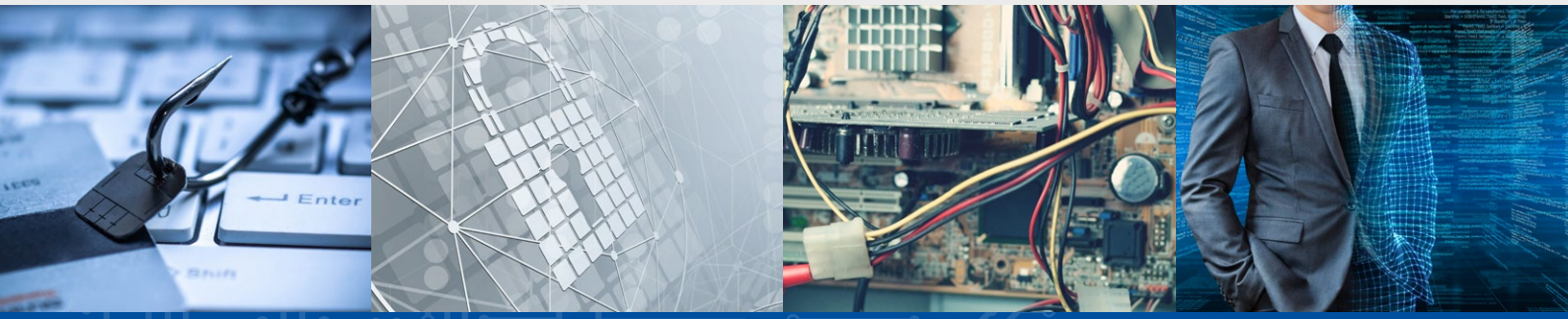
THE EU CYBERSECURITY AGENCY

ENISA PROGRAMMING DOCUMENT 2018–2020

Including multiannual planning, 2018 work programme and multiannual staff planning



NOVEMBER 2017

ENISA PROGRAMMING DOCUMENT 2018–2020

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY

CONTACT

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

LEGAL NOTICE

COPYRIGHT NOTICE

Print	ISBN 978-92-9204-227-1	ISSN 2467-4397	doi: 10.2824/337308	TP-AH-18-001-EN-C
PDF	ISBN 978-92-9204-226-4	ISSN 2467-4176	doi: 10.2824/003871	TP-AH-18-001-EN-N

TABLE OF CONTENTS

PART III

WORK PROGRAMME FOR THE YEAR 2018 29

FOREWORD BY THE EXECUTIVE DIRECTOR

For more than a decade now, the digitalisation of our society has generated growth and prosperity for EU citizens.

This digitalisation provides opportunities and means to increase productivity and to modernise so many aspects of our lives. However, at the same time, it brings new challenges for human rights (privacy and data protection issues online), for human safety and security (cybercrime, cyberbullying, cyberstalking) and for democracy (fear of hacked elections, fake news), to name a few.

It is obvious that even if we are facing significant challenges, there is no way back. The only option is to continue to make the most of digitalisation and cyberspace opportunities — by investing more in (cyber)security and in the protection of citizens and the information contained in our infrastructure and networks.

Cybersecurity is an industry/market on its own that will continue to grow. The size of the cybersecurity market in Europe [1] is estimated to increase with a 6 % compound annual growth rate (CAGR) to EUR 24.4 billion in 2018, maintaining a share of over one quarter of the worldwide cybersecurity market. In addition, if Europe does not use cybersecurity as an economic enabler the opportunity costs between 2014 and 2020 are estimated at around EUR 640 billion.

The estimated worldwide economic impact of cyberattacks has now passed half a trillion USD[2]. According to global surveys[3], 15 % of businesses say they have faced a cyberattack in the past year; businesses in the EU (19 %) and North America (18 %) have been most heavily targeted according to the same source. Yet the measurement of the real impact of lack of proper cybersecurity in terms of costs needed for full recovery is still challenging[4]. While some direct costs associated with damaged assets and the investment needed to replace compromised assets are easier to evaluate, the costs/impact of attacks on personal life, freedom, democracy and intellectual property cannot be easily measured.

At the European level, there is an increased need for digital skills and cybersecurity skills in particular. There is also a need for people who have experience of using modern information security techniques within the work environment — this latter requirement is not an issue of

1 Cybersecurity as an Economic Enabler, ENISA, Published on April 2016, available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/cybersecurity-as-an-economic-enabler

2 McAfee, Net Losses: Estimating the Global Cost of Cybercrime, report summary, 2014

3 Grant Thornton, Cyber-attacks cost global business $300bn+, available at: http://www.grantthornton.global/en/insights/articles/cyber-attacks-cost-global-business-over-$300bn-a-year/

4 ENISA, 'The cost of incidents affecting CIIs', August 2016, available at: https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis/

education, but rather of experience. It is acknowledged currently that 44 % of European citizens do not have basic digital skills[5]; Europe also lacks skilled ICT specialists to fill the growing number of job vacancies in all sectors of the economy.

Standardisation and certification play an important role in securing modern systems and ENISA continues to play an active role in both areas. In particular, ENISA has supported the European Commission over the last year in its efforts to align current approaches to certification of security products with the needs of today's society and is looking forward to contributing further to this key area.

The cybersecurity talent shortage[6] is estimated at more than a million openings worldwide while competition for qualified cybersecurity professionals is driving up salaries and improving the benefits offered. The problem is here and is likely to stay as the global shortage of cybersecurity professionals is estimated by other sources to reach 2 million by 2019[7].

The EU needs to act and for that it needs a strong and agile cybersecurity agency

ENISA, the cybersecurity agency for the EU, should be in the position to support the EU and Member States in addressing all the risks and challenges brought about by digitalisation. The entire cyber ecosystem has changed. ENISA therefore welcomes the new proposed cybersecurity strategy[8] and the new proposed Cybersecurity Act[9], which recognises this issue and proposes a significant growth in the ENISA resources and budget in the next few years.

In the meantime, however, ENISA has the difficult task of coping with a significant increase in demand for its services whilst operating within current budget and resource constraints. The Agency has achieved this through prioritisation and cutting important tasks. This was not an easy exercise. In order to achieve this, during the preparation of 2018 planning, the Agency included a reduced list of activities, already prioritised with the support of the Management Board. Those tasks which were not marked as being of high priority have been dropped from the work programme in order to satisfy the priority requirements.

In this programming document the planned activities for 2018 to 2020 are presented alongside the detailed work planning for 2018. The document follows the structure laid down by the new Commission guidelines for programming documents provided in the context of the framework financial regulation and the five pillars of ENISA strategy.

Finally, I welcome the new proposed ENISA regulation, the Cybersecurity Act. ENISA welcomes the proposal for a strengthened ENISA with additional resources and staff.

Udo Helmbrecht
Executive Director, ENISA

5 European Commission, Digital Single Market, 'The Digital Skills and Jobs Coalition', available at: https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition

6 IEEE, The Institute, Ian Chant, 'The Cybersecurity Talent Shortage Is Here, and It's a Big Threat to Companies', April 2017, https://cybersecurity.ieee.org/blog/2017/04/13/the-institute-the-cybersecurity-talent-shortage-is-here-and-its-a-big-threat-to-companies/

7 Jeff Kauflin, 'The Fast-Growing Job With A Huge Skills Gap: Cyber Security', March 2017, https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/

8 European Commission, Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU, JOIN(2017) 450, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:450:FIN

9 European Commission, Proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM(2017) 477, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN

MISSION STATEMENT

ENISA is the European Union Agency for Network and Information Security (NIS), established in 2004.

As set out in 2013 in its renewed mandate, ENISA has been set up 'for the purpose of contributing to a high level of Network and Information Security within the Union [...] thus contributing to the establishment and proper functioning of the internal market'[10], contributing to growth and employment in Europe.

The mission of ENISA is to contribute to securing Europe's information society by raising 'awareness of network and information security and to develop and promote a culture, of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organisations in the Union'[11].

In doing so, ENISA will act 'without prejudice to the competences of the Member States' regarding their national security[12] and in compliance with the right of initiative of the European Commission. In order to achieve its mission, several objectives and tasks[13] have been attributed to ENISA, 'without prejudice to the competences of the Member States regarding network and information security and in any case to activities concerning public security, defence, national security'[14].

In line with these objectives and tasks, the Agency carries out its operations in accordance with an annual and multiannual work programme, containing all of its planned activities, drawn up by the Executive Director of ENISA and adopted by ENISA's Management Board (MB).

ENISA's approach is strongly impact driven, based on the involvement of all relevant stakeholder communities, with a strong emphasis on pragmatic solutions that offer a sensible mix of short-term and long-term improvements. The Agency also provides the Union institutions, bodies and agencies (hereinafter: 'Union institutions') and the Member States with a mechanism allowing them to call upon its services to support their network and information security (NIS) capability development[15], resulting in a more agile and flexible approach to achieving its mission.

10 Regulation (EU) No 526/2013 of the European Parliament and the Council of 21 May 2013, Article 1(1).

11 Article 1(1) of ENISA Regulation (EU) No 526/2013

12 Article 1(2) of ENISA Regulation (EU) No 526/2013

13 Articles 2 and 3 of ENISA Regulation (EU) No 526/2013

14 Article 1(2) of ENISA Regulation (EU) No 526/2013

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

ENISA strategy and the strategic objectives

The strategic objectives of ENISA, set out in ENISA's strategy for 2016–2020 released in January 2016, are as follows:

#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 evolution 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.

PRINCIPLES

In implementing its strategy, ENISA's action will be guided by the following principles:

- **Affirming itself as main point of reference of the EU on NIS issues** with a view to promoting a coherent EU approach to NIS;
- **Adding value through complementarity with Member State authorities and NIS experts,** primarily competent on cybersecurity matters with whom it will reinforce its ties via the development of sustainable cooperation in its various domain of competence;
- **Liaising closely with competent EU institutions, agencies, and bodies** dealing with other aspects of NIS (Europol, European Defence Agency, European External Action Service, sectoral agencies, etc.);
- **Achieving results by leveraging relevant stakeholder communities,** allowing ENISA to strengthen its knowledge of national NIS developments and facilitate the involvement of NIS experts in its activities, including national NIS competent authorities, the private sector and academia;
- **Supporting public and private cooperation,** with a view to reducing the fragmentation of the DSM and supporting the development of the digital security industry in Europe.

I

PART I
GENERAL CONTEXT

THREAT LANDSCAPE

In a constantly evolving digital environment, threats to the network and information systems in Europe are growing rapidly. While all economic and societal activities today rely upon information systems and communication networks, the development of European digital society can only be sustainably achieved with the establishment of proper network and information security (NIS) practices, policies, organisations and capacities.

The ENISA threat landscape (ETL)[16] for 2016 shows that cyberthreats have undergone significant evolution in terms of sophistication and impact, such as 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 the front pages of the media on an almost weekly or monthly basis. Security incidents involving the internet of things (IoT) and large volume DDoS attacks complement the threat landscape.

Cyberthreat agents have performed a variety of malicious acts greatly increasing the estimates of cybercrime monetisation as illustrated by the following cases:

- Cybercrime capitalisation in 2016 almost reached the level of the second most valuable US company.
- Ransomware families are 175 % up and the average ransom is 100 % up (USD 600-700).
- Data breaches are 20 % up on last year.
- The first 1Tbps DDoS attack has happened. It has shown the impact DDoS-attacks may have (internet service latencies).
- Cyberspace is a recognised battlefield. This creates a new centre of gravity for the whole cybersecurity 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 cyberthreat agents are always a step ahead of the defenders. Still, there are some changes in the current state-of-play:

- Defenders have expanded their knowledge on modus operandi by using/implementing cyberthreat intelligence and applying it to their business products and processes in order to enhance their proactive protection strategies.
- Defenders have implemented deanonymisation methods to identify adversaries hiding behind the dark net.

16 ENISA threat landscape report 2016, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

- Defenders have understood that defence is only one side of the coin and are slowly beginning to explore active/offensive defence capabilities.
- Attackers have leveraged vast publicly available intelligence, such as published malware source code, to evolve their methods.
- Attackers put quite a lot of effort into investing and supporting their infrastructure as well as marketing their products and services to maintain their lucrative business.

In 2017 the frequency and impact of serious incidents has been growing. Two major cybersecurity incidents with EU-wide impact (WannaCry, NotPetya) have drawn everyone's attention to the reality of cyberthreats and their possible critical impacts.

The cooperation between law enforcement agencies and private sector organisations was an important factor in identifying malicious activities and infrastructure takedowns and it is likely that such cooperation activities, between communities as well as between Member States, will play an increasingly important role both in the fight against cybercrime and in the attempt to reinforce EU systems against potential attacks.

In conclusion, on top of an active cybercrime scene, the ETL has indicated that high-profile (state-sponsored) attackers have taken further action with their involvement in highly sophisticated and stealthy cyberattacks, cyberespionage, cybersabotage acts and multi-layer attacks that have been considered to possibly influence political developments.

POLICY INITIATIVES

Since it was set up with the name European Network and Information Security Agency in 2004, ENISA has actively contributed to the raising of awareness of NIS challenges in Europe, to the development of Member States' NIS capacities and to the reinforcement of the cooperation of Member States and other NIS stakeholders.

Since NIS has featured high on the EU political agenda — notably in the European cybersecurity strategy (2013), the European cyberdefence policy framework (2014) and the European digital single market (DSM) (2015) — ENISA will in the future, more than ever, need to accompany the efforts of Member States and Union institutions to reinforce NIS across Europe. Above all, the recent adoption of the directive of the European Parliament and the Council concerning measures to ensure a high common level of network and information security calls for an enhanced commitment of ENISA to supporting a coherent approach towards NIS across Europe.

While ENISA should continue its well-established activities — from support for the reinforcement of Member States' national capacities to the organisation of cyber crisis exercises — the adoption of the NIS directive will require the development of further areas of action in order to accompany the evolution of NIS in Europe. ENISA will, in particular, play a key role in: steering NIS operational cooperation by actively supporting Member States' CSIRTs' cooperation within the future European CSIRTs Network between the Member States and the institutions. ENISA will provide thereby input and expertise to policy-level collaboration between national competent authorities in the framework of the Cooperation Group, supporting the reinforcement of the NIS of Union institutions close cooperation with CERT-EU and with the institutions themselves. In parallel, ENISA will continue to 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.

While many Union bodies are developing activities related to cybersecurity(Europol, European Defence Agency, European External Action Service, etc.), ENISA aims to be the key point of reference for strategic analysis and advice on NIS issues .The Agency seeks to engage with other relevant actors and to use its experience and expertise to support them in their activities. Furthermore, ENISA will support other stakeholders, in particular the private sector, to engage in Europe's efforts to ensure a significant improvement of the state of its cyber security.

In this respect, the publication of the new EU cybersecurity strategy, on 13 September 2017, has identified ENISA as a key pillar of the EU's ambition to reinforce cybersecurity across Europe. The strategy in particular foresees the strengthening and reinforcing ENISA:

- Section 2.1 addresses ENISA and the strengthening of the Agency. A permanent mandate for it is proposed.
- ENISA's role in the NIS directive is acknowledged.
- An EU cybersecurity certification framework is proposed. It is proposed that ENISA develop certification schemes and provide secretariat assistance to the EU cybersecurity certification group. Frameworks are envisaged for:
  - critical high-risk applications;
  - widely deployed digital products and services; and
  - low-cost digital devices.

ENISA welcomes the renewed cybersecurity strategy[17] and the new proposed Cybersecurity Act[18].

17 European Commission, Joint communication to the European Parliament and the Council Resilience, 'Deterrence and defence: building strong cybersecurity for the EU', JOIN(2017) 450, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:450:FIN

18 European Commission, Proposal for a regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on information and communication technology cybersecurity certification ('Cybersecurity Act'), COM(2017) 477, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN

PART II

MULTIANNUAL PROGRAMMING 2018–2020

2.1 MULTIANNUAL PROGRAMME

This section reflects mid-term priorities that should guide the activities of the Agency for the next 3 years.

Priorities are completed with indications on;

- guidelines which should underpin ENISA's implementation of the multiannual and annual programming document;
- the expected added value of the Agency's work in achieving these priorities.

Annual outputs will derive from these priorities.

2.1.1 Activity 1 — Expertise. Anticipate and support Europe in facing emerging network and information security challenges

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 on which to offer analyses and general recommendations.
- Seek to explore in particular issues related to software (e.g. mobile), ICS/SCADA, smart infrastructure and the IoT.

Guidelines

- Collate and analyse as a priority available expertise provided by national NIS competent authorities, closely liaise with them to support its stocktaking activity and when making 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 taking into account 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 (OES)).
- Take a holistic approach encompassing the technical, organisational, regulatory and 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 and crisis and CSIRT cooperation.

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 telecoms package, eIDAS and the NIS directive.
- Deliver 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 that are underestimated today but may increase in the future).

Guidelines

- Seek synergies among national incident reports in its analyses mentioned above.
- Ensure that the EU threat landscape benefits 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 CSIRTs 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 (OES, 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 threat taxonomies (e.g. incident taxonomies) (Activity 4).

Multiannual priorities (2018-2020) for Objective 1.3. Research and development, innovation

Priorities

- Support Member States and the European Commission in defining EU priorities in the field of research and development (R & D) within the context of the European Cyber Security Organisation (ECSO), the contractual Public and Private Partnership (cPPP).

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 avoid duplication of the 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 reducing the gap between research and implementation.
- Support its work under Activity 2 by ensuring synergy between its advisory role on R & D within the context of ECSO and its advisory role on other EU NIS policy issues addressed within and outside the context of ECSO, in particular related to the establishment of a functioning DSM.

2.1.2 Activity 2 — Policy. Promote network and information security as an EU policy priority

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) with a view to 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, offer NIS expert advice to the European Commission and other relevant Union institutions on these policy developments.

Guidelines

- Closely liaise with the European Commission with a view to 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 advise on possible new policy developments.
- Foster dialogue among and with national NIS competent authorities' experts and other relevant stakeholders with a view to developing in-depth and high-quality expertise to advise 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 on matters 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 NIS aspects in key EU policies offering a digital dimension.
- Contribute to ensuring 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.

Multiannual priorities (2018-2020) for Objective 2.2. Supporting EU policy implementation

Priorities

- Support national NIS competent authorities to work together towards the implementation of already agreed EU policies (legislation) with a NIS dimension, by allowing them to share national views and experiences and build upon those to draw up consensual recommendations.
- Focus on the NIS directive in particular regarding requirements related to OES (e.g. identification, security requirements, incident reporting) and on eIDAS as well as on the NIS aspects of the general data protection regulation (GDPR) (and more generally data protection) and the ePrivacy 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. OES).
- Aim at limiting the number of dialogues with a view to 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 undertake its stocktaking.

Added value

- Support Member States in implementing 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 a harmonised approach on implementation of EU policies and in particular legislation, even when mandatory harmonisation of national approaches is not enforced, such as in the NIS directive regarding OES.

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

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

Priorities

- Advise 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 CSIRTs Network and national CSIRTs which ENISA should continue to work on with the aim of fostering the rise of EU Member States' CSIRTs.
- Develop a NIS national capacities metric, building upon capacities foreseen in the NIS directive, allowing an assessment of the state of NIS capacity development within the EU.
- Identify and draw recommendations on other national NIS capacities which are spread across the EU NIS community and would contribute to reinforcing the NIS of the EU, such as national cybersecurity assessments, PPPs such as in the field of CIIP, national information sharing schemes, etc.

Guidelines

- Carry out a regular stocktaking of national NIS capacity initiatives with a view to identify trending developments and collecting and analysing different approaches and practices.
- Liaise closely with national NIS competent authorities' experts with a view to retrieving view, experience and best practices on national NIS capacity developments.
- Take into account developments and recommendations that may arise from the CSIRTs Network as well as the Cooperation Group.
- Adopt a holistic approach concerning NIS capacities ranging from technical to organisational and policy ones.
- While creating a general NIS capacity metric, seek as a priority to identify the main trends at EU level and to advise individual Member States upon their request.
- Explore the development of tools and initiatives with a view to making ENISA's recommendations more visible and increasing their impact (e.g. summer school, onsite training)

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 contribute 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 the Connecting Europe Facility (CEF)) facilitating cooperation within the CSIRTs Network and the development

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

Priorities

- Offer proactive advice to the Union institutions on the reinforcement of their NIS.
- Seek to assist with 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 training, awareness-raising and development of education material.

Guidelines

- Identify priorities for EU agencies and bodies with the most NIS capacity-building needs by establishing regular interactions with them (e.g. annual workshops) and focus on these priorities;
- Make partnerships with CERT-EU and institutions with strong NIS capabilities with a view to 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 European Cyber Security Month (ECSM).

Identify priorities for EU agencies and bodies with the most NIS capacity-building needs by establishing regular interactions with them (e.g. annual workshops) and focus on these priorities

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.

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

Priorities

- Advise the private sector on how to improve its own NIS through the elaboration of key recommendations for cybersecurity.
- Support information-sharing among the public and private sectors on NIS developments at European level.

Guidelines

- Prioritise building upon existing work done at the national level in relation with the 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 enterprises, NIS experts or non-experts) and adopt a holistic approach towards NIS capacities ranging from technical/operational to organisational and policy capacities.
- With a view to supporting information sharing on NIS developments at European level, contribute to the functioning of ECSO as foreseen in Objectives 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.
- Also offer 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 the private sector on the need to reinforce its 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.

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

Priorities

- Organise the ECSM and the European Cyber Security Challenge (ECSC) with a view to making these events sustainable EU 'rendezvous '.
- Carry out regular stocktaking of national awareness-raising initiatives.
- Building upon this stocktaking and in liaison with the ECSM and ECSC, analyse and draw up 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 who are 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.

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.

Added value

- Allow the organisation of Europe-wide events, increasing visibility on cybersecurity and on ENISA with the EU citizens, businesses, academia and the NIS community, including NIS students.
- Foster harmonisation 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.

2.1.4 Activity 4 — Community. Foster the emerging European network and information security community

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

Priorities

- Further develop and organise Cyber Europe 2018 and 2020, exploring new dimensions and formats with the aim of further preparing the Member States and Union institutions for cyber crises 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 CSIRTs Network foreseen in the NIS directive.
- Contribute actively to the implementation of the blueprint by supporting Member States in implementing EU-level orientations, mechanisms, procedures and tools within national crisis management frameworks.
- Integrate existing and future EU-wide crisis management orientations, mechanisms, procedures and tools within the already existing crisis management framework of the Member State.
- 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 standard operating procedures (SOPs)) supporting crisis management at EU level, to be tested in the exercises.
- Support its activities under Objective 4.2 regarding the CSIRTs Network to ensure consistency in the development of procedures and tools for daily information exchange on crisis management.
- Explore the opportunity to participate as observer to other national or international exercises to draw lessons from them, 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 MB.
- Evaluate the impact of the organisation of previous exercises and build upon the lessons learned to support the evolution of future exercises and in particular to further develop the exercise platform.

Added value

- Allow the organisation of Europe-wide events, increasing the visibility of cybersecurity and of ENISA with other Union institutions, Member States, citizens, businesses and academia.
- Continue to reinforce cooperation among Member States and to further develop tools and procedures supporting their response to cross-border crises, 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 advise on national cyber crisis capacity developments.

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

Priorities

- Provide the secretariat to the CSIRTs Network foreseen in the NIS directive.
- Actively support its functioning with a view to 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 CSIRTs Network and advise, upon request, Member States' CSIRTs on projects to be proposed within the framework of future CEF calls for projects.

Guidelines

- Develop a trustworthy and sustainable dialogue with Member States' CSIRTs and CERT-EU within this framework.
- Link its activities with those carried out under Objective 4.1 building upon ENISA's expertise on cyber crisis management, with a view to the development of tools and procedures by the CSIRTs Network from daily information exchange on cyber crises.

Added value

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

2.1.5 Activity 5 — Enabling. Reinforce ENISA's impact

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

Priorities

- Increase and improve the recruitment of new NIS experts with the aim of achieving the priorities laid out in the work programme.
- Develop internal management with a view to supporting the development of ENISA's internal expertise as well as ensuring the 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 necessary to achieve the multiannual priorities of the work programme.
- Improve recruitment effectiveness and internal processes, in particular with a view to accelerating and smoothing the recruitment process, thus contributing to improving ENISA's internal expertise.
- Promote the development of sustainable team-work among ENISA's experts.
- Continue to recruit seconded national experts.
- Continue to improve processes for monitoring financial flows and maintain high commitment and payment rates and thus guarantee full implementation of the work programme.

Added value

- Improve the general quality and efficiency of ENISA's activities by strengthening the Agency's quality management system.
- Support, in particular, the development of structured dialogues with national NIS competent authorities' expert, building upon the teams of internal experts.

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

Priorities

- Increase and improve the involvement of Member States' national NIS competent authorities' experts with the implementation of the work programme (stocktaking, involvement in the implementation of outputs).
- Proactively engage with other competent Union bodies (e.g. European Commission, other agencies, CERT-EU) with a view to identifying possible synergies, avoiding redundancy and providing advice building on ENISA's NIS expertise.
- Seek to increase and evaluate added value and the impact of its activities on the European NIS community.
- Communicate in a transparent manner with stakeholders, in particular with Member States, on activities to be carried out and inform them about their implementation.
- When relevant and on an ad hoc basis, contribute to the Union's efforts to cooperate with non-EU countries and international organisations to promote international cooperation on NIS.

Guidelines

- When provided for by the work programme, establish, whenever relevant on a multiannual basis, structured dialogues with national Member States' voluntary experts with a view to 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, with a view to engaging with the private sector.
- Further develop tools and procedures to facilitate and make transparent the involvement of all stakeholders, in particular regarding the principles and modalities of the participation and consultation of national NIS competent authorities.
- Prioritise building upon the network of liaison officers as the main exchange point for ENISA and Member States with a view to achieving these priorities.
- Carry out regular in-depth evaluations with a view to assessing the mid- to long-term impact of its action in certain areas of expertise.

Added value

- Build trust and mutual expertise with Member States' experts and other stakeholders and contribute to reinforcing 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 of the needs of the European NIS community and in particular of those of the Member States.
- Benefit from the European NIS community's expertise — and in particular from Member States' expertise — thus offering tailored, high-quality and up-to-date analysis and recommendations with high European added value.

2.2 MONITORING THE PROGRESS AND THE ACHIEVEMENTS OF THE AGENCY. SUMMARISING THE KEY INDICATORS FOR THE MULTIANNUAL ACTIVITIES

The Agency has developed key indicators to provide the metrics to measure the performance, results and impact of the Agency's outcomes, outputs and impact. A detailed presentation of key performance indicators (KPIs), key results indicators (KRIs) and key impact indicators (KIIs) is provided in Annex B.

2.3 HUMAN AND FINANCIAL RESOURCE OUTLOOK FOR THE YEARS 2018-2020

Annex 1 provides an outlook for resources and contains a brief description of new tasks and efficiency gains.

PART III

WORK PROGRAMME FOR THE YEAR 2018

The ENISA work programme for the year 2018 follows the structure presented in the multiannual programming in Part 2. 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 the added value of the activity, the main challenges for 2018 and a link to the multiannual objectives.

The main outputs/actions in the specific year, for this case for 2018, are listed within each objective. Several outputs are defined for each objective.

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 a 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 out in response to requests. Article 14 requests, named after Article 14 of the ENISA regulation, allow the Member State and the 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

3.1.1 Objective 1.1. Improving the expertise related to network and information security

Output O.1.1.1 — Good practices for security of the 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 concerning

Smart Infrastructures, Industry 4.0[19], 5G[20], Smart Grids[21], etc. IoT security should thus be considered in this context[22].

The Agency will identify and analyse existing security practices and standards in the area of IoT security for CII and Smart Infrastructure taking into consideration existing national expertise and practices. ENISA will compare these practices and standards and develop good practices for security of IoT, with a particular focus on the impact on end-users.

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)[23] and the 5G Infrastructure Public–Private Partnership (5G PPP)[24]).

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 the public sector, such as DG Communications Networks, Content and Technology and the Joint Research Centre, and from the private sector, including CII providers, integrators and manufacturers.

This work item builds on the previous work of ENISA in the area of IoT, Intelligent Cars, Smart Cities, Smart Hospitals and Smart Airports (2015–2016 work programme).

19 See https://ec.europa.eu/digital-single-market/en/fourth-industrial-revolution

20 See https://ec.europa.eu/digital-single-market/en/towards-5g

21 See https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters

22 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.

23 More information on the Alliance for Internet of Things Innovation (AIOTI) is available at: https://ec.europa.eu/digital-single-market/en/alliance-internet-things-innovation-aioti

24 More information on the 5G Infrastructure Pubic–Private Partnership (5G PPP) is available at: https://5g-ppp.eu/

3.1.2 Objective 1.2. NIS threat landscape and analysis

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. It contains tactical and strategic information about cyberthreats and also refers to threat agents and attack vectors used. The report is based on an intensive information collection exercise, including annual incident reports, followed by analysis and consolidation of publicly available information on cyberthreats. It contains cyberthreat intelligence by means of interrelated threat related information objects.

The ENISA Threat Landscape (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, ENISA will make available to the public all relevant material that has been collected during the year.

The visualisation and quick availability of threat information will be in the focus in 2018. The ENISA threat landscape will be accompanied by an end-user application (web-based) that will provide available information online. In this manner, ETL users will be in a 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 its cooperation with CERT-EU in the area of threat landscaping. This 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 memorandums of understanding) will be maintained and expanded.

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. As from 2018, the Agency will produce two distinct types of note; 'CSIRT Info Notes' and 'General Info Notes'.

CSIRT Info Notes

CSIRT Info Notes cover incidents with an EU dimension that are within the scope of the activities of the CSIRTs Network. Such notes will only be published following the agreement of the CSIRTs Network.

General Info Notes

General Info notes cover significant developments and announcements in the field of cybersecurity. General Info notes are not associated with the response to incidents but are rather explanatory notes, regarding — for example — events that have a certain level of public and media attention. For General Info notes, ENISA will consult the CSIRTs Network as appropriate.

Both types of note will be logically integrated with the cyberthreat information, building a single interconnected knowledge base.

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 a neutral overview of the state of play regarding an incident in 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.

ENISA will further assess the dissemination efficiency of the procured cyberthreat information, in the form of both ETL and Info Notes, by assessing their impact among key stakeholder. This will be done by using appropriate tools for analytics on user access and user enrolment. In addition to the ENISA website, Info Notes will be disseminated via the ENISA ETL platform in 2018.

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

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

Current and foreseen activities in this area include:

- Incident notification in the telecom sector (Article 13a of the telecom package); currently ENISA supports activities in this area by managing the informal Article 13a Expert Group, keeping in touch with industry and collecting incidents for the annual incident report. Further support is needed as the telecom package is currently under review and significant improvements will be made to Article 13a.
- Incident notification for the trust service providers (Article 19 of the eIDAS regulation): in 2018 ENISA will continue receiving the annual incident reports from the competent authorities and 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 private stakeholders to better understand the needs and challenges of the sector.
- Incident notification in the context of the NIS directive: as the NIS directive entered into force in August 2016, with a 2-year timeline for implementation, all stakeholders involved must prepare themselves for this step; further guidelines and support are 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 and 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.

As incident reporting obligations become more complex, one of the objectives of the activities developed by ENISA in this sector is developing efficient reporting schemes across sectors and across geographical borders.

ENISA has significant expertise in 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 and development, innovation

Output O.1.3.1 — Guidelines for 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 seek to make available a gap analysis and/or provide guidance to implement existing NIS standards. Additionally ENISA manages the relationship it has developed with the EU SDOs (CEN/CENELEC and ETSI) by contributing to their standardisation work at the strategic and tactical levels (e.g. by joining the CEN/CENELEC Cybersecurity Focus Group (CSCG), observing relevant technical and conference programme committees, etc.). New requirements associated with the transposition or implementation of the legal framework in the Member States will be taken into account, including the 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, facilitating the adoption of standards and governance of EU standardisation in the area of NIS. ENISA brings to this relationship its technical and organisation know-how in NIS which can be further leveraged into standards in terms of extending or assessing them to render them more appropriate to stakeholders and more compliant with the prevailing regulatory framework. By bringing its concrete NIS policy expertise, ENISA will produce 'how to' and 'what else' guides in an effort to contribute to European standardisation.

In carrying out this work, ENISA will consult with the Member States, industry and organisations that develop standards (e.g. ETSI, CEN, CENELEC), as well as Commission services and agencies with policy competence in these areas as appropriate.

Output O.1.3.2 — Priorities for EU research and development (Priority 1)

This study will provide an analysis of areas covered by the NIS directive, the general data protection regulation and the Commission decision on cPPP and will aim to show where R & D activities funded in the context of Horizon 2020, CEF (Connecting Europe Facility), TRANSITS and GEANT could achieve the greatest impact.

ENISA will work closely with ECSO and cPPP on cybersecurity in order to align the work being carried by them with the ENISA work programme. In addition, the Agency will offer support to the National Public Authority Representatives Committee (NAPARC) 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.

This study will provide an analysis of areas covered by the NIS directive, the general data protection regulation and the Commission decision on cPPP.

Additionally, ENISA will continue supporting and advising the Commission and designated organisations in this area (e.g. ECSO) as well as in the Member States on how 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

Output O.1.4.1 — Response to requests under expertise activity (Priority 1)

Article 14 requests allow the Member States 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 of expertise.

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

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

3.1.5 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 IoT E: IoT security workshop	Engage 5 leading IoT developers and 5 leading stakeholders from 5 EU Member States 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 Member States 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.
Output O.1.2.3 — Support incident reporting activities in EU	P: Annual incident analysis report for the telecom sector, Q4 E: Article 13a[25] meeting P: Annual incident analysis report for the trust service providers, Q4 E: Article 19[26] meetings S: Support Member States and the Commission in implementing the NIS directive incident reporting requirements P: Incident reporting framework for the NISD, Q4	More than 20 NRAs/EU Member States contribute to preparation of the report (Article 13a) 3 workshops per year (Article 13a) More than 10 supervisory bodies/ EU Member States contribute to preparation of the report (Article 19) 2 workshops per year (Article 19) Engage more than 10 Member States in discussions and work related to implementing NISD incident reporting
Objective 1.3. Research and development, innovation		
Output O.1.3.1 — Guidelines for 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 organisations (SDOs) and relevant services of the European Commission
Output O.1.3.2 — Priorities for EU research and development	P: Study and support activities on priorities for EU research & development in the context of Horizon 2020, Q4	Involve 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.	

3.2 ACTIVITY 2 — POLICY. PROMOTE NETWORK AND INFORMATION SECURITY AS AN EU POLICY PRIORITY

3.2.1 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 (Priority 1)[25, 26]

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 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.

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

The digitalisation of several critical and noncritical sectors and the emergence of new technologies such as IoT require a coherent policy framework on NIS. This is likely to allow the integration of existing policies (e.g. NISD, DSM, etc.) and the addition of new ones (e.g. IoT policy, cPPP, etc.) within a common and integrated framework.

ENISA will take stock of existing policy initiatives and assess the needs for new and emerging areas. In cooperation with Member States and the private sector the Agency will develop the key elements of such a framework and seek validation of the idea from all relevant stakeholders.

3.2.2 Objective 2.2. Supporting EU policy implementation

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 Commission and the Member States through the eIDAS experts' group. Specific implementation guidelines and technical recommendations for approval of which the eIDAS expert group will be consulted will address operational aspects of trust service providers, conformity assessment bodies and supervisory authorities. These recommendations will complement the existing knowledge base that ENISA has 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.

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 cybersecurity 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 will be done by reusing or customising existing results or by developing new, specific results meeting the needs and requirements of the Cooperation Group.

The Agency may analyse specific issues identified in the work programme of the Cooperation Group, consult with Member States' competent authorities and develop recommendations and suggestions that would allow the Commission and Member States to take informed decision on NIS matters.

In addition, ENISA will continue its efforts to support Member States 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 the public and private sector. Such good practices may be used, as much as possible, by Member States when defining, at national level, their criteria for the identification of OES.

Output O.2.2.3 — Baseline security recommendations for the OES sectors and DSPs (Priority 1)

ENISA will develop guidelines for assisting Member States to assess the compliance of DSPs and OES with security requirements set by the NISD.

ENISA, building on its expertise in security requirements developed for DSPs and OES, will work closely with Member States and the private sector to identify such cost-effective practices and maturity security frameworks that would constitute the basis for these guidelines.

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 OES (e.g. C2M2, NICE-CMM) or the generic IT models (e.g. ISO 27001) and interact with all important stakeholders from the public as well as the private sector.

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

Output O.2.2.4 — Supporting the payment services directive (PSD) implementation (Priority 1)

Payment Service Directive (PSD) 2 was adopted and will be transposed by Member States by January 2018 at the latest. The European Banking Authority (EBA), as the responsible Agency, in cooperation with ENISA and the relevant competent authorities of the Member States, develops 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 on its expertise in the field of risk management, minimun 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, such as NIS directive.

In this context the Agency will continue its cooperation with the EBA and the European Central Bank (ECB) and Member States' competent authorities on other cybersecurity-related topics including mandatory incident reporting, use of cloud computing, mobile payments and the use of blockchain by the finance sector. ENISA will also, through this cooperation with these stakeholders, align, as much as possible this work with the NISD implementation because finance is one of the key sector of this directive.

Output O.2.2.5 — Contribute to EU policy in the area of privacy and data protection (Priority 2)

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 the GDPR and ePrivacy directive will be addressed. ENISA will support the implementation of the regulatory aspects by acting as policy, technical and organisational adviser 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. Cooperation activities with the European Data Protection Supervisor (EDPS) and national data protection authorities will be continued and further enhanced.

Output O.2.2.6 — NIS directive transposition (Priority 1)

According to Article 25(1) of the NIS directive, the Member States shall adopt and publish, by 9 May

25 Article 13a of the amended Framework Directive 2002/21/EC (2002).

26 Article 19 of the eIDAS regulation (2014).

2018, the laws, regulations and administrative provisions necessary to comply with this directive. In order to support the Member States over this task, ENISA will take stock of the NISD implementation status together with other relevant stakeholders (e.g. sectorial NIS regulations). 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 transposition process. This will further strengthen the cooperation amongst Member States and at EU level, during the period of transposition, and will provide them with the appropriate knowledge for the successful completion of the task.

3.2.3 Objective 2.3. Response to Article 14 requests under policy activity

Output O.2.3.1 — Response to requests under policy activity (Priority 1)

Article 14 requests allow the Member States 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.

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

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

3.3.1 Objective 3.1. Assist Member States' capacity building

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 Member State representatives contribute to/participate in the activity
Output O.2.1.2 — Towards a framework for policy development in cybersecurity	P: Towards a framework for policy development in cybersecurity, Q4 E: Workshop with stakeholders, Q3	More than 10 private companies and 10 EU Member State representatives contribute to/participate in the activity
Objective 2.2. Supporting EU policy implementation		
Output O.2.2.1 — Recommendations for technical implementation 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/Member State 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 Member State. More than 50 stakeholders participate in the activity
Output O.2.2.2 — Supporting the implementation of the NIS directive	P: Guidelines on the parameters of the identification of OES (implementation of Article 5(7)), Q4 2018 P: Guidelines for collecting and analysing security incidents for OES and DSPs, Q4, 2018 P: Good practices on interdependencies between OES and DSPs, Q4 2018 S: Support the work of the Cooperation Group by providing in due time advice and expertise on deliverables identified by the group (e.g. on notification requirements for DSPs, on guidelines concerning the mandatory sharing of information between affected Member States (Articles 14(5) and 16 (6)) in Q1/2018 E: 2 workshops related to the tasks of the NISD, Q2-Q4 S: Contribute to the activities of Member State and the private sector in the area of OES. Q1-Q4	Engaging at least 15 Member State and 15 private stakeholders in the ENISA contributions to the implementation of the NIS directive ENISA provides contributions as requested. 10 OES participate in the workshops. 10 Member States participate in the activity.
Output O.2.2.3 — Baseline security recommendations for the OES sectors and DSPs	P: Guidelines on assessing DSPs and OES compliance with the NISD security requirements, Q4 E: 2 workshops with stakeholders from OES sectors, Q2-Q4	Engage 20 Member States in the development of good practices for OES and DSPs Engage 15 private sector in the development of good practices for OES and DSPs More than 10 Member States 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 State regulatory bodies and at least 10 private financial institutions in this study.
Output O.2.2.5 — Contribute to EU policy in the area of privacy and data protection	E: 2 workshops with relevant stakeholders, Q1-Q4 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, Annual privacy forum (APF) 2018	Engage more than 40 participants from relevant communities, including providers, data controllers and national bodies in the activity. At least 5 representatives from different bodies/ Member States participate in the preparation of the recommendations. At least 5 representatives from different bodies/ Member States participate in the preparation of the recommendations. More than 60 participants from relevant communities
Output O.2.2.6 — NIS directive transposition	P: NISD transposition status report E: Workshop S: Cooperation Group support	At least 15 Member States participate in the stock-taking exercise.
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.	

Output O.3.1.1 — Update and provide technical training for Member State and EU bodies (Priority 1)

In 2018 most of the activities in this area aim at maintaining and extending the collection of good practice guidelines and training 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 training and services in order to improve the 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 materials based on emerging technologies in order to reinforce Member State CSIRT skills and capacities to efficiently manage cybersecurity events. A special emphasis in this output is laid on supporting Member State CISRTs and EU bodies with concrete advice (like good practice material) and concrete action (like CSIRT training). ENISA will also offer, upon request, direct support to individual Member States by providing technical training and advisories.

In 2018 ENISA will further enhance its methodology, seminars and training 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 training on these subjects. In addition, this activity will cover the delivery of these training programmes upon request.

Output O.3.1.2 — Support EU Member States in the development and assessment of NCSS (Priority 1)

The NIS directive sets as priority for the Member States to adopt a national NIS strategy and to monitor its implementation. ENISA will continue assisting Member States to develop their capabilities in the area of national cybersecurity strategies (NCSS). The Agency, building on previous years' work in this area, will assist Member States to deploy existing good practices in the related areas 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 Member States and the 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 Member States ENISA will validate and update its existing NCSS good practice guide and evaluation/assessment framework for NCSS.

Finally, ENISA will continue updating ENISA's map of EU NCSS as well as enhancing this map with information collected on the NIS objectives each Member State targets. In that context, relevant qualitative and quantitative metrics will be identified. ENISA will further enhance the material provided in the e-Learning tool launched in 2015.

Output O.3.1.3 — Support EU Member States in their incident response development (Priority 1)

In 2018 ENISA will concentrate its efforts on assisting Member States with their incident response capabilities by providing a state-of-the-art view of the CSIRT landscape and development in Europe. In close cooperation with the NISD CSIRTs 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 request, direct support to individual Member States to assess and improve their incident response capabilities.

The main objectives of this output in 2018 are to help Member States and ENISA's other 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 in securing their networks. Another objective of this output is to further develop and apply ENISA recommendations for the CSIRT baseline capabilities and maturity framework. ENISA will continue supporting cross-border CSIRT community projects and tools development, as well as the global dialogue about common definitions and the maturity framework in the incident response domain.

3.3.2 Objective 3.2. Support EU institutions' capacity building.

Output O.3.2.1 — Representation of ENISA on the Steering Board of CERT-EU and representation of the EU agencies using the CERT-EU service (Priority 1)

In 2017, the operations of CERT-EU were put on a formal legal basis by way of an arrangement among a number of EU institutions. A Steering Board (SB) has been created to supervise the activities of CERT-EU, and a number of EU bodies and institutions are represented on it. A place for ENISA was also created on the SB, to represent ENISA and the EU agencies that use the services of CERT-EU.

CERT-EU was set up to provide CERT services to the EU bodies and institutions. ENISA sits on the SB. ENISA is appointed to the CERT-EU's SB to represent itself and a list of EU Agencies that may use their services.

In this context ENISA will also liaise with the EU agencies on operational issues related to CERT-EU's activities in order to ensure that the viewpoints of the Agencies are adequately represented. ENISA will also report in to the CERT-EU SB on the evolution of Services required by the Agencies.

3.3.3 Objective 3.3. Assist in improving private sector capacity building and general awareness

In close collaboration with Member States and with the private sector, ENISA will help EU citizens to gain essential cybersecurity knowledge and skills to help protect their digital lives. Aspects like cybersecurity culture, cyber hygiene liability and insurance will be analysed.

In 2018 activities 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 those Member States.

Output O.3.3.1 — Cyber Security Challenges (Priority 1)

In order to promote capacity building and awareness on NIS among the emerging young generation of cybersecurity experts in Member States, ENISA will continue to promote and advise the Member States on running national cybersecurity challenge competitions in 2018. The Agency will also continue its European Cyber Security Challenge annual activity. Its support to the national and European activities will aim at schoolchildren, university students as well as young talents and 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 attract a large number of participants from different Member States for the final competition.

Output O.3.3.2 — European Cyber Security Month deployment (Priority 1)

The metrics built into the European Cyber Security Month (ECSM) 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 EU citizens. Previously proposed pillars remain: support a multi-stakeholder governance approach; encourage common public–private activities; and assess the impact of activities, optimising and adapting to new challenges as appropriate. Past work on cybersecurity culture will be leveraged with a view to testing guidelines in practice.

3.3.4 Objective 3.4. Response to Article 14 requests under capacity activity

Output O.3.4.1 — Response to requests under capacity activity (Priority 1)

Article 14 requests allow the Member States 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.

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.

3.3.5 Type of outputs and performance indicators for each outputs of Activity 3 — Capacity

Summary of outputs in Activity 3 — Capacity. Support Europe in 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 training for Member States and EU bodies	S: Customise existing training material to the needs of an NISD sector and delivery of a training session. P: Q4: Update of existing operational training material (details on operational category can be found on ENISA training website) S: TRANSITs (European CSIRT training event) support	At least 10 Member States participate in the sectorial training. At least 1 item of training material updated to support improved operational practices of CSIRTs in at least 15 Member States. Support at least 3 events. At least 70 % of participants in training (online or onsite) evaluate the experience as positive or very positive.
Output O.3.1.2 — Support EU Member States 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 Member States on NCSS development, Q2-Q4	Engage at least 20 Member States in this activity/workshop.
Output O.3.1.3 — Support EU Member States in their incident response development	P: Q4: CSIRTs landscape in Europe P: Q2 and Q4: CSIRT online inventory update — European interactive map of CSIRTs P: Q4: CSIRT maturity: common definitions and terminology (national CSIRT, incident taxonomy, CSIRTs typology, etc.) in line with CEF CSP implementation S: Q1-Q4, continue activities and involvement in CSIRT structures (e.g. FIRST, TF-CSIRT, NATO NCIRC, GFCE)	CSIRTs landscape report based on input from at least 30 European countries. 2 inventory updates (Q2, Q4) During 2018, support provided at least for 2 incident response stakeholders to enhance their CSIRT baseline capabilities or maturity. At least 2 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 — CERT-EU engagement on behalf of ENISA and EU agencies	S: Attending CERT-EU SB meetings S: Liaison with EU agencies using CERT-EU services	Consultation with EU agencies and representing their views at CERT-EU SB level.
Objective 3.3. Assist in improving general awareness		
Output O.3.3.1 — Cyber Security Challenges	S: Q1-Q4: European Cyber Security Challenge support E: Q2-Q3: 'Award workshop' for winners of the European Cyber Security Challenge 2018 (ENISA promotes best of the best)	At least 2 additional EU Member States organise national cybersecurity challenges in 2018 and participate in the European Cyber Security Challenge Final.
Output O.3.3.2 — European Cyber Security Month deployment	S: Q1-Q4: ECSM support P: Q4, An evaluation report P: Q4, A report on cybersecurity culture guidelines testing	All 28 EU Member States and other partners and representatives from different bodies/Member States participate in/support ECSM 2018 (private and public sectors).
Objective 3.4. Response to Article 14 requests under capacity activity		
Output O.3.4.1. Response to requests under capacity activity	S: Answers to requests.	

3.4 ACTIVITY 4 — COMMUNITY. FOSTER THE EMERGING EUROPEAN NETWORK AND INFORMATION SECURITY COMMUNITY

3.4.1 Objective 4.1. Cyber crisis cooperation

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 CSIRTs Network set up under the NIS directive.

The high-level exercise programme brief will include the strategic dimensions of the exercise and 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 MB after consultation with the Member State Cooperation Group and the CSIRTs Network set up under the NIS directive. Following this ENISA will assemble a group of planners from the participating countries to work closely towards developing a detailed exercise plan (ExPlan) in 2017-2018. ENISA will involve the group of planners in the relevant planning steps and take into account their input. The exercise planning will avoid overlaps with other major related activities.

ENISA will consult Member States and seek the agreement of its MB after consultation with the Cooperation Group and the CSIRTs Network on a possible joint EU–NATO cyber exercise in the coming year.

Finally, in 2018 ENISA will organise the EuroSOPEx exercise for the EU public authorities' points of contact, as these will be represented in the CSIRTs Network only to keep and even raise the momentum of cooperation between them. As in previous years the exercise will be planned with the support of representatives from the organisations involved. The exercise is expected again to have as high-level goals to raise awareness of cooperation procedures, train participants in using the cooperation infrastructure, such as structures relating to communication and information sharing, and ultimately contribute to increased trust within the CSIRTs Network. Guidance should be found within the CSIRTs Network on planning the exercise. No private or other entities will be involved in this exercise.

Output O.4.1.2 — Lessons learnt and advice related to cyber crisis cooperation (Priority 1)

Since 2015 ENISA has provided the secretariat for the Member States developing standard EU-level operational and technical cooperation procedures. The upcoming policy framework, the NIS directive, is expected to strengthen this by making this supporting role more formal as the secretariat for the cooperation of the EU operational cybersecurity network (CSIRTs Network).

In this context, ENISA will offer support for the network, helping the further development of EU-level cooperation with standard operation procedures at both levels, including the point of contact management. Alert exercises and communication checks will also be organised based on the defined procedures.

ENISA will also support the 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 the Commission communication on strengthening Europe's cyber resilience system (COM(2016) 410). ENISA will review and highlight the cyber crisis management good practices. Already existing schemes will form 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.

Output O.4.1.3 — Support activities for cyber exercise planning and cyber crisis management (Priority 1)

Cyber Exercise Platform (CEP) development and content management

ENISA has been developing the Cyber Exercise Platform (CEP) since 2014. CEP hosts a number of services that ENISA offers to the Member States and EU institutions, such as exercise organisation and management, an 'exercise playground' with technical incidents, a map of exercises and hosting of the exercise development community. With this

activity, ENISA would like to maintain and enhance the experience offered by CEP, including user support.

In addition, new content and exercise incident challenges and material will be developed in order to retain the interest of the stakeholders and make CEP a central tool in cybersecurity exercising for all stakeholders. The CEP platform opens new opportunities for ENISA to enlarge the user base and thus offer to the operational cybersecurity 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 CEP registrations.

EU-level cyber crisis and incident management procedures and Connecting Europe Facility (CEF) Cybersecurity Digital Service Infrastructure (DSI)

In 2018 ENISA will have to start preparing to manage, support and operate the centralised components of the MeliCERTes platform, formerly known as the CEF CSP Cybersecurity DSI Core Service Platform. MeliCERTes is expected to be the key cooperation mechanism for computer emergency and response teams in the European Union and will enhance the EU-wide capability for preparedness, cooperation and information exchange for a better coordination and response to cyberthreats and crises. With the final responsibility for MeliCERTes, and for its maintenance, ENISA is following closely the development of the platform and is actively supporting the Commission and the consortium in the different activities which are being carried out.

By the end of 2018 ENISA will be expected to have implemented some of the systems and functionalities for the management, maintenance and further development of the MeliCERTes platform, together with the development of some of the related internal and external operational processes.

Finally, following possible requests or support by national authorities, EU bodies and organisations on the organisation and planning of exercises, ENISA may offer training on CEP and on cyber crisis management (CCM).

3.4.2 Objective 4.2. CSIRT and other NIS community building

Output O.4.2.1 — EU CSIRTs Network secretariat and support for EU CSIRTs 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 of the members of the CSIRTs 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's 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 work programme2015, subject to the agreement of the CSIRTs Network.

Trust is an important asset for CSIRT operations and so 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's governance.

The Agency will further improve, develop and secure the CSIRTs Network infrastructure for its members' smooth collaboration and administration use (CSIRTs Network portal and other communication means).

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

In 2018 the key goal will be to build upon the progress ENISA has made in supporting different operational communities (e.g. CSIRTs, law enforcement, European FI-ISAC) to enhance mutually satisfactory ways to collaborate and support exchange of good practices among different stakeholders in operational communities in Europe. In detail, ENISA will continue its effort to support the EU-wide objectives on the fight against cybercrime by liaising with various stakeholders at EU (e.g. Europol) as well as at Member State level.

3.4.3 Objective 4.3. Response to Article 14 requests under community activity

Output O.4.3.1 — Response to requests under community building activity (Priority 1)

Article 14 requests allow the Member States 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.

ENISA will further improve, develop and secure the CSIRTs Network infrastructure for its members' smooth collaboration and administration use (CSIRTs Network portal and other communication means).

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 output 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 % of EU/EFTA Member States and countries confirm their support for Cyber Europe 2018
Output O.4.1.2 Lessons learnt and advice related to cyber crisis cooperation	S: Support for the Cyber SOPs editorial team of the CSIRTs Network, Q4. P: Good practices in cyber crisis cooperation and management, Q4	At least 80 % of the participating Member States agree to the developed operational procedures
Output O.4.1.3 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 CSIRTs Network secretariat and support for EU CSIRTs Network community building	S: Provide CSIRTs Network secretariat tasks (e.g. logistics, organisation of the meeting, agenda management, meeting minutes; conference calls; working groups management and support; facilitate ad hoc operational cooperation) E: Network meetings organisation and support (maximum 3 events) S: Q1-Q4: Facilitate preparation of the first evaluation report for the Cooperation Group S: Q1-Q4, EU CSIRTs Network communication support; enabling new means for communication in line with decisions in the CSIRTs Network — communication check exercise S: Q1-Q4, Improve CSIRTs Network portal functions and security including data retention and storage policy E: Trust-building exercise (co-located with the regular network meeting) P: Q4, Further support for network-specific information exchange and secure communication issues (CSIRTs Network action plan review and update) P: CSIRT maturity assessment and peer review implementation and support	Engage all 28 designated Member State CSIRTs and CERT-EU in the activities described in the network work programme (action plan 2017-2022) 28 Member States' dedicated CSIRTs and CERT-EU participated in CSIRTs Network regular meetings Work of ENISA successfully reflected by existing CSIRT communities (FIRST, TF-CSIRT, EU CSIRTs Network) and other national CSIRTs networks. Input received from at least 10 Member State CSIRTs network teams for the portal's further development Provide guidelines for CSIRTs Network members for performing the self-assessment and peer review. Review, update and adoption of the mid-term goals of the action plan.
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 cooperation, Q4 E: Q3, annual ENISA/EC3 workshop for national and governmental CSIRTs and their LEA counterparts	At least 5 Member State CSIRT representatives and 5 Member State LEA representatives participate in the preparation of the report. At least 15 Member States participate in the 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

3.5.1 Objective 5.1. Management and compliance

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 Director's Office** Unit (EDO) has been established. The tasks covered by the EDO include: policy advice, legal advice, MB Secretariat and coordination and control of the work programme.

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

The EDO also supports the administration of the MB meetings and the administrative correspondence that takes place between meetings, including the management of the MB portal.

The EDO supports the Executive Director in his relations with the press.

In 2018 the EDO will continue to support the 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 programmes, projects and services relating to the overall management of the Agency, supporting the Executive Director's decisions in areas such 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's Internal Audit Service, the European Court of Auditors, the European Ombudsman, the European Anti-Fraud Office, DG Human Resources and Security, DG Budget, DG Communications Networks, Content and Technology, 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 effectiveness of the Agency, and provide a continuous contribution to the ENISA strategy both internally and externally, seeking the optimal solutions for delivering on its mandate and providing the required assurance over compliance.

The aim is to equip the Agency with adequate and modern procedures and tools to minimise the resources used across it, maximising the intended delivery of the work programme and statutory commitments.

Internal control

ENISA is in process of implemented a quality management system (QMS) to support its regulatory and strategic goals. It is following as indicative the ISO 9001:2015 standards as they are designed to help organisations ensure that they meet the needs of customers and other stakeholders while meeting statutory and regulatory requirements. The methodology is based on the Plan-Do-Check-Act (PDCA) cycle that has been duly documented in a dedicated SOP and applied accordingly.

Internal Control reviews and evaluates risk management, governance and internal control processes of the Agency, in order to provide independent and objective assurance to the Senior Management, Executive Director and the MB.

IT

In 2015 ENISA set out to define its ICT strategy for the years 2015-2018. The main thrust of this strategy is to consolidate systems and applications on a maximum of two platforms, maximise data sharing, make applications available in a secure way on the most widely used mobile devices and to progressively move the Agency's IT infrastructure to the Cloud. Due to the size of the Agency and effective resources management, the IT tasks will be outsourced as far as possible to concentrate the available resources in the operational area of the Agency.

By mid-2018 it is expected that all business applications will be securely available on the most widely used mobile

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 %

devices. By this timeframe the platform consolidation should be complete and mature, with adequate, flexible and advance reporting and monitoring tools. It is expected that the support technology in the Agency will be consolidated in 2018, with modern, adequate and flexible business applications.

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 sound financial management, efficiency and economy principles as set down in the financial regulation. As the Agency resources are derived from the EU budget, management is required to comply with a set of regulations, rules and standards set out by the competent EU institutions. The Finance, accounting and procurement unit is responsible for high-quality reporting (annual accounts) and contributions 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 including applications for budget management, budget reporting and procurement planning and 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 with 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's annual and multiannual programming from inception to execution. The financial resources are allocated according to the expressed needs of the organisational units reflecting the priorities set by the Agency's management.

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 %

Key objectives for the year 2018 include high budget commitment and payment rates, a low number of budget transfers during the year, planned and justified carry overs and reduced average payment delays.

Human resources

The ultimate goal of the human resources (HR) unit is to attract, select, develop and retain highly qualified staff, to put in place optimal organisational structures, to promote a safe working environment and to create a culture that reflects ENISA's vision and values in which staff can give their best towards achieving the organisation's objectives. By offering a broad array of services (recruitment, performance management, learning and development, career management, working conditions, social rights, etc.) the objective is to deliver a successful day-to-day management of ENISA personnel and external staff (e.g. trainees) in compliance with the Staff Regulations. This is why more effort will be put into developing and deploying tools and policies 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 %	90 %	90 %
Respect the recruitment procedure time framework.	Average length of recruitment procedure: (in line with standard EU HR definition this is the time between the end of the publication and the signature of the reserve list by the ED)	3 months	3 months	3 months
Turnover of staff	Reduce the turnover of statutory staff (TA and CA)	< 12 %	< 12 %	< 12 %

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

- Inform and advise ENISA of its obligations pursuant to Regulation 45/2001/EC[27] 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 for exercising their rights under the Regulation, as well as the requirements for prior checks 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 the EDPS on issues related to the processing of personal data; cooperate and consult with the EPDS whenever needed.

Legal affairs, data protection and information security coordination

Legal affairs

The Legal Affairs Unit will continue supporting the legal aspects associated with the operation of the Agency. This includes dealing with matters such as contracts, procurement, employment-related issues, data protection and corporate governance. The legal affairs function also includes dealing with complaints to the European Ombudsman and representing the Agency before the Courts of the Union.

Data protection compliance tasks and data protection office

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 on developing and implementing information security policies, standards, guidelines and baselines that seek to secure the confidentiality,

27 Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF . Note that the Regulation is currently under review, see relevant European Commission's proposal: http://ec.europa.eu/newsroom/document.cfm?doc_id=41158

integrity and authentication of the information systems of the Agency. The ISO is instrumental in incident handling and incident response and security event monitoring. It also leads the security training for the Agency's staff and 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 in IT security.

3.5.2 Objective 5.2. Engagement with stakeholders and strong international activities

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 including institutional and industry representatives, academics, citizens etc.

Dissemination and outreach

The Agency will continue developing various tools and channels including its website with a strong emphasis on social media. Dissemination activities are the responsibility of the stakeholders' communication team, which will seek the appropriate level of outreach activities to take ENISA´s work to all interested parties and to provide added value for Europe.

ENISA´s image of quality and trust is paramount for all stakeholders. It is of utmost importance to have EU citizens from all backgrounds trust in ENISA's work. The cybersecurity challenges are increasing throughout the world and Europe is no exception. With this objective, ENISA´s image needs to be continuously reinforced. Outreach for the Agency's work is essential to create a strong NIS culture among the various actors in Europe. ENISA is well aware of this fact and will work with all interested parties to reach the citizens that require information about its work.

Activities are planned in several Member States to engender cybersecurity awareness across Europe, fulfilling ENISA´s mandate, mission and strategy up until 2020.

Internal communications

Stakeholder communications cover both internal and external groups. From an internal perspective the team is responsible for supporting communication activities that 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 programme. An annual review of this strategy is envisaged to ensure that it is kept up to date and appropriate for the Agency.

Permanent Stakeholders Group

In 2018, ENISA will continue to reinforce the contribution of the Permanent Stakeholders Group (PSG) to the work programme.

The PSG is composed of 'nominated members' and members appointed 'ad persona'. The total number of members is 33 and they come from EU and EFTA countries. They 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 'nominated members' represent national regulatory, data protection and law enforcement authorities.

Task	Objective	How to measure the indicator	Level of completion		
			2018	2019	2020
Level of staff satisfaction with internal communications	Measure user satisfaction	Ad hoc survey or included in the regular staff survey	70 %	80 %	90 %
Audience reached by internal communication	Measure the audience reached through different internal communication channels (e.g. intranet, newsletters, staff meetings)	• Intranet statistics (general and by content) • Number of newsletter sent • Level of participation in staff meetings	70 %	80 %	90 %

The PSG is established by the ENISA regulation ((EU) No 526/2013). The MB, acting on a proposal by the Executive Director, establishes a PSG for a term of office of 2.5 years.

A new PSG was elected in 2017.Its role is to advise the Executive Director on the development of the Agency's work programme, and on ensuring communication with the relevant stakeholders on all related issues.

National Liaison Officer network

ENISA kicked off various activities aiming at strengthening cooperation with its National Liaison Officers' (NLO) network in 2017. NLOs are key actors for the Agency's daily work and they warrant the interaction with select public sector entities in the Member States while they provide assurance in terms of outreach effective liaison with the Member States and dissemination of ENISA deliverables.

In 2018 ENISA will build upon these activities and strengthen its cooperation with the NLO network, as the first point of contact with the Member States, with an emphasis on:

- an NLO meeting to discuss possible improvements in the collaboration with ENISA and input to selected ENISA projects, aimed at leveraging the NLO network for the dissemination of ENISA's work to the Member States and EFTA countries;.
- sending information to the members of the NLO network at regular intervals on upcoming ENISA project-related tenders, vacancy notices and events organised by ENISA or to which it contributes (for example as co-organiser, etc.);
- maintaining and sharing with the NLO network information on all relevant ENISA projects and activities (e.g. the unit responsible for a particular project, relevant tender results, etc.) while maintaining and expanding online resources available as appropriate.

Additionally, guidelines provided by the MB on missions, objectives and functioning of the NLO network will guide the development of this important tool for community building.

International relations

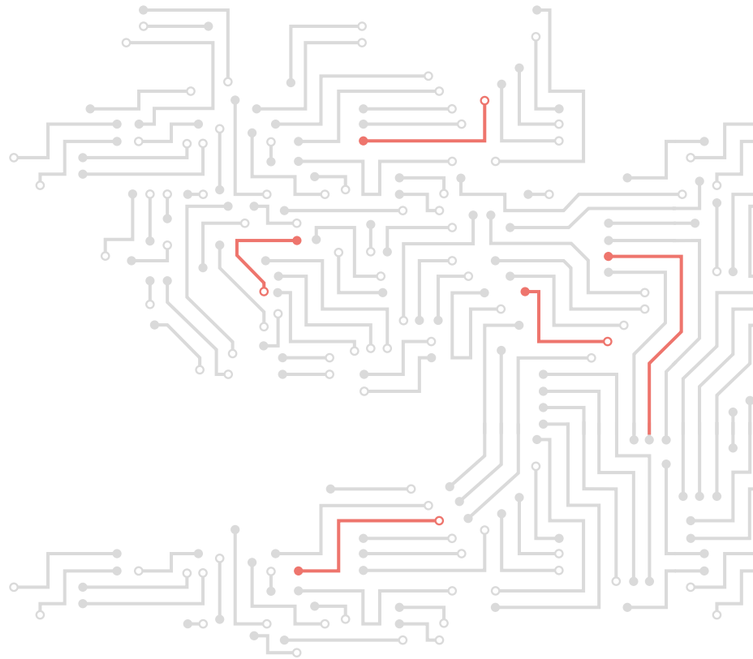
Under the Executive Director's guidance and initiative, ENISA will seek to strengthen contacts at an international level.

ENISA should participate in international cybersecurity fora such as the Organisation for Economic Cooperation and Development (OECD), ICANN and the IGF in so far as these groups are discussing items related to the Agency's 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, the National Institute of Standards and Technologies in the US, 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 under takes for the NIS directive.
- Starting in 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 those of other global players. An example here is provided by the work that the International Telecommunication Union (ITU) is doing with CSIRTs, which needs to be aligned and will create added value and harmonisation for 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 Executive Director should attend international conferences in order to enhance the Agency's visibility.

3.6 LIST OF OUTPUTS IN THE 2018 WORK PROGRAMME

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 the internet of things
Objective 1.2. NIS threat landscape and analysis
Output O.1.2.1 — Annual ENISA threat landscape
Output O.1.2.2 — Restricted and Public Info notes on NIS
Output O.1.2.3 — Support incident reporting activities in the EU
Objective 1.3. Research and development, innovation
Output O.1.3.1 — Guidelines for European standardisation in the field of ICT security
Output O.1.3.2 — Priorities for EU research and development
Objective 1.4. Response to Article 14 requests under expertise activity
Output O.1.4.1 — Response to requests under expertise activity
Activity 2 — Policy. Promote network and information security as an EU policy priority
Objective 2.1. Supporting EU policy development
Output O.2.1.1 — Support the policy discussions in the area of certification of products and services
Output O.2.1.2 — Towards a framework for policy development in cybersecurity
Objective 2.2. Supporting EU policy implementation
Output O.2.2.1 — Recommendations supporting implementation of the eIDAS regulation
Output O.2.2.2 — Supporting the implementation of the NIS directive
Output O.2.2.3 — Baseline security recommendations for the OES sectors and DSPs
Output O.2.2.4 — Supporting the payment services directive (PSD) implementation
Output O.2.2.5 — Contribute to EU policy in the area of privacy and data protection
Output O.2.2.6 — NIS directive transposition
Objective 2.3. Response to Article 14 requests under policy activity
Output O.2.3.1 — Response to requests under policy activity
Activity 3 — Capacity. Support Europe in 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 training for Member States and EU bodies
Output O.3.1.2 — Support EU Member States in the development and assessment of NCSS
Output O.3.1.3 — Support EU Member States in their incident response development
Objective 3.2. Support EU institutions' capacity building.
Output O.3.2.1 — Representation of ENISA on the Steering Board of CERT-EU and representation of the EU agencies using the CERT-EU service
Objective 3.3. Assist in improving general awareness
Output O.3.3.1 — Cyber Security Challenges
Output O.3.3.2 — European Cyber Security Month deployment
Objective 3.4. Response to Article 14 requests under capacity activity
Output O.3.4.1 — Response to requests under capacity activity
Activity 4 — Community. Foster the emerging European network and information security community
Objective 4.1. Cyber crisis cooperation
Output O.4.1.1 — Cyber Europe 2018
Output O.4.1.2 — Lessons learnt and advice related to cyber crisis cooperation
Output O.4.1.3 — Support activities for cyber exercise planning and cyber crisis management
Objective 4.2. CSIRT and other NIS community building.
Output O.4.2.1 — EU CSIRTs Network secretariat and support for EU CSIRTs Network community building
Output O.4.2.2 — Support the fight against cybercrime and collaboration between CSIRTs and LEA
Objective 4.3. Response to Article 14 requests under community activity
Output O.4.3.1 — Response to requests under community building activity



A

ANNEX 1
RESOURCE ALLOCATION PER ACTIVITY 2018–2020

Sections A.1.1 and A.1.2 of this Annex present the evolution of the past and current situation as well as the outlook in a chart showing the distribution of resources proposed for 2018, while Section A.1.3 provides allocations per activities.

A.1.1 OVERVIEW OF THE PAST AND CURRENT SITUATION

The work programme for 2018 follows the COM guidelines C(2014) 9641 final from 16.12.2014 and MB decisions. It is structured following the objectives and the priorities of the Agency as described in the new ENISA strategy.

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

In 2017, however, a slight increase in Title II was adopted. In 2018, the budget of Title III will be optimised in order to increase the budget in operations.

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

From 2015 until 2018, some reorganisations were carried out in order to maximise the efficiency, effectiveness and use of the posts attributed to the Agency.

The human and financial resources in respect of the past and current situation are presented in the annexes to this report.

A.1.2 RESOURCE PROGRAMMING FOR THE YEARS 2018–2020

The distribution of the 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 Annex A.1.3. The budget and posts distribution is based on the activity-based budgeting (ABB) methodology of the Agency detailed in Annex A.1.3.

Following the publication of the NIS directive the Agency is reallocating budget and resources to the new tasks/activities envisaged for the Agency in the directive. Another area which will probably require more budget/resources is the Cyber Security 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 will any other relevant changes in ENISA's scope and tasks.

The Stakeholders Relations and Administration Department has already optimised all its resources. Improvements to achieve gains in effectiveness and

efficiency have been developed. ENISA performs an internal check of relevance and optimisation of workflows, procedures and rules, to seek optimisation and efficiency. As an example the so-called 'Paperless', (electronic workflow IT tool) which routes documents to staff involved in preparation, review and approval of all kinds of documents and transactions, represents a huge improvement and cost savings in all processes of the Agency.

Moreover, the Stakeholders Relations and Administration Department applies a strict policy on the ratio between administrative support and coordination staff and operational staff, according to the methodology set by the European Commission and the benchmarking exercise within the institutions and EU agencies. In December 2016 only 19.04 % of staff occupied administrative support and coordination functions, although the Commission benchmark allows for a level of up to 25 %.

Job type	2016	2015
Total administrative support and coordination	19.04 %	20.22 %
Administrative support	15.47 %	16.85 %
Coordination	3.57 %	3.37 %
Total operational	66.66 %	66.29 %
Top operational coordination	7.14 %	8.99 %
General operational	59.52 %	57.30 %
Total neutral	14.29 %	13.48 %
Finance and control	14.29 %	13.48 %

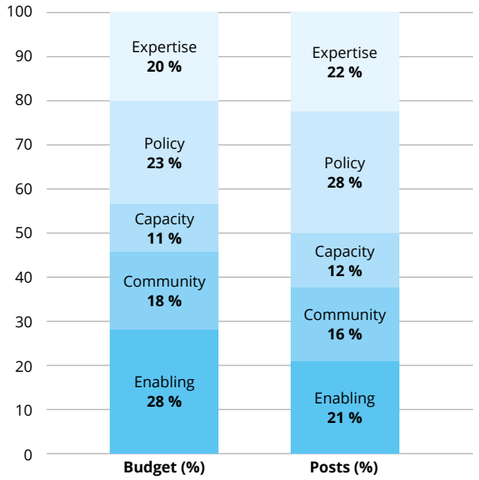
In addition, this version of the work programme takes account of the prioritisation exercise carried out during the consultation with the MB. Certain activities had to be removed from the work programme as there are not enough resources for the year 2018. Such de-prioritising activities include:

- activities to support a DSM for high-quality NIS products and services;
- support for the assessment of existing policies/procedures/practices on NIS within EU institutions;
- planning and organisation of EuroSOPEx 2018.

For the years 2019-2020, the Agency will gradually increase the share of Activity 2, Policy, if more resources become available.

The budget and resources allocations within the summary tables and annexes are in line with COM(2013) 519[28].

Budget and posts distribution (ABB)



28 Communication from the Commission to the European Parliament and the Council 'Programming of human and financial resources for decentralised agencies 2014-2020', available at: http://ec.europa.eu/budget/library/biblio/documents/fin_fwk1420/COM_2013_519_en.pdf

A.1.3 OVERVIEW OF ACTIVITIES' BUDGET AND RESOURCES

The budget and posts distribution is based on the 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 enable better estimation of resources needed for each ENISA activity, the budget forecast should be split into 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 redistributed 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 redistribution.

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

Title	Total ABB budget (EUR)	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	2 657 730.16	23.05
Activity 3 — Capacity. Support Europe in setting up state-of-the-art network and information security capacities	1 233 285.46	10.33
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**

ANNEX 2

HUMAN AND FINANCIAL RESOURCES 2018–2020

The tables below show the expected expenditure based on the same structure for the next 3 years. Seven SNEs were approved for ENISA without any additional budget to recruit them.

EXPENDITURE OVERVIEW

Job type	2017		2018		2019		2020	
	CA	PA	CA	PA	CA	PA	CA	PA
Title 1	6 387 979	6 387 979	6 386 500	6 386 500	6 492 000	6 492 000	6 597 120	6 597 120
Title 2	1 770 700	1 770 700	1 687 500	1 687 500	1 741 000	1 741 000	1 797 500	1 797 500
Title 3	3 086 000	3 086 000	3 375 000	3 375 000	3 426 000	3 426 000	3 479 380	3 479 380
Total expenditure	**11 244 679**	**11 244 679**	**11 449 000**	**11 449 000**	**11 659 000**	**11 659 000**	**11 874 000**	**11 874 000**

CA – Commitment appropriations, PA – Payment appropriations

The tables on the following pages show the commitments and payment appropriations based on the same structure for the coming years.

Commitment appropriations

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**

Payments appropriations

Expenditure	Payment 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**

Table 2 — Revenue overview

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**

Revenue

Revenues	2016	2017	2018		VAR 2018 /2017	Envisaged 2019	Envisaged 2020
	Executed budget	Budget	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	0		0.00 %	0	0
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**

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	11 034 366
Payments made (-)	8 710 278	9 395 559	9 860 775
Carry-over of appropriation (-)	1 333 221	674 521	1 176 717
Cancellation of appropriations carried over (+)	74 505	80 675	38 616
Adjustment for carry over of assigned revenue appropriations from previous year (+)		800	3 127
Exchange rate differences (+ /-)	291	278	-180
Adjustment for negative balance from previous year (-)			
Total	**50 269**	**80 397**	**38 436**

Cancellation of appropriations

Cancellation of commitment appropriations
No commitment appropriations were cancelled.

In 2016 ENISA demonstrated 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 EUR 968 198.32, representing 9.29 % of total C1 appropriations 2016 (up 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.

ANNEX 3
HUMAN RESOURCES — QUANTITATIVE

Table 1 — Staff population and its evolution; overview of all categories of staff

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	28	34	33	34	34	34
	AST	15	14	15	14	14	13	13	13
	AST/SC								
Total		**45**	**48**	**43**	**48**	**47**	**47**	**47**	**47**
CA GFIV		9	16	12	28	18	28	28	28
CA GF III		11	15	12	2	13	2	2	2
CA GF II		1	1	0	0	0	0	0	0
CA GFI		1	1	1	0	1	0	0	0
Total CA		**22**	**33**	**25**	**30**	**32**	**30**	**30**	**30**
SNE		**2**	**3**	**1**	**6**	**3**	**6**	**6**	**6**
Structural service providers									
TOTAL		**69**	**84**	**69**	**84**	**82**	**83**	**83**	**83**
External staff for occasional replacement									

NB: An additional 7 SNE positions were granted to the Agency without the corresponding budget so selections could not take place as budget was not available.

Table 2 — Multiannual staff policy plan for 2018–2020

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	
	OF	TA	OF	TA	OF	TA	OF	TA	OF	TA	OF	TA	OF	TA	OF	TA
AD 16																
AD 15		1		1				1				1		1		1
AD 14																
AD 13																
AD 12		3		2				3				3		3		3
AD 11				1												
AD 10		5		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				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**				**47**		**47**		**47**

OF – Officials

ANNEX 4
HUMAN RESOURCES — QUALITATIVE

A4.1 RECRUITMENT POLICY

Statutory staff

The recruitment procedure itself, as laid down in the Staff Regulations, is being streamlined to improve time-to-hire and to optimise procedures.

ENISA is implementing actions including:

- launching numerous calls and exploring effective reserve lists;
- enhanced visibility of career opportunities via revamped job vacancy templates, targeted dissemination of vacancies through traditional routes across Member States and proactive use of social media;
- increased quality of recruitment documents with new FAQs for candidates, new guidelines for Selection Boards and new and simpler financial rules for the reimbursement of candidates;
- the acquisition in 2018 of a modern e-recruitment tool;
- development of modern competency-based interview questions;
- optimisation of internal procedures bringing efficiency in delivering services and projecting ENISA's image in the European Job Market.

The job family and job category framework is being consolidated in line with the Annex I of the SR:

Assistant Job Family:

- Assistant Job Category (staff carrying out administrative, technical activities such as assistance and/or secretariat requiring a certain degree of autonomy): typically, these posts are filled by grades SC1-SC2, AST1-AST3, FGI, FGII
- Technical Assistant Job Category (staff providing support with a medium degree of autonomy in the drafting of documents and assistance in the implementation of policies/projects/procedures/processes): typically, these posts are filled by grades AST4-AST7, FG III
- Senior Assistant Job Category (staff carrying out administrative, technical activities requiring high degree of autonomy and carrying out significant responsibilities in terms of staff management, budget implementation or coordination): typically, these posts are filled by grades AST7-AST11 and only for the two Assistants to Head of Departments by FG IV

Operational Job Family:

- Junior Officer/Administrator Job Category (staff providing junior expertise in a specific field of knowledge): typically, these posts are filled by grades AD5, FG IV 13
- Officer/Administrator Job Category (staff providing officer expertise in a specific field of knowledge): typically, these posts are filled by grades AD6-AD7, FG IV 14-18
- Lead Officer/Administrator (staff providing top level expertise in a specific field of knowledge): typically, these posts are filled by grades AD8-AD9
- Team Leader Job Category (staff providing operational excellence with some managerial responsibilities): typically, these posts are filed by grades AD7-AD9, FG IV 14-18

Managerial Job Family:

- Middle Manager Job Category (staff providing operational vision and managerial expertise including financial management): typically, these posts are Head of Unit positions filled by grades AD9-AD12
- Senior Manager Job Category (staff providing strategical vision and managerial expertise including financial expertise): typically, these posts are Head of Department position (filled by grades AD11-AD13)
- Executive Director (filled by grades AD14-15)

Following the 2014 SR reform, ENISA adopted and is applying the new implementing rules on the engagement and use of Temporary Staff for Agencies (TA 2f), thus ensuring a more consistent staff policy and allowing inter-mobility between EU agencies.

Concerning the duration of employment, Temporary Agents and Contract Agents are offered typically long term contract of three years, renewable for another limited period of 5 years. These contracts are converted into contracts of indefinite period if a second renewal is offered and accepted. All contracts renewals are subject to an assessment of the performance of the staff member and depend on budget availability and the business needs for the function occupied as stipulated in the ED Decision 38/2017 of 6 June 2017 concerning employment contract renewal. In addition, ENISA is activating short-term contract agents (2 years, renewable once for a maximum 1 year) to be allocated depending on business needs or any other human resources constraints (such as long-term sick leave or part time, etc.). This engagement of staff allows the Agency to keep an adequate degree of flexibility and adapt the workforce based in the business needs.

Non-statutory staff

ENISA welcomes Seconded National Experts (SNEs) as an opportunity to foster the exchange of experience and knowledge of the Agency working methods and to widen the expertise network. Experts can be seconded to ENISA for the duration of a minimum 6 months to a maximum of 4 years. ENISA offers paid traineeship opportunities to talented, highly qualified young professionals at the start of their careers, in a field of their choice. Trainees have the opportunity to immerse themselves in the Agency's work and in the European system in general. The traineeship may last from a minimum of 6 months to a maximum of 12 months.

Finally, in compliance with both the EU legal framework and Greek labour legislation, ENISA's policy is intended to rely on interim services under specific circumstances and for a limited period of time. The Agency holds a framework contract which has been awarded to a temping agency.

A.4.2 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 drives 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 appraisal and promotion are two different exercises.

Table 1 — Reclassification of temporary staff/promotion of officials

Category and grade	Staff in activity at 1. 1. 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. 1. 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. MOBILITY POLICY

All internal moves are processed via Article 7 of the Staff Regulations and for transparency purposes are published internally on INTRAENISA. In order to create a motivated and versatile workforce, ENISA has adopted an ED Policy 01/2017 of 22 February 2017 on Internal Mobility Policy. ENISA also joined the inter-agency job market (IAJM) with the view, as for all other agencies, to offer possibilities of mobility to staff in Agencies by assuring a continuation of careers and grades. In 2016, 1 staff member moved via the IAJM.

Additionally, ENISA is also opened to mobility between the Agencies and the EU Institutions. In 2016 no mobility was organised and in 2017 one mobility was organised.

A.4.4. LEARNING AND DEVELOPMENT

In order to make the most out of its internal expertise and to develop mechanisms to retain staff, the organisation is focusing on developing an ENISA's learning and development framework 2017-2020. The objective is to ensure the efficient delivery of learning interventions, the compliance with mandatory training (e.g. Ethics and Integrity) and to support the acquisition of specific and strategic knowledge.

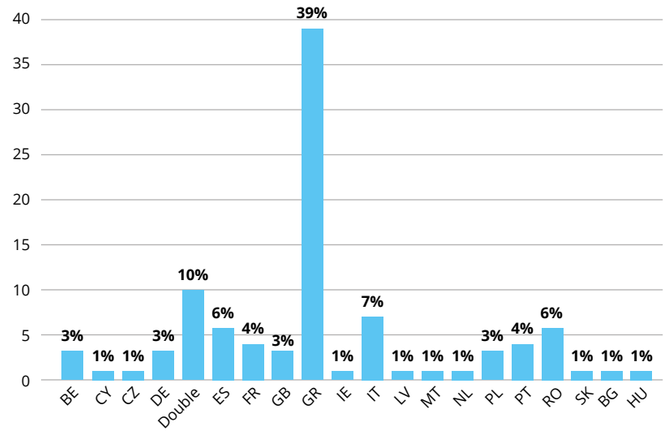
A.4.5. GENDER AND GEOGRAPHICAL BALANCE

Total number of Staff as of 31/12/2016: 69 (43 TA's: 28 AD's + 15 AST's + 25 CA's + 1 SNE).

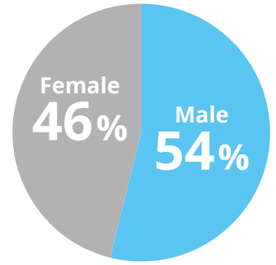
The overall gender balance among ENISA staff shows a male prevalence which is understandable given the scope of the Agency's work. As a measure to promote equal opportunities, the terms of published vacancy notices prevent any kind of discrimination and the Selection Board's composition is balanced in term of gender and nationality as far as possible. For instance, in 2016 the Management Team welcomed a French female manager as Head of HR and ENISA will pursuit this objective.

With regard to the geographical balance, while there is no quota system in operation, the Staff Regulations require when recruiting to strive for a broad balance among nationalities and to adopt measures if there is imbalance between nationalities among staff. ENISA is paying great attention to this requirement as reflected by the latest recruitments.

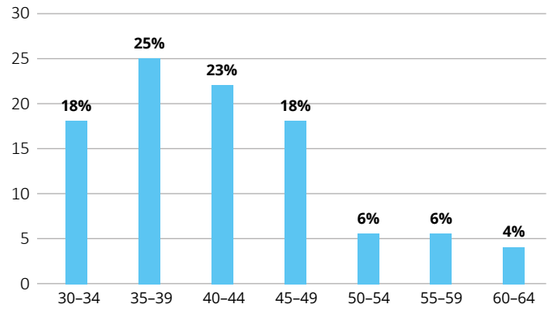
Per Nationality



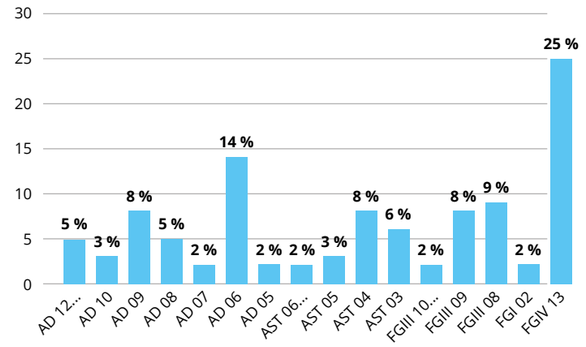
Per Gender



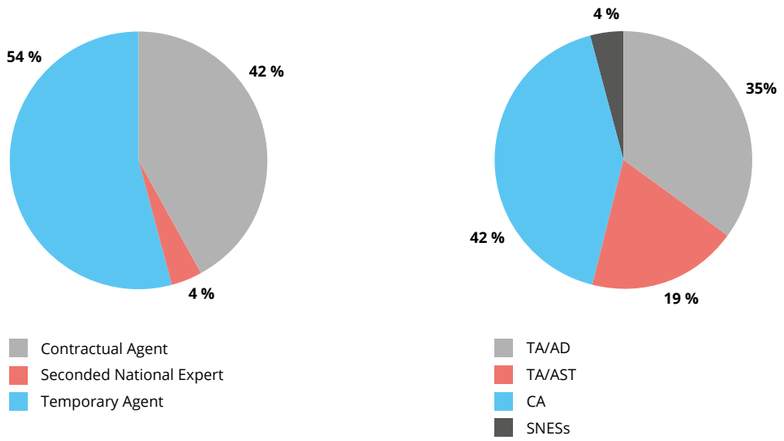
Per Age



Per Category



Per Category



A.4.6. SCHOOLING

A European School is located in Heraklion and is used by ENISA staff (for the school year 2016-2017, only 4 pupils attend nursery/primary school and 2 pupils attend Secondary school).

The rest of ENISA pupils attend various schools in Athens based on service level agreement concluded with a number of international schools (for the school year 2016-2017, 20 pupils attend nursery school, 20 pupils attend kindergarten school and 18 pupils attend primary and secondary school). ENISA considers schooling as an essential part of its Staff Policy and thus, contribute to the expenses of school care for the children.

ANNEX 5
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 2017.

ANNEX 6
PRIVILEGES AND IMMUNITIES

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

ANNEX 7
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.

Overall, the evaluation of activities foreseen in the 2014 work programme concludes 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

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 cybersecurity area, with a lack of trust among stakeholders, weaknesses and differences in national capabilities, weak communication structures, insufficient exchanges of information in 'real life' etc., representing hurdles that need to be surmounted over the medium to long term.	Continue trust building and cooperation activities as a means to overcome barriers to cooperation during crisis.
Efficiency	The operational budget of ENISA is limited, and the main expenditure relates to staff costs. In the light of the resources available (staff and expenditures), ENISA manages to produce quite a high number of deliverables which also have generated considerable outreach in terms of downloads. No indication of low efficiency was identified in the evaluation period, though specific cost saving measures could not be established.	N/A
Coordination and coherence	Overall, it can be concluded that ENISA effectively cooperates and engages with its main stakeholders, as stipulated in its mandate. The support provided by ENISA is seen as a complement to that of other public interventions, and no adverse effects were identified.	N/A

ANNEX 8
RISKS FOR 2018

The Risk Assessment is ongoing by the European Commission's Internal Audit Service (IAS).

ANNEX 9
PROCUREMENT PLAN FOR 2018

The Risk Assessment is ongoing by the European Commission's Internal Audit Service (IAS).

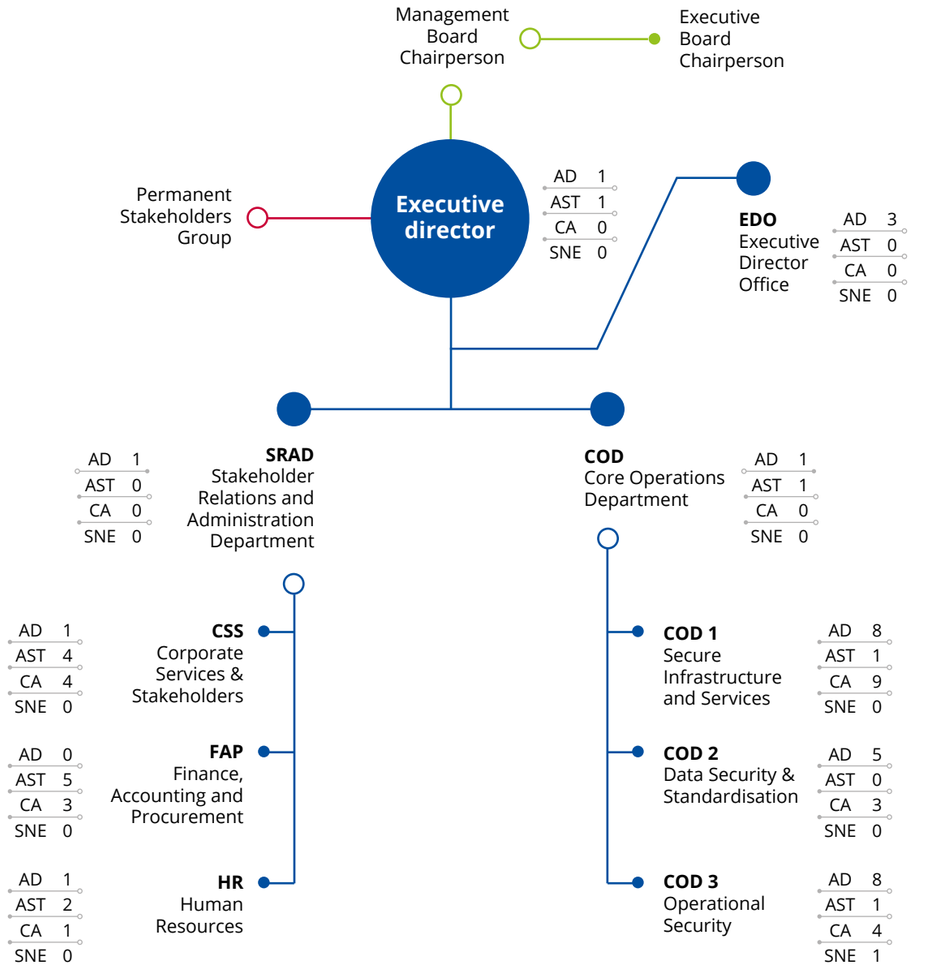
2018 work programme procurement planning — Preliminary budget breakdown	Direct budget (in EUR)	Procurement (tender) procedure required	Launch Q1-Q4?	All other expenditure
Activity 1 — Expertise. Anticipate and support Europe in facing emerging network and information security challenges	557 500.00	415 000.00	Q1-Q4	142 500,00
Activity 2 — Policy. Make network and information security an EU policy priority	646 500.00	460 000.00	Q1-Q4	186 500,00
Activity 3 — Capacity. Support Europe in setting up state-of-the-art network and information security capacities	300 000.00	130 000.00	Q1-Q4	170 000,00
Activity 4 — Community. Make the European network and information security community a reality	496 000.00	355 000.00	Q1-Q4	141 000,00
Activity 5 — Enabling. Reinforce ENISA's impact				
Objective 5.1. Management and compliance				
Management and Compliance	265 000.00	140 000.00	Q1-Q4	125 000.00
Objective 5.2. Engagement with stakeholders and International relations				
Engagement with stakeholders and International relations	505 000.00	370 000.00	Q1-Q4	135 000.00
Total Activity A5	**766 000.00**	**510 000.00**		**256 000.00**
Total A1-A5	**2 766 000.00**	**1 870 000.00**		**896 000.00**

ANNEX 10
ENISA'S ORGANISATION

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

- A Management Board: The MB ensures that the Agency carries out its tasks under conditions which enable it to serve in accordance with the founding regulation.
- An Executive Board: The Executive Board prepares decisions to be adopted by the MB 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 organised as follows (staffing as 31. 12. 2016):



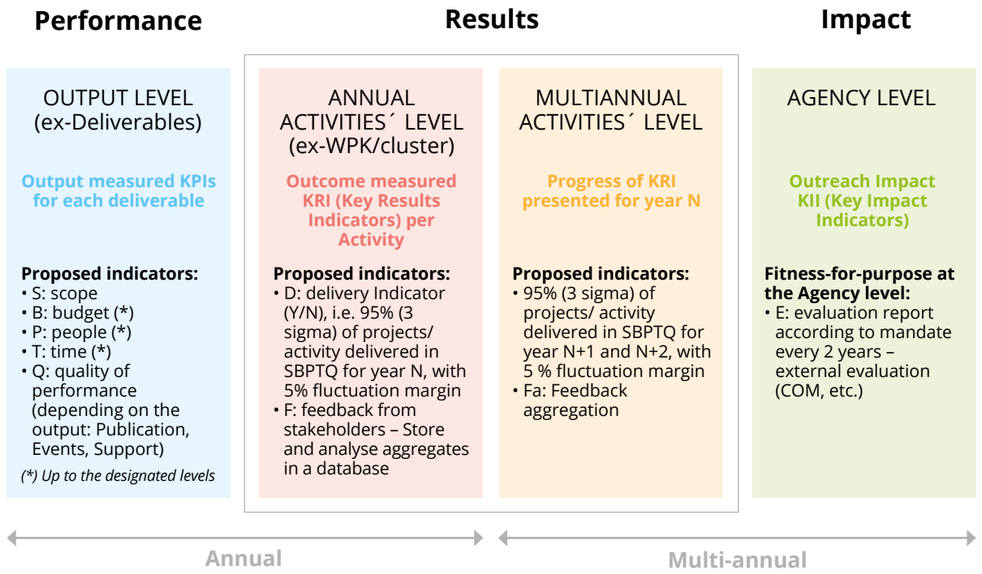
ANNEX 11

SUMMARISING THE KEY INDICATORS FOR THE MULTIANNUAL ACTIVITIES

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

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

The chosen approach initially sets the designated levels of key indicators; each type of indicator is grouped alongside other similar ones at the appropriate level. This approach has been developed taking into account the capability of the Agency to report, and the need to avoid any unnecessary burden on the Agency. The Agency's capability to report reflects effort and 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 multiannual measurements are presented hereunder:



Key indicators at ENISA seek to measure:

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

- Results that are a concern at the annual and at multiannual activities' level. The indicators used are as follows:
  - Delivery indicator aiming at delivery of at least 95 % against work programme planning. This is equivalent to a 3σ (3 Sigma) organisation (reaching between 93.3 % and 99.3 %); clearly the Agency has historically proven its operational ability to deliver at much higher level, meeting 6σ (6 Sigma) specification requirements (at 99.99 %). However allowing for a 3 Sigma level meets the above-mentioned deviation rate of ± 5 %[29]. The criteria used, being scope, budget, people, time and quality, they all refer to the proper execution of the project leading up to the production of output. This evaluation is done at the end of the project within ENISA.
  - Following the production process that leads up to an output, feedback from stakeholders is collected on each output. Results are further aggregated on a multiannual 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 on the following page.

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

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

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

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

Key indicators in ENISA								
Output level			**Activities level**			**Agency level**		
Scope (e.g. Scope drift as compared to approved work programme plan)	S	Variable: TLR	Deliverables (number of deliverables realised against the work programme 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 multiannual 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, Member State participation etc.)	Q	Integer: quantitative target	(**)Aggregations of deliverables or categories thereof					

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 Member States involved, experts from Member State 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/ Member State 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 multiannual level.

Aggregated outcome at the annual activity level in years n, n+1 and n+2				Multiannual 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	Multiannual 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

ANNEX 12
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 Standardisation
CENELEC: European Committee for Electrotechnical Standardisation
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: Cybersecurity strategy
DG: European Commission Directorate-General
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 Director's 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
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
MFF: Multi annual financial framework
M2M: Machine to machine
MB: Management Board
MS: Member State
NAPARC: National Public Authority Representatives Committee
NCSS: National cybersecurity 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 organisation
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 training
TSP: Trust service provider
US: United States of America
WP: Work programme

ANNEX 13
LIST OF POLICY REFERENCES

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

Reference	Policy/legislation reference. Complete title and link
2016	
The NIS directive	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30, available at: ELI: http://data.europa.eu/eli/dir/2016/1148/oj
Commission 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
Commission 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) 2016/680 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, pp. 89-131, available at: http://data.europa.eu/eli/dir/2016/680/oj
PNR Directive	Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132–149, available at: ELI: http://data.europa.eu/eli/dir/2016/681/oj
2015	
Digital single market strategy for Europe (DSM)	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM/2015/0192 final, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX:52015DC0192

Reference	Policy/legislation reference. Complete title and link
Payment services directive	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), OJ L 337, 23.12.2015, p. 35–127, available at: http://data.europa.eu/eli/dir/2015/2366/oj
The European Agenda on Security	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, The European Agenda on Security, COM/2015/0185 final, available at:http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2015:0185:FIN
2014	
eIDAS regulation	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73–114, available at: http://data.europa.eu/eli/reg/2014/910/oj
Communication on thriving data driven economy	Towards a thriving data-driven economy, COM(2014) 442 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions, July, 2014, available at: https://ec.europa.eu/digital-agenda/en/news/communication-data-driven-economy
2013	
Council conclusions on the cybersecurity strategy	Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, agreed by the General Affairs Council on 25 June 2013, http://register.consilium.europa.eu/pdf/en/13/st12/st12109.en13.pdf
Cybersecurity strategy of the EU	Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667
ENISA regulation	Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, OJ L 165, 18.6.2013, p. 41–58, available at: http://data.europa.eu/eli/reg/2013/526/oj
Directive on attacks against information systems	Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14.8.2013, p. 8–14, available at: http://data.europa.eu/eli/dir/2013/40/oj
Framework financial regulation	Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council, OJ L 328, 7.12.2013, p. 42–68, http://data.europa.eu/eli/reg_del/2013/1271/oj
Commission 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 cybersecurity (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

Reference	Policy/legislation reference. Complete title and link
2011	
Council conclusions on CIIP	Council conclusions on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cybersecurity' (CIIP), 2011, Adoption of Council conclusions, available at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010299%202011%20INIT
Commission 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	
Commission 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

NOTES

TP-AH-18-001-EN-N

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 https://www.enisa.europa.eu

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

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

enisa.europa.eu

Publications Office

ISBN 978-92-9204-226-4