Policy Development

Priorities

- carry out a regularly updated stocktaking of ongoing and future EU policy initiatives with NIS implications and make it available to the European Commission and national NIS competent authorities;
- focus in particular on policies related to the sectoral dimension of NIS, such as in the energy and transport sectors and on policies dedicated to NIS (e.g. DSM, IT security certification, crisis cooperation blueprint, education and training, information hub) in view of ensuring coherence with the framework and principles agreed upon in the NIS directive;
- seek to identify when possible NIS challenges that may require policy developments at EU level;
- build upon this stocktaking and taking into accounts NIS challenges previously identified, offering NIS expert advice the European Commission and other relevant Union institutions on these policy developments;

Guidelines

- closely liaise with the European Commission in view of establishing an up-to-date stocktaking of ongoing and future initiatives;
- benefit from its work undertaken in Objective 1 on NIS challenges and threats to advice on possible new policy developments;
- foster dialogue among and with national NIS competent authorities' experts and other relevant stakeholders in view of developing in-depth and high quality expertise in view of advising on EU policy developments;
- ensure coherence of its work on DSM related policy developments with work undertaken within the framework of ECSO and when relevant contribute to that work according to its responsibilities with ECSO;
- regularly inform national NIS competent authorities on a policy level via the Cooperation Group established by the NIS directive of interest to the group;

Added-value

- foster awareness of the EU NIS community on EU policy developments with a NIS dimension;
- foster the inclusion of a NIS aspects in key EU policies offering a digital dimension;

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

- contribute to ensure coherence between future sectoral policy initiatives including regulations with the framework and principles agreed upon by the Member States and the European Parliament in the NIS directive, acting as an "umbrella" of EU policy initiatives with a NIS dimension;

2.2.2.2 Multiannual priorities (2018-2020) for Objective 2.2. Supporting EU Policy Implementation

Priorities

- support national NIS competent authorities to work together towards the implementation already agreed EU policies (legislations) with a NIS dimension, by allowing them to share national views and experiences and build upon those to draw consensual recommendations;
- focus on the NIS Directive in particular regarding requirements related to Operators of Essential Services (e.g. identification, security requirements, incident reporting) and on eIDAS as well as on NIS aspects of, GDPR (and more generally data protection) and the ePrivay directive.

Guidelines

- establish structured dialogues, whenever possible sustainable on a multiannual basis, with voluntary national NIS competent authorities' experts, themselves liaising with national stakeholders'' (e.g. Operators of Essential Services - OES);
- aim at limiting the number of dialogues in view of increasing the participation of all Member States and in a spirit of efficiency, such as on the NIS of OES by favouring a cross-sectoral approach, while taking gradually into account sector specificities;
- regularly inform national NIS competent authorities on a policy level via the Cooperation Group established by the NIS directive and in particular make its stocktaking;

Added-value

- support Member States implement EU policies by making available high quality recommendations building upon the experience of the EU NIS community and reduce duplication of efforts across the EU;
- foster the harmonized approach on implementation of EU policies and in particular legislations, even when mandatory harmonization of national approaches is not enforced, such as in the NIS Directive regarding OES;

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. It will focus in priority

on those highlighted in the NIS Directive such as the development and efficient functioning of National/Governmental CSIRTs, the collaboration amongst national competent authorities in the framework of the Cooperation Group, the development of national strategies, the establishment of necessary national incident reporting schemes and information security trainings. Upon request, ENISA will offer direct support to individual Member States[4]. To that end, the Agency will develop proactive relationships with Governments across the EU.

- Private sector: ENISA will support Member States in engaging with the private sector on their NIS, encouraging companies to take a whole-business approach to cyber threats from the board level to the operational level. ENISA will also work with the private sector to help in improving cyber security of networks within companies, taking into account the views of the private sector with experience on specific NIS topics. ENISA will work closely with the NLO community in order to define exactly how this dialogue will occur.
- Union institutions: in close coordination with the Union institutions, ENISA will support them in reinforcing their NIS capabilities and to that end, will establish a close and sustainable partnership with CERT-EU. As part of this mission, ENISA will advise on key orientations and, upon request, on actions to be implemented in order to achieve a high level of NIS across all Union institutions. ENISA will, also, produce with CERT-EU information notes on threats and risks with a view to making the EUIs and agencies more secure. ENISA will, whenever this is adequate, build on experience gained by CERT-EU and the Union institutions to contribute to the broader EU NIS community.
- Citizens: alongside Member States, ENISA will help EU citizens to gain essential cyber security knowledge and skills to help protect their digital lives. This will include promoting an annual European Cyber Security month and working with the Member States delivering projects like the Cyber Security Challenge as well as national initiatives, upon request from a Member State.

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

To achieve this, the activities covering capacity building are structured in 4 objectives, targeting the above mentioned four main actors (grouped as follows: MS's and EU's institutions, private sector and general awareness) and a separate objective addressing the Article 14 requests in this area. The multiannual objectives for 2018-2020 are described in the next sub-sections.

2.2.3.1 Multiannual priorities (2018-2020) for Objective 3.1 Assist Member States' capacity building

Priorities

- advice and assist Member States in developing national cybersecurity capacities building upon national experiences and best practices;
- focus on NIS capacities foreseen in the NIS Directive, building on ongoing activities in the CSIRT Network and national CSIRTs which ENISA should continue to work on with the aim of fostering the rising of EU Member States' CSIRTs;
- develop a NIS national capacities metrics, building upon capacities foreseen in the NIS directive, allowing an assessment of the state of NIS capacity development with the EU;

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

- identify and draw recommendations on other national NIS capacities which the spread across the EU NIS community would contribute to reinforcing the NIS of the EU, e.g. national cybersecurity assessments, PPPs such as in the field of CIIP, national information sharing schemes, etc.

Guidelines

- carry on a regular stocktaking of national NIS capacity initiatives with a view of identify trending developments in view of collecting and analysing different approaches and practices;
- liaise closely with national NIS competent authorities' experts in view of retrieving view, experience and best practices on national NIS capacity developments;
- take into account developments and recommendations that may arise from the CSIRT network as well as the Cooperation Group;
- adopt a holistic approach of NIS capacities ranging from technical to organizational and policy ones;
- while creating a general NIS capacity metrics, seek in priority to identify main trends at EU level and advice individual Member States upon their request;
- explore the development of tools and initiatives with a view to making ENISA's recommendations more visible and increase their impact (e.g. summer school, onsite trainings)

Added-value

- continue to support the development of national NIS capacities reinforcing the level of preparedness and response capacities of Member States thus contributing to the overall cybersecurity of NIS across the EU;
- foster sharing of best practices among Member States;
- indirectly contributing to capacity building of governments beyond the EU by making its recommendations and training material available on its website, thus contributing to the international dimension of its mandate;
- in the context of CSIRTs, contribute to its work under Activity 4 by supporting the development of CSIRTs maturity as well as tools (e.g. in the context of CEF) benefiting to the cooperation within the CSIRT network and the development

2.2.3.2 Multiannual priorities (2018-2020) for Objective 3.2 Assist and EU institutions' capacity building

Priorities

- offer proactive advice to the Union institutions on the reinforcement of their NIS;
- seek to assist in and facilitate EU Institutions in relation to approaches on NIS;
- inform on a regular basis, when possible in cooperation with CERT-EU, the European Commission and other relevant Union institutions, bodies and agencies on threats to NIS via the production of information notes;
- provide (upon request and in coordination with the institutions) capacity building support in areas like trainings, awareness, and development of education material.

Guidelines

- identify in priority on EU agencies and bodies with most NIS capacity building needs by establishing regular interactions with them (e.g. annual workshop) and focus in priority on them;

- partner with CERT-EU and institutions with strong NIS capabilities in view of supporting its actions under this objective;
- build upon its expertise on national NIS capacity building and NIS challenges to support ENISA's work under this objective;
- envisage linking its work regarding Union institutions with general awareness raising campaigns (e.g. ensuring involvement of Union institutions in the ECSM).

Added-value

- support the development of NIS capacities of Union institutions thus contributing to raising the level of the overall cybersecurity of NIS across the EU;
- foster sharing of best practices among Union institutions and reduce duplication of efforts and convergence of their approaches to NIS;
- complement CERT-EU, responsible for the "reactive" dimension of the NIS of Union institutions, by offering advice on the "prevention" dimension of NIS;

2.2.3.3 Multiannual priorities (2018-2020) for Objective 3.3 Support private sector capacity building

Priorities

- advice private sector on how to improve their own NIS through the elaboration of key recommendations for the cybersecurity of private sector;
- support information sharing from among public and private sectors on NIS developments at European level;

Guidelines

- build in priority upon existing work done at national level in relation with private sector on the basis on regular stocktaking of national expertise on this issue (e.g. cyber hygiene) as well as upon its work under Activity 1 to offer high-quality, up-to-date and high value recommendations to the benefit of the EU NIS community;
- adapt its recommendations to specific target audiences (SMEs, large size enterprises, NIS experts or non-experts) and adopt a holistic approach of NIS capacities ranging from technical/operational to organizational and policy capacities;
- with a view of supporting information sharing on NIS developments at European level, contribute to the functioning of ECSO as foreseen in Objective 1.3 and 2.1 and when wishing to interact with specific sectors, liaise with Member States primarily responsible for interacting with private stakeholders nationally;
- offer as well advice on how to improve private-private exchanges of information (e.g. via ISACs) and on an ad hoc basis and without prejudice to its achieving its priorities under this objective, continue to support specific European ISACs.

Added-value

- raise awareness within private sector on the need to reinforce their NIS;
- support the development of the NIS of businesses across the EU and support national NIS competent authorities in their similar efforts towards private sector, thus contributing to raising the level of the overall cybersecurity of NIS across the EU;

2.2.3.4 Multiannual priorities (2018-2020) for Objective 3.4 Assist in improving general awareness

Priorities

- Organize the European Cybersecurity Month (ECSM) and the European Cybersecurity Challenge (ECSC) with a view of making these events sustainable EU « rendez-vous » ;
- Carry out regular stocktaking of national awareness raising initiatives;
- building upon this stocktaking and in liaison with the ECSM and ECSC, analyze and draw recommendations and advice on best practices in the field of awareness raising, in particular with regard to communication activities;

Guidelines

- establish a structured and sustainable (multiannual) dialogue with voluntary national NIS competent authorities' experts on awareness raising and communication, responsible for the national dimension of the ECSM and ECSC;
- adopt a holistic approach to awareness raising and adapt its recommendations to specific target audiences, from the citizens to public authorities;
- explore ways of using adapted communication channels within the framework of the ECSM and ECSC;

Added-value

- allow the organization of European-wide events, increasing visibility on cybersecurity and on ENISA with the EU citizens, businesses, academia and the NIS community, including NIS students;
- foster harmonization of tailored awareness raising messages across the EU with increased impacts, building upon the strengths of existing national initiatives thanks to the sharing of best practices among them;
- strengthen cooperation among the Member States;
- facilitate the development of national awareness raising initiatives on a national level.

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 prioritise the following:

- CSIRT cooperation among the Member States, by supporting voluntary cooperation among Member States CSIRTs, within the CSIRT network established by the NIS Directive. As part of this activity, ENISA will provide the secretariat of this network and actively support its functioning by suggesting ways to improve cooperation among CSIRTs and supporting this cooperation, including by developing and providing guidance on best practices in the area of operational community efforts, such as on information exchange.
- Cyber crisis cooperation among Member States, by continuing to support the organization of the Cyber Europe exercises which shall remain one of ENISA's key priority activities, while ensuring adequate synergies with the CSIRT network. Building on its experience with Cyber Europe and on

the secretariat of CSIRT Network, this stream of work could be further developed in the next years, in particular with regard to ENISA role in the forthcoming blueprint for cyber crisis cooperation.
- The Connecting Europe Facilities (CEF) Cybersecurity Digital Infrastructure (DSI) will be key stream of work contributing to CSIRT's cooperation, in particular because ENISA is expected to operate and host and maintain the Core Service Platform (CSP) modules that are centralised.
- Dialogue among NIS related communities, including between CSIRTs and law enforcement and data privacy communities, in order to support a coherent EU-wide approach to NIS. In this context, ENISA will continue to interact with Europol (EC3) and the EDPS.
- 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 two objectives described from multiannual perspective in the following subsections.

2.2.4.1 Multiannual priorities (2018-2020) for Objective 4.1 Cyber crisis cooperation

Priorities

- further develop and organize Cyber Europe 2018 and 2020, exploring new dimensions and formats with the aim of further preparing the Member States and Union institutions to cyber crisis likely to occur in the future in the EU;
- integrate existing and future EU-wide crisis management orientations, mechanisms, procedures and tools within the framework of Cyber Europe exercises, in particular the CSIRT network foreseen in the NIS Directive;
- contribute actively to the implementation of the blueprint by supporting MS in implementing into national crisis management frameworks EU-level orientations, mechanisms, procedures and tools;
- integrate existing and future EU-wide crisis management orientations, mechanisms, procedures and tools within the already existing crisis management framework of the MS;
- follow up closely the development of the CEF Cybersecurity DSI CSP and ensure the smooth handover to ENISA and adoption by the CSIRT community;
- proactively promote its expertise in the field of cyber crisis management and exercises to the benefit of other Union institutions and Member States wishing to develop exercises with a cyber dimension. In doing so, ensure consistency with the Cyber Europe framework;

Guidelines

- maintain its existing structured and sustainable dialogue with national NIS competent authorities;
- support the development of tools and procedures (e.g. technical and operational SOPs) supporting crisis management at EU level, to be tested in the exercises;
- support its activities under Objective 4.2 regarding the CSIRT network to ensure consistency in the development of procedures and tools for daily information exchange to crisis management;
- explore the opportunity to participate as observer to other national or international exercises to draw lessons-learned, as well as to invite observers from other Union institutions and international organisations (e.g. NATO) to observe Cyber Europe, on an ad hoc basis and subject to approval from the Management Board;

- evaluate the impact of the organization of previous exercises and build upon these lessons-learned to support the evolution of future exercises and in particular further develop the exercise platform;

Added-value

- allow the organization of European-wide events, increasing visibility on cybersecurity and on ENISA with other Union institutions, Member States, citizens, businesses, academia;
- continue to reinforce cooperation among Member States and to further develop tools and procedures supporting their response to cross-border crisis, thus raising the overall level of preparedness of the EU;
- contribute to the development of the international dimension of its mandate;
- support its work under objective 2.1 by advising on policy developments related to cyber crisis cooperation at EU level, building upon its long experience of cyber crisis exercises and under objective 3.1 by building upon its cyber crisis expertise to advice on national cyber crisis capacity developments;

2.2.4.2 Multiannual priorities (2018-2020) for Objective 4.2 CSIRT and other NIS community building

Priorities

- provide the secretariat to the CSIRT network foreseen in the NIS directive;
- actively support its functioning with a view of facilitating its establishment, allow quick wins and guarantee the smooth functioning of the network by 2020 supporting tangible cooperation among CSIRTs;
- take advantage of the development of the CSIRT core platform within the framework of the "Connecting European Facility" (CEF) mechanism to support the functioning of the CSIRT network and advice, upon request, Member States' CSIRTs on projects to be proposed within the framework of future CEF call for projects;

Guidelines

- develop a trustworthy and sustainable dialogue with Member States CSIRTs and CERT-EU within the framework;
- liaise its activities with those carried out under objective 4.1 building upon the ENISA's expertise on cyber crisis management, in view of the development of tools and procedures by the CSIRT network from daily information exchange to cyber crisis;

Added-value

- support increased NIS information exchange among CSIRTs and contribute to reinforcing cooperation among Member States in case of incidents or of a crisis, thus contributing to increasing EU's overall preparedness and response capacities;
- build ground for reinforced cooperation in the future;
- support its work under objective 1.2 on threat assessment and objective 3.1 by using the CSIRT network as a for a to promote its efforts towards the reinforcement of on national CSIRT capacities;

2.2.5 Activity 5 – Enabling. Reinforce ENISA's impact

The constant need to adapt to a very dynamic sector, cybersecurity, which have daily new challenges it is itself a challenge for ENISA. For this it is crucial to have adequate internal services to enable the activity and effective management leadership to maintain and react in time and effectively.

ENISA is engaged strength the stakeholder's involvement in the overall ENISA's challenges and develop specific activities to outreach adequately across Europe and at international level.

This activity has two main objectives which are introduced below.

- Objective 5.1. Management and compliance

The Agency will act according to the following key general principles and rules:

  - ENISA will ensure a responsible financial management of its resources within the legal framework. In the next five years, ENISA will continue to improve processes for monitoring financial flows and expects to maintain high level project implementation (commitments) and payment rates.
  - ENISA will guarantee a high level of transparency regarding its internal processes and way of working in line with the defined principles applied to the EU institutions.
  - ENISA will increase and maintain internal IT-security expertise within the Core Operations, 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, Article 2 of the ENISA Regulation).
  - 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.
  - ENISA will continue to see full compliance, following the European Court of Auditors and Internal Audit Service.
  - ENISA will also support the code of Good Administration suggested by the European Ombudsman

- Objective 5.2. Engagement with stakeholders and international activities

As a multiannual objective, ENISA will seek to improve its focus on key activities and engage the higher possible number of relevant stakeholders. This includes the various groups of stakeholders that count with institutional, academia, industry, citizens, etc, for adequate outreach of ENISA's work.

The Agency continuously reinforce the media presence in several communication channels including the web site and with strong emphases in social media and press seeking the appropriate level of outreach activities to take ENISA´s work to all interested and to provide added value to Europe.

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 outreach of the Agency work is essential to create the NIS culture across the several actors in Europe.

The main objectives set are:

- 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, within the Quality Management System, 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 and EU institution level and will focus on issues of real-added value for Europe.

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.

These two main objectives presented above are described from a multiannual perspective in the next sub-sections. Each objective is presented providing priorities for 2018-2020, the guidelines on how to achieve the objectives and the added-value provided by ENISA.

2.2.5.1 Multiannual priorities (2018-2020) for Objective 5.1 Management and compliance

Priorities

- increase and improve the recruitment of new NIS experts and aim with the aim of achieving priorities laid out in the WP;
- develop internal management in view of supporting the development of ENISA's internal expertise as well as ensuring staff's well-being, personal development and professional commitment;
- ensure the responsible financial management of its resources within the financial and legal framework;
- guarantee a high level of transparency regarding its internal processes and working methods;

Guidelines

- propose the alignment of the multiannual staff policy plan with the internal expertise's needs necessary to achieve the WP multiannual priorities;
- improve recruitment effectiveness and internal process, in particular in view of accelerating and smoothing the recruitment process, thus contributing to improving ENISA's internal expertise;
- promote the development sustainable team-work among ENISA's experts;
- continue to offer the recruitment of Second National Experts;
- continue to improve processes for monitoring financial flows and expects to maintain high commitment and payment rates to guaranty full implementation of WP.

Added-value

- improve the general quality and efficiency of ENISA's activities by strengthening the Quality Management System of the Agency;
- support, in particular, the development of structured dialogues with national NIS competent authorities' experts building upon internal experts' teams;

2.2.5.2 Multiannual priorities (2018-2020) for Objective 5.2 Engagement with stakeholders and international relations

Priorities

- increase and improve involvement of Member States' national NIS competent authorities' experts towards the implementation of the WP (stocktaking, involvement in the implementation of outputs);
- proactively engage with other competent Union institutions (e.g. European Commission, other agencies, CERT-EU) in view of identifying possible synergies, avoid redundancy and provide advice building on ENISA's NIS expertise;
- seek to increase and evaluate added-value and impact of its activities with the European NIS community;
- communicate in a transparent manner with stakeholders, in particular with Member States, on activities to be carried out inform them on their implementation;
- when relevant and on an *ad hoc* basis, contribute to the Union's efforts to cooperate with third countries and international organizations to promote international cooperation on NIS;

Guidelines

- when provided by the WP, establish structured and, whenever relevant on a multiannual basis, dialogues with voluntary national Member States' experts in view of delivering its outputs (e.g. working groups such as on cyber crisis cooperation);
- rely upon national Member States when primarily responsible for national public private cooperation, in view of engaging with private sector;
- further develop tools and procedures to facilitate and make transparent involvement of all stakeholders in particular regarding the principles and modalities of the participation and consultation of national NIS competent authorities;
- build in priority upon the Network of Liaison Officers as main exchange point for ENISA and Member States' in view achieving these priorities;
- carry out regular in-depth evaluations in view of assessing mid-long term impact of its action in certain areas of expertise;

Added-value

- build trust and mutual expertise with Member States' experts and other stakeholder's and contribute to reinforce their adherence to and involvement with ENISA's work;
- build trust and cooperation with other Union institutions and contribute to reinforcing their own NIS;
- increase ENISA's understanding on the needs of the European NIS community and in particular of the Member States;
- benefit from the European NIS community's expertise – and in particular from Member States' expertise – thus offering tailored, quality and up-to-date analysis and recommendations with high European added-value;

The Management Board may in the future give further orientations and guidelines on issues related to

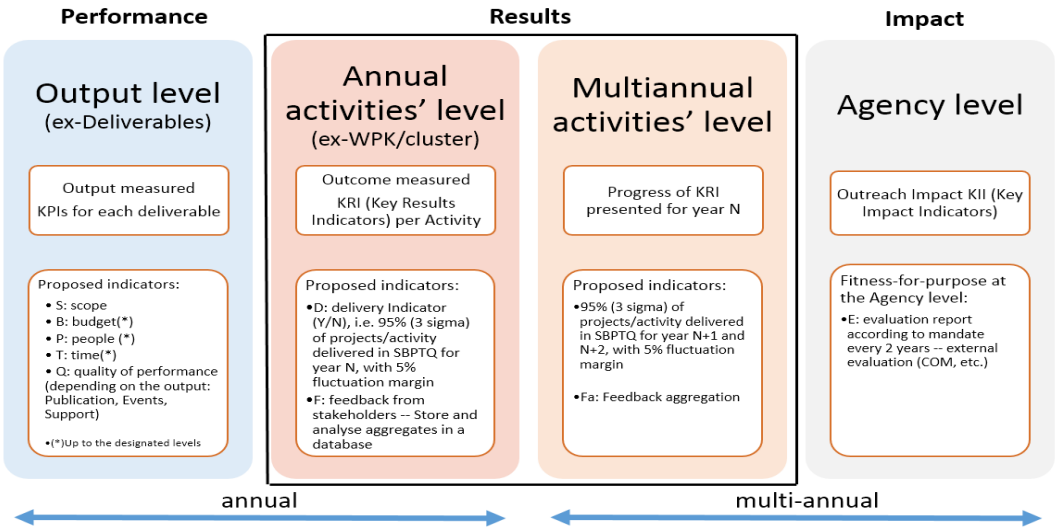
Activity 5, in particular with regard to principles which should underpin international relations of ENISA.

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

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

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

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



Key indicators at ENISA seek to measure:

- Performance that is a concern at the output level when deliverables are produced. Metrics used, are project management-based and they include:

a. Adherence to the scope of the deliverable or project
b. Budget (or financial resources) available to the output or project, remaining within prescribed levels with a ±5% margin
c. People (or human resources) available to the output or project, remaining within prescribed levels with a ±5% margin
d. Time available to carry out the output or project remaining within prescribed levels with a ±5% margin

e. Quality of performance depending on the type of output, according to the classification of output in the work program (being, publication, event, support).

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

a. Delivery indicator aiming at delivery of at least 95% against work program planning. This is equivalent to a 3σ (3 Sigma) organisation (reaching between 93.3% and 99,3%); clearly the Agency has historically proven its operational ability to deliver at much higher level, meeting 6σ (6 Sigma) specification requirements (at 99,99%). However allowing for a 3 Sigma level meets the above-mentioned deviation rate of ±5%.[5] The criteria used, being scope, budget, people, time and quality, they all refer to the proper execution of the project leading up to the production of output. This evaluation is done at the end of the project within ENISA.

b. Following the production process that leads up to an output, feedback from stakeholders is collected on each output. Results are further aggregated on a multi-annual basis by the Agency.

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

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

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

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

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

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

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

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

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

**Publication e.g. methods for security and privacy cost analysis*
***Event e.g. WS on privacy and security*
****Support e.g. NIS portal*

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

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

2.4 Human and financial resource outlook for the years 2018-2020

2.4.1 Overview of the past and current situation.

WP 2018 is following the COM guidelines and MB decisions. The Work Programme is structured following the objectives and the priorities of the Agency as described in the new ENISA strategy.

Regarding ENISA's budget, the variations between the years 2015 and 2016 is neutral. The budget remained with the same amount aligned with COM communications.

While in 2017, a slight increase in the title II was adopted. In 2018, the budget of Title III was optimized in order to increase the budget in operations.

Regarding ENISA's establishment plan, it is noted that ENISA is losing one post in 2018. This fact will have direct impact in the capacity of the agency to deliver and will reduce outputs.

From 2015 until 2018, only some re-organisations were performed in order to maximise the efficiency, effectiveness and use of the posts attributed to the Agency.

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 2018-2020

The distribution of budget and resources for 2018 for the activities A1 to A5 is presented in the charts at the end of this section. 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 quantified. This will be updated in future versions as any other relevant change in the ENISA scope and tasks.

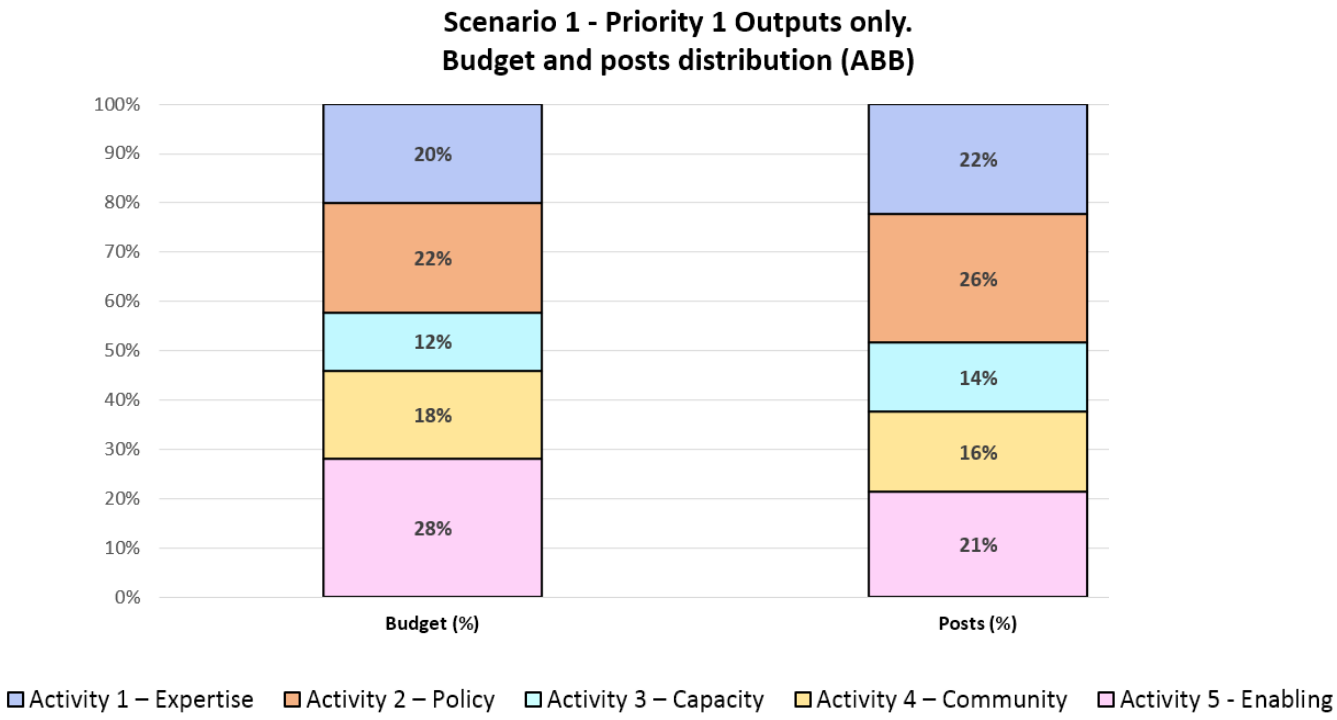
In addition, this version of the work programme takes account of the prioritisation exercise carried out during the consultation with the Management Board.

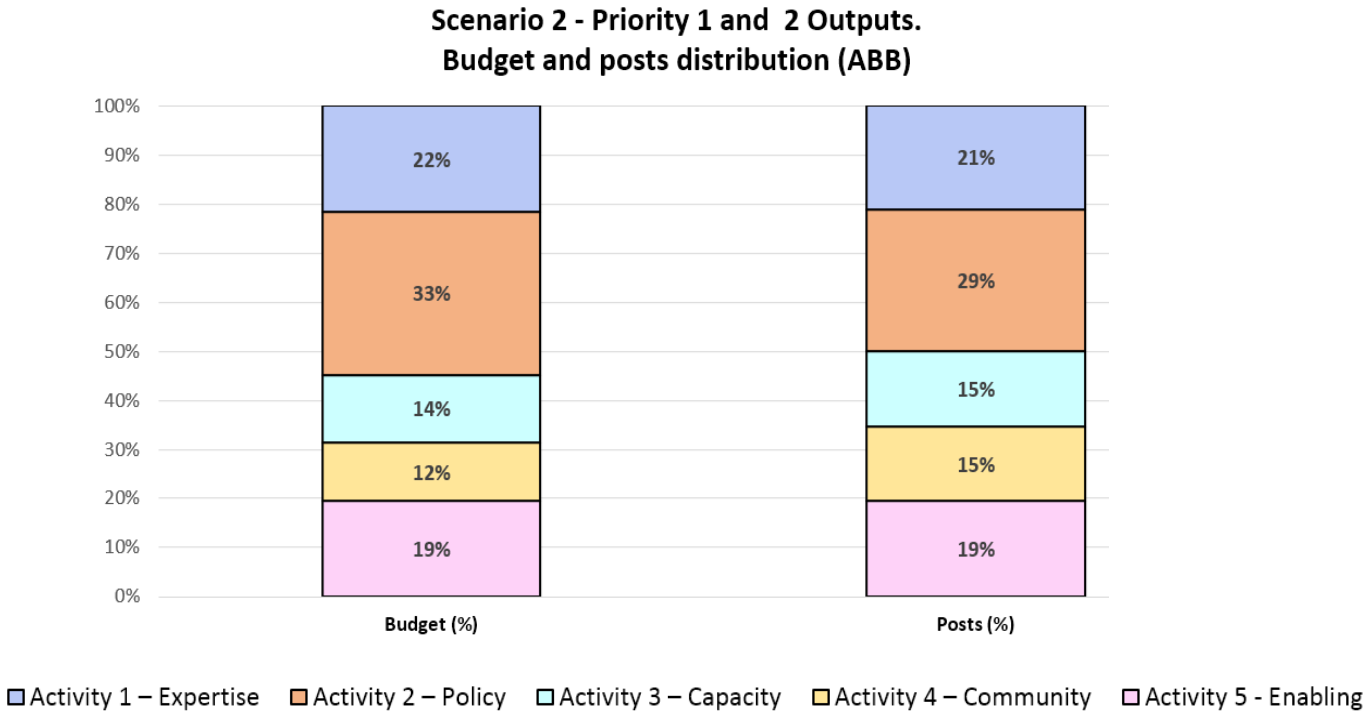
Following the list of outputs in the table 3.6.1, a differentiation between two priorities is done based on the resources ENISA is receiving.

The priorities 1 are covered with budget and establishment plan as 2017. In order to allow ENISA to provide the Outputs that are under priority 2, a request of an addition of 2.5 million euros and of 6 new post is introduced.

For years 2018-2020, the Agency will gradually increase the share of the activity 2, Policy if more resources become available.

The budget and resources allocations for priority 1 within the summary table and Annexes are in line with the COM Multiannual Financial Framework (MAFF) 2014-2020.


Scenario 1 - Priority 1 Outputs only.
Budget and posts distribution (ABB)
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
20%
22%
12%
18%
28%
22%
26%
14%
16%
21%
Budget (%)
Posts (%)
Activity 1 – Expertise
Activity 2 – Policy
Activity 3 – Capacity
Activity 4 – Community
Activity 5 - Enabling


Scenario 2 - Priority 1 and 2 Outputs.
Budget and posts distribution (ABB)
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
22%
33%
14%
12%
19%
21%
29%
15%
15%
19%
Budget (%)
Posts (%)
Activity 1 – Expertise
Activity 2 – Policy
Activity 3 – Capacity
Activity 4 – Community
Activity 5 - Enabling

3. Section III. Work Programme Year 2018

The ENISA Work Programme for the year 2018 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 2018 and link to the multi-annual objectives.

The main outputs/ actions in the specific year, for this case for 2018, 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 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 Network and Information security

The goal of the studies under this objective is to develop recommendations to secure Internet of Things components. This can cover Critical and Smart Infrastructures in light of the NIS Directive and in relation to the perceived level of maturity of each Essential Service Operator and end users.

The good practices for security of Internet of Things will be based on existing guidelines, 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 – Good practices for security of Internet of Things (Priority 1)

IoT is at the core of operations for many Essential Service Operators as defined in the **NIS Directive**, especially considering recent initiatives towards Smart Infrastructures, Industry 4.0[6], 5G[7], Smart Grids[8], etc. IoT security should thus be considered in this context[9].

The Agency will identify and analyse existing security practices and standards in the area of IoT security for CII and smart Infrastructure. ENISA will compare these practices and standards and develop good practices for security of Internet of Things focused with particular focus on the end users impact.

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)[10], the 5G Infrastructure Pubic Private Partnership (5G PPP)[11]).

The Agency will develop targeted IoT case studies to identify risks and vulnerabilities, by defining appropriate attack scenarios, and providing relevant recommendations and good practices. Moreover, it will define IoT security requirements to ensure "security for safety".

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

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).

3.1.2 Objective 1.2. NIS Threat Landscape and Analysis

The Objective 'NIS Threat landscape and Analysis' has three 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.
- Restricted and public Info notes on NIS, covers incidents, significant developments and announcements in the field of cyber security

[6] See https://ec.europa.eu/digital-single-market/en/fourth-industrial-revolution
[7] See https://ec.europa.eu/digital-single-market/en/towards-5g
[8] See https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters
[9] Nevertheless, non-critical operators, who might also be involved in IoT activities, face no regulation and may have little incentive to invest in securing their systems. Considering the particularities of IoT, security should be seen as a primary concern even for the latter operators.
[10] 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
[11] The 5G Infrastructure Pubic Private Partnership (5G PPP), more info available at: https://5g-ppp.eu/

The ENISA Threat Landscape (ETL) report gives 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 2018, 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 (Priority 1)

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. It contains cyber threat intelligence by means of interrelated information objects.

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 visualization and quick availability of threat information will be in the focus in 2018. The ENISA Threat Landscape is being 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. In 2018, this platform will be used for integration of additional relevant information.

In 2018, 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. In carrying out this work, synergies with related experts (i.e. ENISA ETL Stakeholder Group) and vendors (through MoUs) will be maintained and expanded.

3.1.2.2 Output O.1.2.2 – Restricted and public Info notes on NIS (Priority 1)

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 not a response but rather explanatory notes, regarding - for example - events that reach a certain level of public and media attention.

ENISA provides balanced and neutral information regarding such events, covering issues, points of action, mitigation measures, summaries, related practices, etc. Hence, the objective of this work is to provide neutral overview of the state-of-play regarding an incident at a near-time manner.

ENISA's intention is to continue providing Info Notes as a reliable and continuous service to its stakeholders in a timely manner. Info Notes will be logically integrated with the cyber-threat information, building thus a single interconnected knowledge base.

ENISA will further assess the dissemination efficiency of the procured cyber-threat information, both of ETL and Info Note, by assessing its impact of among key stakeholder. This will be done by using appropriate tools for analytics on user access and user enrolment. In addition to the ENISA web site, in 2018 Info Notes will be disseminated via the ENISA ETL platform.

3.1.2.3 Output O.1.2.3 – Support incident reporting activities in the EU (Priority 1)

As incident reporting obligations become more complex, developing efficient reporting schemes across sectors and across geographical borders, thereby making sure they remain simple, pragmatic and relevant for both public and private sector without increasing the cost of operation is one of the objectives of the activities developed by ENISA in this sector.

Current and foreseen activities in this area include:

- Incident notification in the telecom sector (Art. 13a telecom package); currently ENISA support activities in this area by managing the informal Art. 13a Expert Group, keeping in touch with industry and collecting the incidents for the Annual Incident Report. Further support is needed as the telecom package is currently under review and significant improvements will be brought to art. 13a.
- Incident notification for the trust service providers (Art. 19 eIDAS regulation): In 2018 ENISA will continue receiving from the competent authorities the annual incident reports, will analyse them and produce a consolidated, anonymised incident analysis report. In addition, the Agency will continue engaging with the competent authorities towards a harmonised implementation of this article and also engage with the privet stakeholders to better understand the needs and challenges of the sector.
- Incident notification in the context of the NIS Directive: as the NIS directive has entered into force August 2016, with a 2-year timeline for implementation, all stakeholders involved must prepare themselves for this step; further guidelines and support is needed from ENISA to facilitate a smooth transition towards the new provisions. More specifically ENISA can assist stakeholders in developing incident reporting frameworks and procedures, agree on the parameters and thresholds upon which an incident is considered significant as well as the ex-post analysis of the reported data.
- Any legal requirements in relation to reporting stipulated in the draft Regulation on ePrivacy.

ENISA has significant expertise on ***incident reporting*** at the EU level through the work carried out with Member States and telecoms providers on the transposition of Article 13a of the Telecommunications framework Directive of 2009. The Agency also contributed to the interpretation of Article 19 of the eIDAS regulation and now helps trust service providers in implementing this article.

3.1.3 Objective 1.3. Research & Development, Innovation

The actions presented in this Objective are structured in two dimensions. The first dimension covers the ICT standardisation in the EU and aims to assess the existing needs and gaps in the field. 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 (Priority 1)

Building on its own policy work, existing standards and the requirements of the Member States, this activity will provide guidance to implement existing standards and an overview of gaps that are likely to result in future standardisation. At all times new requirements and priorities associated with the emerging legal framework and its transposition or implementation in the Member States will be taken into account, including NIS Directive, the Commission's communication on cPPP, automated processes and systems etc. This output will seek to analyse the gaps and provide guidelines for, in particular, the development or repositioning of standards, facilitation of the adoption of standards and governance of EU standardisation in the area of NIS. Bringing in its concrete NIS policy expertise, ENISA will produce "how to" and "what else" guides in an effort to contribute to the valuable European standardisation work.

In carrying out this work, ENISA will consult with the Member States, industry and standards developing organisations (e.g. ETSI, CEN, CENELEC), as well as Commission services and Agencies with policy competence thereto as appropriate.

3.1.3.2 Output O.1.3.2 – Priorities for EU Research & Development (Priority 1)

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.

Additionally, ENISA will continue supporting and advising the Commission as well as designated organisations in this area (e.g. ECSO) as well as in the Member States to meet their goals by bringing in its concrete NIS policy expertise.

3.1.4 Objective 1.4. Response to Article 14 Requests under Expertise Activity

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

3.1.4.1 Output O.1.4.1 – Response to Requests under Expertise Activity (Priority 1)

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.

3.1.5 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 –Good practices for security of Internet of Things	P: Good practices for security of Internet of Things E: IoT security workshop	Engage 5 leading IoT developers and 5 leading stakeholders from 5 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, Q4, information offering during the year.	Engage more than 10 MS in discussions and work related to implementing NISD incident reporting
Output O.1.2.2 – Restricted and public Info notes on NIS	P: Info notes on NIS	Coverage of all major incidents relevant to EU NIS policy priorities. Expand coverage to all key ENISA stakeholder groups.
Output O.1.2.3 – Support Incident reporting activities in EU	P: Annual Incident Analysis Report for the Telecom Sector, Q4 E: Art. 13a[12] meeting P: Annual Incident Analysis Report for the Trust Service Providers, Q4 E: Art. 19[13] meetings S: Support MS and the EC in implementing the NIS directive incident reporting requirements P: Incident Reporting Framework for the NISD, Q4	More than 20 NRAs/EU MS contribute in preparation of the report (Art. 13a) 3 workshops per year (Art. 13a) More than 10 SBs/EU MS contribute in preparation of the report (Art. 19) 2 workshops per year (Art. 19) Engage more than 10 MS in discussions and work related to implementing NISD incident reporting
Objective 1.3. Research & Development, Innovation		
Output O.1.3.1 – Guidelines for the European standardisation in the field of ICT security	P: Guidance and gaps analysis for European standardisation in NIS, Q4.	Participation in drafting and review of the guidelines of at least 5 representatives of European Standard Developing Organizations (SDOs) and relevant services of the European Commission
Output O.1.3.2 – Priorities for EU Research & Development	P: Study and support activities on priorities for EU research & development in the context of H2020, Q4	Involving at least 5 representatives from different stakeholders – research, industry, governmental
Objective 1.4. Response to Article 14 Requests under Expertise Activity		
Output O.1.4.1 – Response to Requests under Expertise Activity	S: Answers to requests.	

[12] Article 13a of the amended Framework Directive 2002/21/EC (2002).
[13] Article 19 of the eIDAS regulation (2014).

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

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

3.2.1 Objective 2.1. Supporting EU policy development

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

In the policy development area the Agency will co-operate with public and private stakeholders to develop insights, consolidate views and provide recommendations in areas where the EU take action to further develop its policy. Examples include Certification, the DSM and the evolving role of the cPPP is likely to give raise to interesting input to the policy area.

3.2.1.1 Output O.2.1.1 – Support the policy discussions in the area of certification of products and services (Priority 1)

Taking due account of recent legislative and policy developments, such as the adoption of the NIS Directive and the publication of the Commission Communication "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry", the Agency will continue to support the Commission and the Member States (taking account of the “cybersecurity Council conclusions”) in identifying a certification framework for ICT security products and services by promoting 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 join ongoing initiatives and it will seek to stimulate standardisation initiatives with SDOs (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.

Policy areas to be considered include but are not limited to mapping existing European certification schemes, recommendations on next steps to take at EU level, analysis of impact of certification for manufacturers and end-users etc. ENISA will carry out support activities in the area of certification and if needed, it will organise its own workshops bringing together key stakeholders.

3.2.1.2 Output O.2.1.2 – Towards a framework for policy development in the cybersecurity (Priority 1)

The digitalisation of several critical and noncritical sectors as well as the emergence of new technologies such as IoT requires a coherent policy framework on NIS. Such a policy framework is likely to allow integrating existing policies (e.g. NISD, DSM, etc.) among themselves and adding new ones (e.g. IoT policy, cPPP, etc.) towards a common and integrated framework.

ENISA will take stock of existing policy initiatives and assess the needs for new and emerging areas. In co-operation with MS and private sector the Agency will develop the key elements of such a framework and validate the idea with all relevant stakeholders.

3.2.1.3 Output O.2.1.3 – Towards a Digital Single Market for high quality NIS products and services (Priority 2)

ENISA will continue supporting the Commission in the development of the Digital Single Market (DSM) in Europe from the NIS perspective, notably by supporting start-ups and innovative companies.

The Agency, building upon its previous work on DSM (WP 2016 and 2017) and on the basis of Commission studies and conclusions, will investigate how start-ups can support the NIS market, which are the barriers they face and what opportunities they are offered. To achieve this the Agency will liaise with the Commission, MS, and relevant public and private sector organisations in order to collect critical input and insights.

In that context cyber insurance might prove a good incentive for businesses to invest in information security. To investigate its potential, ENISA has taken stock of existing public and private approaches to cyber insurance and has already identified the barriers, 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).

Through building up to the work done the previous year on a common language for Cyber Insurance contracts, ENISA will put them in practice and investigate how the clauses can meet the requirements of different critical sectors. ENISA will investigate the priorities and the needs for cyber insurance per sector, will analyse the findings and issue recommendations for targeted stakeholders.

The report will include strategic recommendations to the stakeholders categorised per sector. 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 4 main topics:

- Contribute to EU policy in the area of privacy and electronic communications
- Support the implementation of the eIDAS Regulation.
- Support the implementation of GDPR Regulation
- Support the implementation guidelines for the Implementation of Mandatory Incident Reporting in the context of the NIS Directive

In the policy implementation area, the Agency will co-operate with NRAs, competent authorities and private stakeholders to implement existing policies of the EU. Emphasis is given on harmonisation support and guidance that would allow public and private sector to efficiently implement the EU policies. Examples include NIS Directive, Telecom Package, eIDAS, GDPR and ePrivacy Directive.

3.2.2.1 Output O.2.2.1 – Recommendations supporting implementation of the eIDAS Regulation (Priority 1)

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. Aspects to be covered will be agreed with the EC and MS through the eIDAS experts group. Specific implementation guidelines and technical recommendations for whose approval the eIDAS expert group will be consulted will address operational aspects of Trust Service Providers, Conformity Assessment Bodies and Supervisory Authorities while accumulating the experience of best-practises and state-of the art progress, seeking to emphasise

implementation and interoperability aspects. These recommendations will complement the existing knowledge base that ENISA created for the trust service providers. At the same time, ENISA will take utmost account of recommendations and standards being developed by CEN/ETSI/ISO and seek to avoid both duplication of work and potentially opposing approaches.

3.2.2.2 Output O.2.2.2 – Supporting the Implementation of the NIS Directive (Priority 1)

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.

The Agency can analyse specific issues identified in the Work Programme of the Cooperation group and develop recommendations and suggestions that would allow Commission and Member States to take informed decision on NIS matters.

Also ENISA will continue its efforts supporting MS in the identification of OES. Through stock taking and analysis ENISA will identify common approaches, schemes and good practices. The Agency will validate them with relevant public and private sector entities to make sure they meet the needs and requirements of both public 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.

3.2.2.3 Output O.2.2.3 – Baseline Security Recommendations for the OES Sectors and DSPs (Priority 1)

ENISA will address the needs of DSPs and OES to check compliance against the security requirements set by the NISD by developing voluntary self-assess schemes that would be fully compatible with the provisions of the implementing acts and/or the NISD. ENISA, building on its expertise on security requirements developed for DSPs and OESs, will work closely with Member States and the private sector to identify such cost effective practices and maturity security frameworks that would constitute the self-assessment frameworks.

In deriving such a set of common mechanisms, 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 DSPs and OES.

The Agency will also compare and validate the results with other relevant approaches in the area of Operators of Essential Services (e.g. C2M2, NICE-CMM) or the generic IT models (e.g. ISO 27001) and interact with all important stakeholders from public as well as the private sector.

The proper validation of the proposed self-assessment practices would pave the way for wide, de-facto, tacit adoption of them and thus set the basis for sufficient convergence across the EU MS.

3.2.2.4 Output O.2.2.4 – Supporting the Payment Services Directive (PSD) Implementation (Priority 1)

PSD 2 was adopted and will be transposed by MS latest by January 2018. EBA, as responsible Agency, in co-operation with ENISA and relevant competent authorities of MS develop guidelines for Operational and Security Risk management for Payment Service Providers (PSPs). These guidelines define the framework

with the appropriate mitigation measures and control mechanisms to manage the operational and security risks relating to the payment services they provide.

ENISA, drawing from its expertise in the field of risk management, min security measures, resilience, secure authentication mechanisms and others will contribute to this work making sure there is enough consistency between this and other related frameworks, e.g. NISD.

In this context the Agency will continue its co-operation with EBA and ECB and Member States' competent authorities on other cyber security related topics including mandatory incident reporting, use of cloud computing, mobile payments and use of blockchain by the finance sector. Also ENISA through this co-operation with these stakeholders, will align, as much as, this work with the NISD implementation because Finance is one of the key sector of this Directive.

3.2.2.5 Output O.2.2.5 – Contribute to the EU policy in the area of electronic communications sector, privacy and data protection (Priority 2)

The Agency will continue contributing to the amended framework for eCommunications.

The Agency will liaise with NRAs in terms of harmonising to the extent possible the implementation of article 13a (incident reporting, baseline security requirements, root causes, trusted information sharing).

The Agency will support also the private sector to identify challenges and propose good practices for them.

It will also collaborate with EU Commission for the adoption of the new Telecom Framework and contribute to the NIS related aspects of it. Emphasis will be given on transferring the experiences gained so far in the area of article 13a and also on aligning as much as possible this policy with the NIS Directive.

ENISA will continue promoting trust and security in digital services in the DSM by means of technical recommendations on the implementation of EU legislation addressing privacy and personal data protection. In particular, technical implementation of GDPR and ePrivacy Directive will be addressed. ENISA will support the implementation of the regulatory aspects by acting as policy, technical and organisational advisor of the Commission in the area of security of personal data and confidentiality of communications while seeking to elaborate privacy certification schemes and data protection seals. Moreover, ENISA will provide recommendations on shaping technology according to GDPR provisions, such as for example data security, data minimisation, anonymisation and pseudonymisation. The Annual Privacy Forum (APF) will be used as an instrument to bring together key communities in the broader area of privacy and data protection and identify best practises and future challenges both at regulatory and technological levels. Co-operation activities with EDPS and national Data Protection Authorities will be continued and further enhanced.

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

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

3.2.3.1 Output O.2.3.1 – Response to Requests under Policy Activity (Priority 1)

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 certification of products and services	P: Towards a framework for the common European ICT products security certification and ways to accelerate its implementation, Q4 E: 4 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 - Towards a framework for policy development in the cybersecurity	P: Towards a framework for policy development in the cybersecurity, Q4 E: Workshop with stakeholders, Q3	More than 10 private companies and 10 EU MS representatives contribute to/participate in the activity
Output O.2.1.3 - Towards a Digital Single Market for high quality NIS products and services	P: Guidelines on how the DSM strategy can support start-ups P: Recommendations on cyber insurance for critical sectors E: 2 workshops with stakeholders, Q2-Q4 S: Support the Commission in their DSM policy, Q1-Q4	More than 3 leading essential service operators per sector take part in the study More than 10 EU start-ups on NIS to be involved in the study
Objective 2.2. Supporting EU policy implementation		
Output O.2.2.1 – 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. E: Trust Services Forum, Q2	Engaging at least 5 representatives from different bodies/MS in the validation of the recommendations. Review and acceptance by at least 10 stakeholders (trust service providers, conformity assessment bodies, and supervisory authorities) from at least 5 MS. More than 50 stakeholders participate in the activity
Output O.2.2.2 – Supporting the Implementation of the NIS Directive	P: Recommendations and Good Practices on reviewing DSPs' compliance to the NISD security requirements, Q4	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.

	P: Recommendations and Good Practices on reviewing OES compliance to the NISD security requirements, Q4 P: Recommendations and Good Practices on the criteria for choosing OESs Q4 Guidelines on criteria for determining the significance of the impact of an incident concerning OESs in Q1 2018 (See article 6 (2) of the NIS-D and Recital 38 for ENISA) S: Support to the work of the Cooperation Group by providing in due time advice and expertise on deliverables identified by the Group e.g. on guidelines concerning the modalities (format and procedure) of notification requirements for DSPs, and on guidelines concerning the mandatory sharing of information between affected Member States (Art 14 (5) and Art 16 (6)) in Q1/2018 S: Support the Cooperation Group E: 3 workshops related to the tasks of the NISD S: Contribute to the activities of MS and private sector in the area of OES	10 OES participate in the workshops. 10 MS participate in the activity.
Output O.2.2.3 - Baseline Security Recommendations for the OES Sectors and DSPs	P: Criteria for DSP self-assessment against NISD security requirements, Q4 P: Criteria for OES self-assessment against NISD security requirements, Q4 E: 2 workshops with stakeholders from OES sectors, Q2-Q4	Engage 20 MS in the development of self-assessment criteria for OES and DSPs Engage 15 private sector stakeholders in the development of compliance criteria for OES and DSPs More than 10 MS and 15 OES participate in the workshops.
Output O.2.2.4 - Supporting the Payment Services Directive (PSD) implementation	P: Good practices on the implementation of regulatory technical standards S: Support the EBA and ECB in the implementation of the PSD2 E: 2 workshops with relevant stakeholders (and EGFI, EBA) (Q2-Q4)	Engaging at least 15 Member States regulatory bodies and at least 10 private financial institution in this study.
Output O.2.2.5 – Contribute to EU policy in the area of electronic	E: 2 workshops with relevant stakeholders, Q1-Q4	Engage 20 providers and 20 national bodies in the activity

communications sector, privacy and data protection	P: Recommendations on shaping technology according to GDPR provisions, Q4 P: Reinforcing trust and security in the area of electronic communications and online services. E: Q2, APF' 2018	At least 5 representatives from different bodies/MS participate in the preparation of the recommendations. At least 5 representatives from different bodies/MS participate in the preparation of the recommendations. More than 60 participants from relevant communities
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.	

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 program. In 2018, 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 – Update and provide technical trainings for MS and EU bodies (Priority 1)

In 2018 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 2018, 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.

3.3.1.2 Output O.3.1.2 – Support EU MS in the development and assessment of NCSS (Priority 1)

The NIS Directive sets as priority for the MS to adopt a national NIS strategy and to monitor its implementation. 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 existing good practices in the related areas area and offer targeted and focused assistance on specific NCSS objectives (e.g. CIIP, creation of PPPs etc). 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 collected on the NIS objectives each MS targets. ENISA will further enhance the material provided in the e-Learning tool launched in 2015.

3.3.1.3 Output O.3.1.3 – Support EU MS in their Incident Response Development (Priority 1)

In 2018 ENISA will concentrate its efforts on assisting MS to support their incident response capabilities by providing a state of the art view on the CSIRT landscape and development in Europe. In close cooperation with the NISD CSIRT network, the agency will support the development of Member States' national incident response capabilities by providing recommendations on key dimensions of NIS capability building with a focus on the development and efficient functioning of national and sectorial CSIRTs. ENISA will as well offer, upon their request, direct support to single Member States to assess and improve their incident response capabilities.

The main objectives of this output in 2018 is to help MS and another ENISA's incident response stakeholders, such as the EU institutions, bodies and agencies, to develop, extend and deploy 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 CSIRT baseline capabilities and maturity framework. As a continuous effort ENISA will continue supporting cross-border CSIRT community projects, tools development as well as the global dialog about common definitions and maturity framework in the incident response domain.

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, contribute to capacity building in areas like training, awareness and educational material. as well as information notes on threats, risks and incidents with a view of making European's networks more secure.

3.3.2.1 Output O.3.2.1 – NIS Directive transposition (Priority 1)

According to article 25 (1) of the NIS Directive, the Member States shall adopt and publish, by 9 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. In order to support the Member States with this task, ENISA will take stock of the NISD implementation status together with other relevant stakeholders (e.g. sectorial NIS regulations responsible). Then the collected data will be organised according to specific maturity criteria (e.g. C2M2), in order for ENISA to identify lessons learnt and recommend good practices to the Member States, Cooperation Group and the Commission concerning the Directive transposition process. This, will further strengthen the cooperation amongst Members States and at EU level, during the period of transposition and it will provide them with the appropriate knowledge for the successful completion of the task.

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 (Priority 2)

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.

3.3.3 Objective 3.3. Assist private sector capacity building.

While ENISA supports capacity building, the private sector is a key target area. In 2018 work on cybersecurity culture, cyber hygiene as well as aspects associated with liability and insurance are going to be analysed.

There are no identified activities for this objective in 2018.

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 (Priority 1)

In order to promote capacity building and awareness in NIS among emerging young generation of cyber security experts in EU MS, in 2018 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 2018 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 (Priority 1)

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 2018 ENISA intends to explore ways to make use of alternative communication tools such as social media to reach the EU Citizens. Previously proposed pillars remain: support a multi-stakeholder governance approach; encouraging 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 (Priority 1)

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 - 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 (Cyber Crisis Management), 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 5 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.3.1.2 – Support EU MS in the development and assessment of NCSS	P: Update: Tool for evaluating NIS strategies (Q1-Q4) P: Updated - EU's map on NCSS S: support member states in their NIS strategy activities E: Workshops with EU MS on NCSS development, Q2-Q4	Engage at least 20 EU MS in this activity / workshop.
Output O.3.1.3 – Support EU MS in their Incident Response Development	P: Q4: CSIRTs landscape in Europe	CSIRTs landscape report based on input from at least 30 European countries Two inventory updates (Q2, Q4)

	P: Q2 and Q4: CSIRT online Inventory update – European interactive map of CSIRTs E: Q2: Annual ENISA technical CSIRT workshop (13th workshop 'CSIRTs in Europe') P: Q4: CSIRT maturity: common definitions and terminology S: Q1-Q4, continue activities and involvement in CSIRT structures (e.g. FIRST, TF-CSIRT, NATO NCIRC)	During 2018, support provided at least for two incident response stakeholders to enhance their CSIRT baseline capabilities or maturity. At least fifteen MSs participating in the technical CSIRT workshop. At least two international CSIRT entities involved in the CSIRT maturity: common definitions and terminology project
Objective 3.2. Support EU institutions' capacity building.		
Output O.3.2.1 – NIS Directive transposition	P: NISD transposition status report E: workshop S: Cooperation Group support	At least 15 MS participate in the stock taking exercise.
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: 1 workshop with relevant stakeholders, Q2-Q4	At least 3 EU institutions and 5 MS take part in the activity.
Objective 3.3. Assist private sector capacity building.		
-	-	-
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.	

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 by the CEF Governance Board in relation to the core service platform (CSP) developed in the context of the Connecting Europe Facilities (CEF) programme.

Last, growing upon its expertise on cyber crisis management, cyber crisis simulations and cooperation activities within the European cybersecurity operational communities, ENISA will support actively the implementation of the cyber crisis cooperation blueprint.

3.4.1.1 Output O.4.1.1 – Cyber Europe 2018 (Priority 1)

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 CE2016.

CE2018 will focus on testing capabilities and procedures, namely large-scale incident management cooperation procedures at EU and national-levels. The crisis escalation scenario will be realistic and focused in order to capture better how incidents are managed and cooperation happens in real-life. The exercise will include explicit scenarios for the CSIRT Network set up under the NIS Directive.

The high-level exercise program brief will include the strategic dimensions of the exercise will be prepared based on the lessons learned from CE2016, to drive the whole planning process. The exercise brief will be given for comments and approval to ENISA's Management Board after consultation with the MS Cooperation Group and the CSIRT Network 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) in 2017-18. ENISA will involve the group of planners in the relevant planning steps and take into account their input towards a consented plan. The exercise planning will avoid overlaps with other major related activities.

ENISA will consult MS and seek agreement of ENISA's Management Board after consultation with the Cooperation Group and the CSIRT Network set up under the NIS Directive on a possible joint EU-NATO cyber exercise in the coming year.

3.4.1.2 Output O.4.1.2 - Planning and organisation of EuroSOPEx 2018 (Priority 2)

In 2017 ENISA organised the third EuroSOPEx exercise (first was in 2012, second in 2016) dedicated to raise trust and cooperation between the EU national and governmental CSIRTs that participate in the CSIRT Network. In 2018 ENISA will organise the EuroSOPEx exercise for the EU public authorities' points of contact, as these will be represented in the CSIRT Network only to keep and even raise the momentum of cooperation in between them.

As in the previous year the exercise will be planned with the support of representatives from the involved organisations. The exercise is expected again to have as high-level goals to raise awareness of cooperation

procedures, train participants in using the cooperation infrastructures, such as the communication and information sharing and ultimately contribute to increase trust within the CSIRT Network. Guidance should be found in the CSIRT network on planning the exercise. There will not be any private nor other entities involved in this exercise.

3.4.1.3 Output O.4.1.3 – Lessons learnt and advice related to cyber crisis cooperation (Priority 1)

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 (CSIRT Network).

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.

ENISA will also support the EU Commission and Member States in the deployment of the EU Cyber Crisis Cooperation blueprint to enhance cross-border cooperation related to preparedness for a large-scale cyber incident, as presented in Communication COM (2016) 410 on Strengthening Europe's Cyber Resilience System. ENISA will review and highlight the cyber crisis management good practices. Already existing schemes will build the basis of this work, in particular the work of the European Cyber Crises Cooperation Framework (ECCCF). In addition, the activities will be matched with and possibly integrated into traditional crisis cooperation such as the Integrated Political Crisis Response (IPCR) arrangements.

3.4.1.4 Output O.4.1.4 – Support activities for Cyber Exercise Planning and Cyber Crisis Management (Priority 1)

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. The CEP will be constantly improved based on suggestions and lessons learnt from Cyber Europe Exercises series in order to improve usability.

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. The CEP platform opens new opportunities for ENISA to enlarge the user base and thus offer to the operational cyber security communities opportunities to exercise and gain experience and knowledge. One way to enlarge the user base, and thus increase the impact of ENISA, is to offer new and interesting functionalities that will attract new registrations to CEP. Smaller exercises can reuse previously developed material and virtual infrastructures of CEP to design cyber security competitions.

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

In 2018 ENISA will have to prepare to manage and operate the centralised components of the CEF Cybersecurity DSI Core Service Platform (CSP) 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 end 2018 ENISA must be ready to fully assume the responsibility for the management, maintenance and further development of the CEF Cybersecurity DSI CSP, whose handover to ENISA will be completed by 2019.

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.

3.4.2 Objective 4.2. CSIRT and other NIS community building.

ENISA will continue to support the cooperation and information exchange among CSIRTs in the European Union. As part of this activity, ENISA will continue providing the secretariat for the NISD CSIRTs network and will pro-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. ENISA will also support and assure coherent planning of other relevant activities for the CSIRTs network members such as Cyber Europe exercise and the development of EU-level cooperation with standard operation procedures for CSIRTs as well as cross-border CSIRT community projects and tools development following from 3.3.1.3.

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

3.4.2.1 Output O.4.2.1 - EU CSIRT network secretariat and support for EU CSIRT network community building (Priority 1)

ENISA will continue its support to 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 continue its tasks as the secretariat of the CSIRTs network and actively support its functioning by suggesting ways to improve cooperation and trust building among CSIRTs. The agency will also support this cooperation by developing and providing guidance and good practices in the area of operational community efforts, such as on information exchange and secure communication, on request by the members of the CSIRT Network. 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 according to the CSIRTs network own work programme (action plan 2017-2022).

In addition, ENISA will take an active role to support CSIRTs in the CSIRTs network in activities relevant to the CEF work programme. ENISA will actively support teams in deployment and use 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 CSIRT Network.

Trust is an important asset for CSIRTs operations therefore ENISA will continue to improve the level of trust in the network by providing trust building exercises and events in coordination with the CSIRTs network governance.

The agency will further improve, develop and secure the CSIRTs network infrastructure for its member's smooth collaboration and administration use (CSIRT network portal and other communication means).

3.4.2.2 Output O.4.2.2 – Support the fight against cybercrime and collaboration between CSIRTs and LEA (Priority 1)

In 2018, 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 exchange among different stakeholders in operational communities in Europe. In detail, ENISA will continue its effort to support the EU wide objective on fight against cybercrime by liaising with various stakeholders at EU (e.g. EUROPOL), as well as at MS level.

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 (Priority 1)

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 4.1. Cyber crisis cooperation		
Output O.4.1.1 –Cyber Europe 2018	E: Exercise, Q4 P: Report on after action activities (restricted), Q4	At least 80% EU/ EFTA Member States and countries confirm their support for Cyber Europe 2018
Output O.4.1.2 Planning and organisation of EuroSOPEx 2018	E: Exercise, Q4.	At least 80% of the CSIRTs in the CSIRT Network confirm their support for EuroSOPEx 2018
Output O.4.1.3 Lessons learnt and advice related to cyber crisis cooperation	S: support for the Cyber SOPs editorial team of the CSIRT network, Q4. P: Good Practices in Cyber Crisis Cooperation and Management, Q4	At least 80% of the participating MS agree to the developed operational procedures
Output O.4.1.4 Support activities for Cyber Exercise Planning and Cyber Crisis Management	S: Support for CEP, Q4. S: Support CEF (including ENISA handover roadmap) and contribution to the activities of the Cybersecurity DSI Governance Board (Q4).	At least 70% of CEP users evaluate it positively Over 80% of the countries in the Governance Board approve the handover roadmap.
Objective 4.2. CSIRT and other NIS community building.		
Output O.4.2.1 – EU CSIRT network secretariat and support for EU CSIRT network community building	S: provide CSIRTs network secretariat tasks (e.g. logistics, organisation of the meeting, agenda management, meeting minutes; conference calls)	Engage all 28 MS designated CSIRTs and CERT-EU in the activities described in the network work programme (action plan 2017-2022)

	E: network meetings organisation and support (maximum 3 events) S: Q1-Q4: Facilitate CSIRTs regular participation in the EU CSIRT network events S: Q1-Q4, EU CSIRT network communication support S: Q1-Q4, Improve CSIRTs network portal functions and security E: trust building exercise (co-located with the regular network meeting) P: Q4 Guidelines for network specific information exchange and secure communication issues S: provide translation service for CSIRTs network national documentation (budget limitation)	28MS dedicated CSIRTs and CERT-EU participated in CSIRT network regular meetings Work of ENISA successfully reflected by existing CSIRT communities (FIRST, TF-CSIRT, EU CSIRT network) and other national CSIRT networks. Input received from at least 20 CSIRTs network teams for the project 'Guidelines for network specific…'. Translation services provided for at least 20 national documents provided by the CSIRTs network member (subject to the budget availability).
Output O.4.2.2 – Support the fight against cybercrime and collaboration between CSIRTs and LEA	P: Current cooperation between CSIRT and LEA community and on possible ways to further enhance their co-operation, Q4 E: Q3, annual ENISA/EC3 workshop for national and governmental CSIRTs and their LEA counterparts	At least 5 MS CSIRT representatives and 5 MS LEA representatives participate in the preparation of the report At least 15 MS participate at ENISA/EC3 annual workshop
Objective 4.3. Response to Article 14 Requests under Community Activity		
Output O.4.3.1. Response to Requests under Community Building Activity	S: Answers to requests.	

3.5 Activity 5 – Enabling. Reinforce ENISA's impact

Activity 5 covers two main objectives:

- Management and compliance;
- Engagement with stakeholders and international activities.

3.5.1 Objective 5.1. Management and compliance

3.5.1.1 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** Unit (EDO) was established. The tasks covered by EDO include: Policy advice, Legal advice, Management Board Secretariat and Coordination and Controlling of the Work Programme.

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, including the management of the MB Portal.

The EDO supports the ED in his relations with the press.

In 2018, 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, following the applicable rules, one ordinary meeting will be organised during 2018 and informal meetings will be held as necessary. The MB Portal will be supported for EB and MB. In relation to the Executive Board, one formal meeting will be organised per quarter and informal meetings when necessary.

The **Stakeholder Relations and Administration Department** (SRAD) oversees a variety of programs, projects and services relating to the overall management of the Agency, supporting the Executive Director Decision is areas as personnel, finance, communications, press, purchasing, technology, facilities management, health, safety, security, protocol, liaison with local authorities, etc.

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. This also includes coordination with the European Commission Internal Audit Service, European Court of Auditors, European Ombudsman, European Commission European Anti-Fraud Office, EU DG HR, EU DG BUDGE, DG CNECT, etc. All internal policies related to transparency, anti-fraud policy, whistle-blowers protection, declarations of interests, etc. are addressed within this activity.

SRAD strives to maintain and increase the efficiency and effectives of the Agency, and provide continuous contribution to the ENISA strategy both internally and externally seeking the optimal solutions for delivering on the mandate of ENISA and provide the required assurance in compliance.

The aim is to enable the Agency with adequate and modern procedures and tools to minimize the resources across the agency maximizing the intended delivery of the work program and statutory commitments.

3.5.1.2 Internal control

ENISA implemented a Quality Management System (QMS) of the Agency to support its regulatory and strategic goals by means of a quality management approach. ENISA is following the ISO 9001:2015 standards as they are designed to help organizations 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.

3.5.1.3 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 2 platforms, maximise data sharing, make applications available in a secure way on the most widely used mobile devices, and, to progressively move the Agency's IT infrastructure to the Cloud. 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-2018 it is expected that all business applications will be securely available on the most widely used mobile devices. By this timeframe the platform consolidation should be complete and mature, with adequate, flexible and advance reporting and monitoring tools. Is expected that 2018 will consolidate the support technology in the Agency with modern, adequate and flexible business applications.

Task	Objective	Level of completion 2018	Level of completion 2019	Level of completion 2020
Consolidate systems and applications on a maximum of 2 platforms	Efficiency	90%	90%	90%
Maximise data sharing	Efficiency	70%	80%	80%
Move the Agency's IT infrastructure progressively to the Cloud	Efficiency	90%	95%	95%
Business applications will be securely available on the most widely used mobile devices.	Availability	95%	95%	95%
Continuous Operations	Availability	98,5%	99%	99%

3.5.1.4 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 2018, 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 2018 include high budget commitment and payment rates, low number of budget transfers during the year, planned and justified carry overs, and reduced average payment delay.

Task	Objective	Level of completion 2018	Level of completion 2019	Level of completion 2020
Deployment of new financial information systems	Efficiency, better reporting, information quickly provided	95%	95%	95%
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	90%	90%	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	98%	98%	98%

3.5.1.5 Human Resources

The ultimate goal of HR is to attract, select, develop and retain highly qualified staff, to put in place optimal organisational structures, to promote a safe working environment, to create a culture that reflects ENISA's values in which staff can give their best in achieving the organisation's objectives. By offering a broad array of services (Recruitment, Performance management, L&D, Career management, working conditions, Social rights, etc.) HR's objective is to deliver a successful day-to-day management of ENISA personal and external staff (e.g. trainees) in compliance with the Staff Regulations. This is why, more efforts will be put in developing and deploying tools and policy to streamline the efficiency of the different HR processes.

Task	Objective	Level of completion 2018	Level of completion 2019	Level of completion 2020
Posts on the Agency establishment plan filled	Minimum 90 % of the recruitment target reached	85%	85%	90%
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)	2 months	2 months	2 months
Turnover of staff	Reduce the turnover of TA's to less than 10%	<16%	<15%	<15%

3.5.1.6 Legal affairs, data protection and information security coordination

3.5.1.6.1 Legal Affairs

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 to the European Ombudsman and representing the Agency before the European Court of Justice, General Court or Civil Service Tribunal.

3.5.1.6.2 Data Protection Compliance tasks and Data protection Office

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

- Inform and advise ENISA of its obligations pursuant to Regulation 45/2001/EC and document this activity and the responses received.
- Monitor the implementation and application of ENISA's policies in relation to the protection of personal data.
- Monitor the implementation and application of Regulation 45/2001/EC at ENISA, including the requirements for data security, information of data subjects and their requests in exercising their rights under the Regulation, as well as the requirements for prior check or prior consultation with EDPS.
- Monitor the documentation, notification and communication of personal data in the context of ENISA's operations.
- Act as ENISA's contact point for EDPS on issues related to the processing of personal data; co-operate and consult with EPDS whenever needed.

3.5.1.6.3 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 2018 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.

3.5.2 Objective 5.2. Engagement with stakeholders and international activities

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

- Stakeholders Communication and Dissemination Activities
- Outreach and Image building activities
- Permanent Stakeholders Group
- National Liaison Officer Network

3.5.2.1 Stakeholders communication and dissemination activities

In 2018, 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.

3.5.2.1.1 Dissemination and Outreach

The Agency will continue developing various tools and channels including the web site 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.

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.

3.5.2.1.2 Internal communications

Stakeholders' communications comprise the internal and external stakeholders. From an internal perspective the team is responsible to support the 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. A strong corporate culture improves staff engagement and ultimately the implementation of the work program. It is envisaged to do an annual review of this Strategy to ensure that it is kept up to date and appropriate for the Agency.

Task	Objective	Level of completion 2018	Level of completion 2019	Level of completion 2020
Increase the level of awareness of ENISA's work and recent developments related to the Agency.	Develop Internal Communication Strategy	80%	90%	95%
Increase the staff motivation.	Bring all staff members and offices closer for a better and fruitful cooperation	80%	90%	95%

3.5.2.1.3 Permanent Stakeholders Group

In 2018, ENISA will continue and reinforce the contribution of the Permanent Stakeholders Group (PSG) to the ENISA Work Programme.

The Permanent Stakeholders' Group (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.

A new PSG was elected in 2017.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.

3.5.2.1.4 National Liaison Officer Network

ENISA in 2017 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 2018, ENISA will build upon these activities and strength its cooperation with the NLO Network, as the First Point of Contact for ENISA in the MS, with emphasis on:

- An NLO meeting to discuss possible improvements in the collaboration with ENISA and input on selected ENISA projects. Improvements aim at leveraging on the NLO network for the dissemination of ENISA's work to the EU Member States and EFTA countries.
- 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.

3.5.2.2 International relations

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

ENISA should participate in international cybersecurity fora such as the OECD, ICANN, IGF in so far as these groups are discussing items related to our work programme or strategy.

- ENISA will develop contacts with important cybersecurity bodies outside the EU when these are likely to influence the EU cybersecurity programme. The best example is NIST, which plays an important role in the implementation of the US Executive Order and can be seen as performing similar tasks to the tasks that ENISA takes for the NIS Directive.
- Starting 2018 ENISA will follow standards development and certification initiatives at the international level, as some of the issues to be solved in the EU have international scope (notably common criteria certification).
- ENISA will follow the development of relevant subjects at the international level in order to align EU activities with other global players. An example here is provided by the work that ITU is doing with CSIRTs, which needs to be aligned and will create added value and harmonization to all.
- ENISA staff will attend international conferences on an 'as needed' basis. For instance, the Meridian Conference is the main CIIP conference of the year and the FIRST conference plays the same role for CERTs.
- The ED should attend international conferences in order to enhance the Agency visibility.

3.6 Summary tables

3.6.1 List of Outputs work programme 2018

The following table provides the list of Outputs of Work programme 2018 and the associated priority for each Output. The budget and resources tables are using the priority value. Priority 2 activities are going to be delivered only if budget / resources become available.

List of Outputs 2018	Priority
Activity 1 - Expertise. Anticipate and support Europe in facing emerging network and information security challenges	
Objective 1.1. Improving the expertise related to Network and Information security	
Output O.1.1.1 - Good practices for security of Internet of Things	1
Objective 1.2. NIS Threat Landscape and Analysis	
Output O.1.2.1 - Annual ENISA Threat Landscape	1
Output O.1.2.2 - Restricted and public Info notes on NIS	1
Output O.1.2.3 - Support incident reporting activities in the EU	1
Objective 1.3. Research & Development, Innovation	
Output O.1.3.1 - Guidelines for the European standardisation in the field of ICT security	1
Output O.1.3.2 - Priorities for EU Research & Development	1
Objective 1.4. Response to Article 14 Requests under Expertise Activity	
Output O.1.4.1 - Response to Requests under Expertise Activity	1
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 certification of products and services	1
Output O.2.1.2 - Towards a framework for policy development in the cybersecurity	1
Output O.2.1.3 - Towards a Digital Single Market for high quality NIS products and services	2
Objective 2.2. Supporting EU policy implementation	
Output O.2.2.1 - Recommendations supporting implementation of the eIDAS Regulation	1
Output O.2.2.2 - Supporting the Implementation of the NIS Directive	1
Output O.2.2.3 - Baseline Security Recommendations for the OES Sectors and DSPs	1
Output O.2.2.4 - Supporting the Payment Services Directive (PSD) Implementation	1
Output O.2.2.5 - Contribute to the EU policy in the area of electronic communications sector, privacy and data protection	2
Objective 2.3. Response to Article 14 Requests under Policy Activity	
Output O.2.3.1 - Response to Requests under Policy Activity	1
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 - Update and provide technical trainings for MS and EU bodies	1
Output O.3.1.2 - Support EU MS in the development and assessment of NCSS	1
Output O.3.1.3 - Support EU MS in their Incident Response Development	1
Objective 3.2. Support EU institutions' capacity building.	
Output O.3.2.1 - NIS Directive transposition	1
Output O.3.2.2 - Restricted. Upon request, support the assessment of existing policies/procedures/practices on NIS within EU institutions	2
Objective 3.3. Assist private sector capacity building.	
Objective 3.4. Assist in improving general awareness	
Output O.3.4.1 - Cyber Security Challenges	1
Output O.3.4.2 - European Cyber Security Month deployment	1
Objective 3.5. Response to Article 14 Requests under Capacity Activity	
Output O.3.5.1 - Response to Requests under Capacity Activity	1

List of Outputs 2018	Priority
Activity 4 - Community. Foster the emerging European network and information security community	
Objective 4.1. Cyber crisis cooperation	
Output O.4.1.1 - Cyber Europe 2018	1
Output O.4.1.2 - Planning and organisation of EuroSOPEx 2018	2
Output O.4.1.3 - Lessons learnt and advice related to cyber crisis cooperation	1
Output O.4.1.4 - Support activities for Cyber Exercise Planning and Cyber Crisis Management	1
Objective 4.2. CSIRT and other NIS community building.	
Output O.4.2.1 - EU CSIRT network secretariat and support for EU CSIRT network community building	1
Output O.4.2.2 - Support the fight against cybercrime and collaboration between CSIRTs and LEA	1
Objective 4.3. Response to Article 14 Requests under Community Activity	
Output O.4.3.1 - Response to Requests under Community Building Activity	1

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.

Scenario 1 – Priority 1 Outputs only **Title**	**Total ABB budget (€)**	**Total ABB posts (FTEs)**
Activity 1 – Expertise. Anticipate and support Europe in facing emerging network and information security challenges	2.291.855,48	18,45
Activity 2 – Policy. Make network and information security an EU policy priority	2.554.956,37	21,72
Activity 3 – Capacity. Support Europe in setting up state-of-the-art network and information security capacities	1.336.059,25	11,66
Activity 4 – Community. Make the European network and information security community a reality	2.039.031,96	13,46
Activity 5 - Enabling. Reinforce ENISA's impact	3.227.096,95	17,72
Total	**11.449.000,00**	**83,00**

Scenario 2 -– Priority 1 and Priority 2 Outputs Title	Total ABB budget (€)	Total ABB posts (FTEs)
Activity 1 – Expertise. Anticipate and support Europe in facing emerging network and information security challenges	3.009.709,44	18,70
Activity 2 – Policy. Make network and information security an EU policy priority	4.627.729,23	25,80
Activity 3 – Capacity. Support Europe in setting up state-of-the-art network and information security capacities	1.926.214,04	13,68
Activity 4 – Community. Make the European network and information security community a reality	1.672.595,86	13,49
Activity 5 - Enabling. Reinforce ENISA's impact	2.712.751,44	17,33
Total	**13.949.000,00**	**89,00**

Annexes A

A.1 Annex I: Resource allocation per Activity 2018 – 2020

Section 2.4.2 of the document presents in a chart the distribution of resources proposed for 2018 while Section 3.6.2 provides allocation per activities.

A.2 Annex II: Human and Financial Resources 2018-2020

The tables below show the expected expenditure based on the same structure for the next years. Scenario 1 covers the available allocated resources and budget while an alternate scenario with 6 more FTE's and an increase in the budget is included.

Expenditure overview.

Scenario 1 – Priority 1 outputs only

Expenditure	2017		2018		2019		2020	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1	6.387.979,00	6.387.979,00	6.386.500,00	6.386.500,00	6.492.000,00	6.492.000,00	6.597.120,00	6.597.120,00
Title 2	1.770.700,00	1.770.700,00	1.687.500,00	1.687.500,00	1.741.000,00	1.741.000,00	1.797.500,00	1.797.500,00
Title 3	3.086.000,00	3.086.000,00	3.375.000,00	3.375.000,00	3.426.000,00	3.426.000,00	3.479.380,00	3.479.380,00
Total expenditure	**11.244.679,00**	**11.244.679,00**	**11.449.000,00**	**11.449.000,00**	**11.659.000,00**	**11.659.000,00**	**11.874.000,00**	**11.874.000,00**

Scenario 2 – Priority 1 & 2 outputs

Expenditure	2017		2018		2019		2020	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1	6.387.979,00	6.387.979,00	7.218.000,00	7.218.000,00	7.186.000,00	7.186.000,00	7.304.000,00	7.304.000,00
Title 2	1.770.700,00	1.770.700,00	1.736.000,00	1.736.000,00	1.787.000,00	1.787.000,00	1.844.000,00	1.844.000,00
Title 3	3.086.000,00	3.086.000,00	4.995.000,00	4.995.000,00	5.056.000,00	5.056.000,00	4.986.000,00	4.986.000,00
Total expenditure	**11.244.679,00**	**11.244.679,00**	**13.949.000,00**	**13.949.000,00**	**14.029.000,00**	**14.029.000,00**	**14.134.000,00**	**14.134.000,00**

The tables below show the commitments and payment appropriations based on the same structure for the next years. Scenario 1 covers the available allocated resources and budget while an alternate scenario with 6 more FTE's and an increase in the budget is included.

Commitment appropriations

Scenario 1 – Priority 1 outputs only

EXPENDITURE	Commitment appropriations						
	Executed Budget 2016	Budget 2017	Draft Budget 2018		VAR 2018 / 2017	Envisaged in 2019	Envisaged in 2020
			Agency request	Budget Forecast			
Title 1 Staff Expenditure	**6.012.003**	**6.387.979**	**6.386.500**	**6.386.500**	**-0,02%**	**6.492.000**	**6.597.120**
11 Staff in active employment	4.587.794	5.184.279	5.186.400	5.186.400	**0,04%**	5.247.000	5.322.120
- of which establishment plan posts							
- of which external personnel							
12 Recruitment expenditure	167.568	283.600	261.100	261.100	**-7,93%**	270.000	270.000
13 Socio-medical services and training	118.052	177.000	190.000	190.000	**7,34%**	195.000	210.000
14 Temporary assistance	1.138.588	743.100	749.000	749.000	**0,79%**	780.000	795.000
Title 2 Building, equipment and miscellaneous expenditure	**1.965.414**	**1.770.700**	**1.687.500**	**1.687.500**	**-4,70%**	**1.741.000**	**1.797.500**
20 Building and associated costs	1.152.253	1.031.500	1.000.500	1.000.500	**-3,01%**	1.021.000	1.051.500
21 Movable property and associated costs	81.449	69.000	60.000	60.000	**-13,04%**	63.000	64.000
22 Current administrative expenditure	63.426	60.000	62.000	62.000	**3,33%**	67.000	67.000
23 ICT	668.286	610.200	565.000	565.000	**-7,41%**	590.000	615.000
Title 3 Operational expenditure	**3.056.558**	**3.086.000**	**3.375.000**	**3.375.000**	**9,36%**	**3.426.000**	**3.479.380**
30 Activities related to meetings and missions	776.562	697.000	715.000	715.000	**2,58%**	736.000	746.000
32 Horizontal operational activities	438.459	530.000	660.000	660.000	**24,53%**	690.000	615.000
36 Core operational activities	1.841.537	1.859.000	2.000.000	2.000.000	**7,58%**	2.000.000	2.118.380
TOTAL EXPENDITURE	**11.033.974**	**11.244.679**	**11.449.000**	**11.449.000**	**1,82%**	**11.659.000**	**11.874.000**

Scenario 2 – Priority 1 & 2 outputs

EXPENDITURE	Commitment appropriations						
	Executed Budget 2016	Budget 2017	Draft Budget 2018		VAR 2018 / 2017	Envisaged in 2019	Envisaged in 2020
			Agency request	Budget Forecast			
Title 1 Staff Expenditure	**6.012.003**	**6.387.979**	**7.218.000**	**7.218.000**	**12,99%**	**7.186.000**	**7.304.000**
11 Staff in active employment	4.587.794	5.184.279	5.632.238	5.632.238	**8,64%**	5.736.000	5.824.000
- of which establishment plan posts							
- of which external personnel							
12 Recruitment expenditure	167.568	283.600	436.762	436.762	**54,01%**	270.000	270.000
13 Socio-medical services and training	118.052	177.000	205.000	205.000	**15,82%**	210.000	225.000
14 Temporary assistance	1.138.588	743.100	944.000	944.000	**27,04%**	970.000	985.000
Title 2 Building, equipment and miscellaneous expenditure	**1.965.414**	**1.770.700**	**1.736.000**	**1.736.000**	**-1,96%**	**1.787.000**	**1.844.000**
20 Building and associated costs	1.152.253	1.031.500	1.001.000	1.001.000	**-2,96%**	1.021.500	1.052.000
21 Movable property and associated costs	81.449	69.000	80.000	80.000	**15,94%**	85.000	87.000
22 Current administrative expenditure	63.426	60.000	70.000	70.000	**16,67%**	75.000	75.000
23 ICT	668.286	610.200	585.000	585.000	**-4,13%**	605.500	630.000
Title 3 Operational expenditure	**3.056.558**	**3.086.000**	**4.995.000**	**4.995.000**	**61,86%**	**5.056.000**	**4.986.000**
30 Activities related to meetings and missions	776.562	697.000	775.000	775.000	**11,19%**	806.000	811.000
32 Horizontal operational activities	438.459	530.000	720.000	720.000	**35,85%**	750.000	675.000
36 Core operational activities	1.841.537	1.859.000	3.500.000	3.500.000	**88,27%**	3.500.000	3.500.000
TOTAL EXPENDITURE	**11.033.974**	**11.244.679**	**13.949.000**	**13.949.000**	**24,05%**	**14.029.000**	**14.134.000**

Payments appropriations

Scenario 1 – Priority 1 outputs only

EXPENDITURE	Payments appropriations						
	Executed Budget 2016	Budget 2017	Draft Budget 2018		VAR 2018 / 2017	Envisaged in 2019	Envisaged in 2020
			Agency request	Budget Forecast			
Title 1 Staff Expenditure	**5.631.392**	**6.387.979**	**6.386.500**	**6.386.500**	**-0,02%**	**6.492.000**	**6.597.120**
11 Staff in active employment	4.587.794	5.184.279	5.186.400	5.186.400	**0,04%**	5.247.000	5.322.120
- of which establishment plan posts							
- of which external personnel							
12 Recruitment expenditure	162.883	283.600	261.100	261.100	**-7,93%**	270.000	270.000
13 Socio-medical services and training	83.932	177.000	190.000	190.000	**7,34%**	195.000	210.000
14 Temporary assistance	796.784	743.100	749.000	749.000	**0,79%**	780.000	795.000
Title 2 Building, equipment and miscellaneous expenditure	**1.455.031**	**1.770.700**	**1.687.500**	**1.687.500**	**-4,70%**	**1.741.000**	**1.797.500**
20 Building and associated costs	904.039	1.031.500	1.000.500	1.000.500	**-3,01%**	1.021.000	1.051.500
21 Movable property and associated costs	36.497	69.000	60.000	60.000	**-13,04%**	63.000	64.000
22 Current administrative expenditure	61.113	60.000	62.000	62.000	**3,33%**	67.000	67.000
23 ICT	453.382	610.200	565.000	565.000	**-7,41%**	590.000	615.000
Title 3 Operational expenditure	**2.768.988**	**3.086.000**	**3.375.000**	**3.375.000**	**9,36%**	**3.426.000**	**3.479.380**
30 Activities related to meetings and missions	689.581	697.000	715.000	715.000	**2,58%**	736.000	746.000
32 Horizontal operational activities	320.939	530.000	660.000	660.000	**24,53%**	690.000	615.000
36 Core operational activities	1.758.468	1.859.000	2.000.000	2.000.000	**7,58%**	2.000.000	2.118.380
TOTAL EXPENDITURE	**9.855.411**	**11.244.679**	**11.449.000**	**11.449.000**	**1,82%**	**11.659.000**	**11.874.000**

Scenario 2 – Priority 1 & 2 outputs

EXPENDITURE	Payments appropriations						
	Executed Budget 2016	Budget 2017	Draft Budget 2018		VAR 2018 / 2017	Envisaged in 2019	Envisaged in 2020
			Agency request	Budget Forecast			
Title 1 Staff Expenditure	**5.631.392**	**6.387.979**	**7.218.000**	**7.218.000**	**12,99%**	**7.186.000**	**7.304.000**
11 Staff in active employment	4.587.794	5.184.279	5.632.238	5.632.238	**8,64%**	5.736.000	5.824.000
- of which establishment plan posts	*0*						
- of which external personnel	*0*						
12 Recruitment expenditure	162.883	283.600	436.762	436.762	**54,01%**	270.000	270.000
13 Socio-medical services and training	83.932	177.000	205.000	205.000	**15,82%**	210.000	225.000
14 Temporary assistance	796.784	743.100	944.000	944.000	**27,04%**	970.000	985.000
Title 2 Building, equipment and miscellaneous expenditure	**1.455.031**	**1.770.700**	**1.736.000**	**1.736.000**	**-1,96%**	**1.787.000**	**1.844.000**
20 Building and associated costs	904.039	1.031.500	1.001.000	1.001.000	**-2,96%**	1.021.500	1.052.000
21 Movable property and associated costs	36.497	69.000	80.000	80.000	**15,94%**	85.000	87.000
22 Current administrative expenditure	61.113	60.000	70.000	70.000	**16,67%**	75.000	75.000
23 ICT	453.382	610.200	585.000	585.000	**-4,13%**	605.500	630.000
Title 3 Operational expenditure	**2.768.988**	**3.086.000**	**4.995.000**	**4.995.000**	**61,86%**	**5.056.000**	**4.986.000**
30 Activities related to meetings and missions	689.581	697.000	775.000	775.000	**11,19%**	806.000	811.000
32 Horizontal operational activities	320.939	530.000	720.000	720.000	**35,85%**	750.000	675.000
36 Core operational activities	1.758.468	1.859.000	3.500.000	3.500.000	**88,27%**	3.500.000	3.500.000
TOTAL EXPENDITURE	**9.855.411**	**11.244.679**	**13.949.000**	**13.949.000**	**24,05%**	**14.029.000**	**14.134.000**

Table 2 – Revenue Overview

The tables below present 2 scenarios. Scenario 1 covers the available allocated resources and budget while an alternate scenario with 6 more FTE's and an increase in the budget is included.

Scenario 1 – Priority 1 outputs only

Revenues	2017	2018
	Revenues estimated by the agency	Budget Forecast
EU contribution	10.322.000	10.529.000
Other revenue	922.679	920.000
Total revenues	**11.244.679**	**11.449.000**

Scenario 2 – Priority 1 & 2 outputs

Revenues	2017	2018
	Revenues estimated by the agency	Budget Forecast
EU contribution	10.322.000	13.029.000
Other revenue	922.679	920.000
Total revenues	**11.244.679**	**13.949.000**

Revenue

Scenario 1 – Priority 1 outputs only

REVENUES	2016	2017	2018		VAR 2018 /2017	Envisaged 2019	Envisaged 2020
	Executed Budget	Revenues estimated by the agency	As requested by the agency	Budget Forecast			
1 REVENUE FROM FEES AND CHARGES							
2. EU CONTRIBUTION	10.120.000	10.322.000	10.529.000		2,01%	10.739.000	10.954.000
of which Administrative (Title 1 and Title 2)							
of which Operational (Title 3)							
of which assigned revenues deriving from previous years' surpluses	50.269	80.397	38.616		-51,97%		
3 THIRD COUNTRIES CONTRIBUTION (incl. EFTA and candidate countries)	277.932	282.679	280.000		-0,95%	280.000	280.000
of which EFTA	277.932	282.679	280.000		-0,95%	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	19.663	0,00	0,00		0,00%	0,00	0,00
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT							
7 CORRECTION OF BUDGETARY IMBALANCES							
TOTAL REVENUES	11.033.974	11.244.679	11.449.000		1,82%	11.659.000	11.874.000

Scenario 2 – Priority 1 & 2 outputs

REVENUES	2016	2017	2018		VAR 2018 /2017	Envisaged 2019	Envisaged 2020
	Executed Budget	Revenues estimated by the agency	As requested by the agency	Budget Forecast			
1 REVENUE FROM FEES AND CHARGES							
2. EU CONTRIBUTION	10.120.000	10.322.000	13.029.000		26,23%	13.109.000	13.214.000
of which Administrative (Title 1 and Title 2)							
of which Operational (Title 3)							
of which assigned revenues deriving from previous years' surpluses	50.269	80.397	38.616		-51,97%		
3 THIRD COUNTRIES CONTRIBUTION (incl. EFTA and candidate countries)	277.932	282.679	280.000		-0,95%	280.000	280.000
of which EFTA	277.932	282.679	280.000		-0,95%	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	19.663	0,00	0,00		0,00%	0,00	0,00
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT							
7 CORRECTION OF BUDGETARY IMBALANCES							
TOTAL REVENUES	11.033.974	11.244.679	13.949.000		24,05%	14.029.000	14.134.000

Table 3 – Budget outturn and cancellation of appropriations

Calculation of budget outturn

Budget Outturn	2014	2015	2016*
Revenue actually received (+)	10.019.554	10.069.280	
Payments made (-)	- 8.710.278	- 9.395.559	
Carry-over of appropriation (-)	- 1.333.221	- 674.521	
Cancellation of appropriations carried over (+)	74.505	80.675	
Adjustment for carry over of assigned revenue appropriations from previous year (+)		800	
Exchange rate differences (+/-)	- 291	- 278	
Adjustment for negative balance from previous year (-)			
TOTAL	50.269	80.397	

Budget Outturn (data available in Q1 2017).
*The Budget Outturn 2016 will be available in March 2017 when the closure of the accounts will be performed.

Cancellation of appropriations

- Cancellation of Commitment Appropriations

No commitment appropriations were cancelled.

In 2016, ENISA demonstrates a commitment rate of 98,47 %, of C1 appropriation of the year at the year-end (31/12), and the non-automatic carry-over of the remaining 1,53% for a project to be contracted in 2017 and to be implemented in 2017 for the office refurbishment in Athens. The non-automatic carry over added to the committed appropriations at year-end show that the appropriations of the year 2016 will be used at 100% rate, which shows the capacity of the Agency to fully implement its annual appropriations. The same commitment rate achieved in 2010, 2011, 2012, 2013, 2014, 2015 and 2016, is maintained for a seventh year in a row. The payment rate reached 89,18% (92,89% in 2015) and the amount carried forward to 2017 was 968 198,32 EUR, representing 9,29 % of total C1 appropriations 2016 (from 7,11% in 2015).

- Cancellation of Payment Appropriations for the year

No payment appropriations were cancelled.

- Cancellation of Payment Appropriations carried over

Fund source “C8” – appropriations carried over automatically from 2015 to 2016.

The appropriations of 2015 carried over to 2016 were utilised at a rate of 94,28 % (automatic and non-automatic carry-overs) which indicates a satisfactory capability of estimation of needs. From the amount of EUR 674 520,54 carried forward, only the amount of EUR 38 615,93 was cancelled, due to the fact that the estimated expenditure deviated from the actual paid amount.

A.3 Annex III: Human Resources – Quantitative

The tables below present 2 scenarios. Scenario 1 covers the available allocated resources and budget while an alternate scenario with 6 more FTE's and an increase in the budget is included.

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

Scenario 1 – Priority 1 outputs only

Staff population		Actually filled as of 31.12 2015	Authorised under EU budget 2016	Actually filled as of 31 12.2016	Authorised under EU budget for year 2017	Expected to be filled as of 31.12.2017	In draft budget for year 2018	Envisaged in 2019	Envisaged in 2020
Officials	AD								
	AST								
	AST/SC								
TA	AD	30	34	29	34	34	34	34	34
	AST	15	14	15	14	14	13	13	13
	AST/SC								
Total		**45**	**48**	**44**	**48**	**48**	**47**	**47**	**47**
CA GFIV		9	30	12	23	23	23	23	23
CA GF III		11	5	11	5	5	5	5	5
CA GF II		1	0	0	0	0	0	0	0
CA GFI		1	0	1	0	0	0	0	0
Total CA		**22**	**35**	**24**	**28**	**28**	**28**	**28**	**28**
SNE		**2**	**1**	**1**	**8**	**8**	**8**	**8**	**8**
Structural service providers									
TOTAL		**69**	**84**	**69**	**84**	**84**	**83**	**83**	**83**
External staff for occasional replacement									

Scenario 2 – Priority 1 & 2 outputs

Staff population		Actually filled as of 31.12 2015	Authorised under EU budget 2016	Actually filled as of 31 12.2016	Authorised under EU budget for year 2017	Expected to be filled as of 31.12.2017	In draft budget for year 2018	Envisaged in 2019	Envisaged in 2020
Officials	AD								
	AST								
	AST/SC								
TA	AD	30	34	29	34	34	40	40	40
	AST	15	14	15	14	14	13	13	13
	AST/SC								
Total		**45**	**48**	**44**	**48**	**48**	**53**	**53**	**53**
CA GFIV		9	30	12	23	23	23	23	23
CA GF III		11	5	11	5	5	5	5	5
CA GF II		1	1	0	0	0	0	0	0
CA GFI		1	1	1	0	0	0	0	0
Total CA		**22**	**35**	**24**	**28**	**28**	**28**	**28**	**28**
SNE		**2**	**1**	**1**	**8**	**8**	**8**	**8**	**8**
Structural service providers									
TOTAL		**69**	**84**	**69**	**84**	**84**	**89**	**89**	**89**
External staff for occasional replacement									

Table 2 – Multi-annual staff policy plan year 2018 – 2020

Scenario 1 – Priority 1 outputs only

Category and grade	Establishment plan in EU Budget 2016		Filled as of 31/12/2016		Modifications in year 2016 in application of flexibility rule		Establishment plan in voted EU Budget 2017		Modifications in year 2017 in application of flexibility rule		Establishment plan in Draft EU Budget 2018		Establishment plan 2019		Establishment plan 2020	
	officials	TA	officials	TA	officials	TA	officials	TA	officials	TA	officials	TA	officials	TA	officials	TA
AD 16																
AD 15		1		1				1				1		1		1
AD 14																
AD 13																
AD 12		3		2				3				3		3		3
AD 11				1												
AD 10		5		2				5				5		5		5
AD 9		9		2				10				10		10		10
AD 8		9		5				15				15		15		15
AD 7		7		2												
AD 6				13												
AD 5				1												
Total AD	**0**	**34**		**29**				**34**				**34**		**34**		**34**
AST 11																
AST 10																
AST 9																
AST 8																
AST 7				1				2				2		2		2
AST 6		3		1				5				5		5		5
AST 5		5		2				5				5		5		5
AST 4		1		5				2				2		1		1
AST 3		3		6				0								
AST 2		2		0				0								
AST 1																
Total AST	**0**	**14**		**15**				**14**				**14**		**13**		**13**
AST/SC1																
AST/SC2																
AST/SC3																
AST/SC4																
AST/SC5																
AST/SC6																
Total AST/SC																
TOTAL		**48**		**44**				**48**				**47**		**47**		**47**

Scenario 2 – Priority 1 & 2 outputs

Category and grade	Establishment plan in EU Budget 2016		Filled as of 31/12/2016		Modifications in year 2016 in application of flexibility rule		Establishment plan in voted EU Budget 2017		Modifications in year 2017 in application of flexibility rule		Establishment plan in Draft EU Budget 2018		Establishment plan 2019		Establishment plan 2020	
	officials	TA	officials	TA	officials	TA	officials	TA	officials	TA	officials	TA	officials	TA	officials	TA
AD 16																
AD 15		1		1				1				1		1		1
AD 14																
AD 13																
AD 12		3		2				3				3		3		3
AD 11				1												
AD 10		5		2				5				5		5		5
AD 9		9		2				10				10		10		10
AD 8		9		5				15				17		17		17
AD 7		7		2												
AD 6				13								4		4		4
AD 5				1												
Total AD	**0**	**34**		**29**				**34**				**40**		**40**		**40**
AST 11																
AST 10																
AST 9																
AST 8																
AST 7				1				2				2		2		2
AST 6		3		1				5				5		5		5
AST 5		5		2				5				5		5		5
AST 4		1		5				2				1		1		1
AST 3		3		6				0								
AST 2		2		0				0								
AST 1																
Total AST	**0**	**14**		**15**				**14**				**13**		**13**		**13**
AST/SC1																
AST/SC2																
AST/SC3																
AST/SC4																
AST/SC5																
AST/SC6																
Total AST/SC																
TOTAL		**48**		**44**				**48**				**53**		**53**		**53**

A.4 Annex IV: Human Resources - qualitative

A.4.1 A. Recruitment policy

A recruitment policy and guidelines are published on the ENISA's website. In 2017, ENISA will look at the recruitment, not as a simple HR process but rather as a Talent Management process by putting the right people in the right job with the right skills at the right time with a focus on retention and engagement. Latest recruitment trends (e.g. using more outbound channels, improving the selling capacity of the job vacancy, looking at communities, building referral programs, link to a workforce strategy, etc.) and outsourcing will also be explored to boost and secure the recruitment at ENISA.

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

ENISA has adopted the Implementing rules: MB 2016/10 on Reclassification of CA's, MB 2016/11 on Reclassification of TA's.

For the forthcoming years, the organisation will strive to see performance management as a business process that improves employee engagement and drive business results. It will enable staff to focus on having a constructive dialogue with the manager and to consider the exercise as a valuable developmental tool, while clarifying that the appraisal and the promotion are two different exercises.

Table 1 - Reclassification of temporary staff/promotion of officials

Category and grade	Staff in activity at 1.01.Year 2016		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	1			
AD 14	0	0			
AD 13	0	0			
AD 12	0	2			
AD 11	0	1		1	3
AD 10	0	3			
AD 9	0	3			
AD 8	0	4		1	2
AD 7	0	2		1	3
AD 6	0	13		1	2
AD 5	0	1			
Total AD	**0**	**30**		**4**	
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	7		2	6
AST 2	0	1		1	4
AST 1	0	0			
Total AST	**0**	**15**		**5**	
AST/SC1					
AST/SC2					
AST/SC3					
AST/SC4					
AST/SC5					
AST/SC6					
Total AST/SC					
Total	**0**	**45**		**9**	

Table 2 - Reclassification of contract staff

Function Group	Grade	Staff in activity at 1.01.Year 2016	How many staff members were reclassified in Year 2016	Average number of years in grade of reclassified staff members
CA IV	18			
	17			
	16			
	15			
	14	3		
	13	6		
CA III	12			
	11			
	10	1		
	9	5		
	8	5		
CA II	7			
	6	1		
	5			
	4			
CA I	3			
	2	1		
	1			
Total		**22**	**0**	

There were no reclassifications for CA staff in 2016.

A.4.3 C. Mobility policy

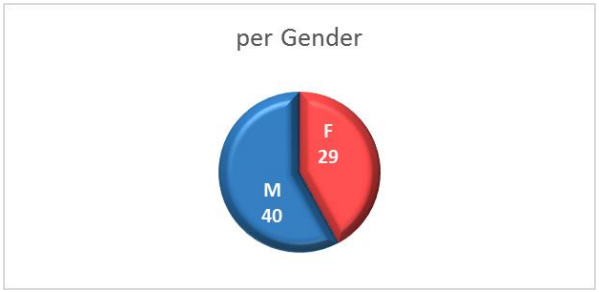
By 2017, ENISA will have an efficient internal mobility policy, beneficial to both the Agency and the individual through satisfying the needs of the organisation (in terms of performance, efficiency, quality of service and adaptation to changes) and the needs of the individual (in terms of interest, challenge, achievement and career development). ENISA will also have an effective implementation of the internal procedures to be organised at the same time as external procedures for the selection of Temporary staff under Article 2(f).

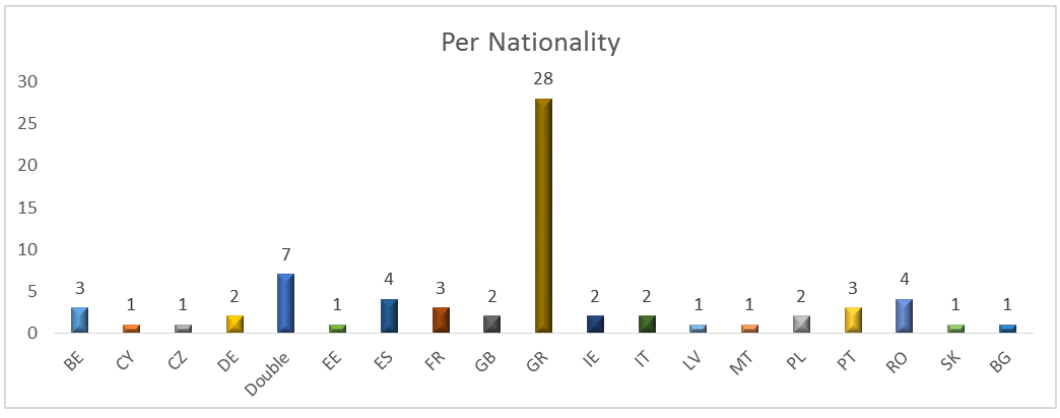
A.4.4 D. Learning and Development

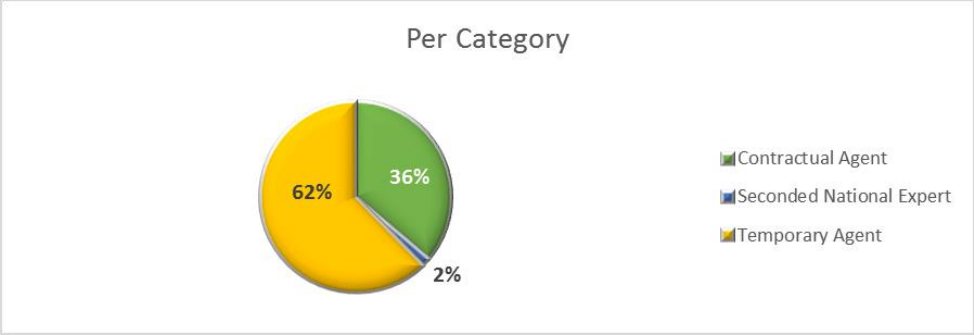
In order to make the most out of its internal expertise and to develop mechanisms to retain staff, the organisation will focus on developing an ENISA's Learning & Development Framework 2017-2020. It will ensure the efficient delivery of learning interventions, the compliance with mandatory trainings (e.g. Ethics and Integrity) and will support the acquisition of specific and strategic knowledge.

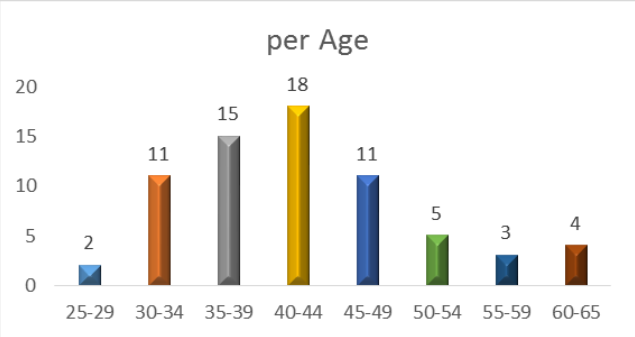
A.4.5 E. Gender and geographical balance

Please see the attached charts illustrating gender, geographical balance and category/grade in the Agency. Total number of Staff as of 31/12/2016: 69 (43 TA's: 28 AD's + 15 AST's + 25 CA's + 1 SNE).









A.4.6 F. Schooling

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

Schooling requirements of the Staff in Athens are meet by service level agreements have been concluded with a number of international schools that are attended by the children of the Staff.

A.5 Annex V: Buildings

ENISA is currently negotiating a reduction in space rented in Heraklion and an increase in the space rented in Athens. It is expected that the relevant contracts will be negotiated and concluded before the end of January 2017.

A.6 Annex VI: Privileges and immunities

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

A.7 Annex VII: Evaluations

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 30.000 EUR. 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 decisions 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 two 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	Continue trust building and cooperation activities as a means to overcome barriers to cooperation during crisis.

	structures, insufficient exchanges of information in "real life" etc., representing hurdles that need to be surmounted over the medium to long term.	
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 .

A.8 Annex VIII: Risks Year 2018

The Self Risk Assessment is on-going by the European Commission Internal Audit Service (IAS).

A.9 Annex IX: Procurement plan Year 2018

Procurement plan for 2018 will be added in the next versions.

A.10 Annex X: ENISA Organisation

As provided in the ENISA Regulation (EU) No 526/2013, the bodies of the Agency comprise:

- A Management Board**:** The Management Board is ensuring that the Agency carries out its tasks under conditions which enables it to serve in accordance with the founding Regulation.
- An Executive Board**:** The Executive Board is preparing decisions to be adopted by the Management Board on administrative and budgetary matters.
- A Permanent Stakeholders' Group**:** The PSG advises the Executive Director in the performance of his/her duties under this Regulation.
- An Executive Director: The Executive Director is responsible for managing the Agency and performs his/her duties independently.

Internally, ENISA is organized as follows:

- Executive Director
- Senior Managers (Head of Departments): provide strategic and financial management and supervise the Units and Sections within their respective fields covering different areas of ENISA activities. Advice and support the Executive Director, Executive Board and Management Board.
- Middle Managers (Head of Units): provide strategic and financial management and supervise the operational management within their respective fields covering different areas of ENISA activities in respect of sound financial management.
- Head of Section: provide strategic and financial management and supervise the operational management within their respective fields covering different areas of ENISA activities in respect of sound financial management.
- Advisors: are typically engaged in drafting reports, analysing and advising the Executive Director and/or Heads of Department in specific areas. Advisors may play a key role in general, legal, technical and budgetary processes and assist the organization in ensuring business continuity.

ENISA

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

Athens Office

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

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