ENISA Programming Document 2019-2021

Including Multiannual planning, Work programme 2019 and Multiannual staff planning

STATUS: CLEAN DRAFT, V4

VERSION: NOVEMBER 2018

Document History

//DRAFT ONLY - THIS SECTION AND PAGE WILL BE DELETED ON FINAL PUBLICATION

DATE	VERSION	MODIFICATION	AUTHOR
December 2017	V1	First draft sent to MB for consultation.	ENISA
January 2018	V2	Updates based on feedback received from MB during consultation. **V2 is the Draft Programming Document 2019 adopted by written procedure by MB (according to Framework Financial Regulation provisions, by end of January 2018) and communicated to Council, EP and European Commission.**	ENISA
July 2018	V2.1.	This version includes changes in content and Annexes to address updates in NISD implementation discussions that took place after January 2018. Version discussed at the 19/07 MB meeting.	ENISA
August 2018	V2.2.	This version includes updates following the MB discussions of 19/07.	ENISA
September	V3	Version to be sent out to MB for decision during MB meeting of 11/10	ENISA
October 2018	V3.1	Version sent to MB on 19/10 for consultation. Deadline 2nd of November.	ENISA
November 2018	V4	Version addressing MB feedback and sent to MB for written approval.	ENISA

About ENISA

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

Table of Contents

Foreword by the Executive Director

While preparing the Work programme 2019 we are in a context of many expectations and positive prospects. ENISA welcomes the new proposed ENISA regulation, the Cybersecurity Act, which provides for a strengthened Agency with additional resources and staff. In addition, ENISA welcomes the 2017 Cybersecurity package of cybersecurity legislative and non-legislative measures. The Agency also looks forward to the new permanent mandate, for the additional resources and additional budget to contribute to the new tasks foreseen in the current version of the Cybersecurity Act.

ENISA welcomes cooperation in the area of cybersecurity. Current challenges are common worldwide; a lot of effort is needed to mitigate the risks and to address such global challenges. Many EU Member States (MS) will benefit from a joint approach and EU institutions and EU bodies like ENISA can help to foster effective EU cooperation, maximizing the outcome and impact of developed solutions, best practices, methodologies and mechanisms supporting cybersecurity.

ENISA welcomes the proposed tasks related to the education and improvement of skills to address the lack of digital and cybersecurity skills in the EU. At European level, there is an increased need for digital skills and cybersecurity skills in particular. It is acknowledged currently that 44% of European citizens do not have basic digital skills[1]; Europe also lacks skilled ICT specialists to fill the growing number of job vacancies in all sectors of the economy.

The Cybersecurity talent shortage[2] is estimated at more than a million openings worldwide with many thousands of companies having difficulties to fill in openings. The problem is here and is likely to stay. The global shortage of cyber security professionals is estimated at two million by 2019[3]. The ENISA Threat Landscape Report 2016 acknowledges the skills shortage[4] and recommends engagements in the areas of cyber-security education, training and awareness.

ENISA is ready to work closely with all relevant stakeholders to make the certification proposal a reality. ENISA welcomes the proposal for an EU wide cybersecurity certification framework presented in the draft Cybersecurity Act. It foresees amongst others: several assurance levels and specific evaluation criteria. In addition, The Cybersecurity Act draft proposes conditions for marking and labelling; it sets out the mechanisms to demonstrate continual compliance as appropriate; it provides for the conditions to grant maintenance and extension of a certificate etc.

The proposal is an EU initiative for an EU-based framework that meets the demand of private stakeholders as well as MS. The prospect for the market can be significant as the EU can reinforce its position in terms of internal market purchasing (private as well as through public procurement) and as a reference point to meet the challenge posed by global competition.

---

[1]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

[2]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/

[3] 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/

[4]ENISA, "*ENISA Threat Landscape Report 2016*", available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

ENISA is looking forward to assuming the new roles seeking to support the Commission in its duties and the MS in transitioning to an EU framework.

An agile ENISA, preparing for the future!
For several years, the agency has been improving its planning, and in consultation with its Management Board set out priorities for its activities in order to be able to deliver the most urgent, important and sensitive results for the protection our EU cyberspace. In the preparation of Work Programme 2019 ENISA, together with its MB, decided to prepare the planning by considering two scenarios. These two scenarios are (a) Scenario 1, which assumes no change to the current mandate and (b) Scenario 2 where it is assumed that the Cybersecurity Act is adopted.

In detail, Scenario 1 (assuming that the new regulation is not in place) uses the resources available in the Multi-annual Financial Framework (MFF) 2014-2020 (COM(2013)519 while Scenario 2, (new regulation in place by latest mid 2019) adds new tasks and activities as proposed in the Cybersecurity Act COM (2017)477 using resources as proposed in the Draft General Budget of the European Union for the financial year 2019[5]. .

In this programming document, the planned activities for 2019 in both scenarios are presented. 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 the ENISA strategy. Activities are labelled, indicating to which Scenario these activities belong. Activities labelled as Scenario 2 are only proposed to be delivered if the draft Cybersecurity Act is adopted. Section "List of Outputs in work programme 2019", just before the Annexes, summarizes the Outputs for the two scenarios: the first list covers the Scenario 1 Outputs, to be delivered independent of the adoption of the Cybersecurity Act, while the second list includes the new Outputs to be delivered as soon as the Cybersecurity Act is published in the official Journal.

I look forward to the next phase in ENISA's development,

Udo Helmbrecht

Executive Director

[5] Draft General Budget of the European Union for the financial year 2019, available at: https://eur-lex.europa.eu/budget/data/DB/2019/en/SEC03.pdf , and COM(2018)600 of May 2018 with breakout for Agencies available at:
http://ec.europa.eu/budget/library/biblio/documents/2019/WD%20III%20Agency_web.pdf
The budget contribution is subject to final adoption of the EU budget.

Mission Statement

Acting as a centre of expertise dedicated to enhancing network and information security in the Union and supporting capacity building of Members States, ENISA was set up in 2004 to contribute to the overall goal of ensuring a high level of network and information security within the EU.

The mission of ENISA has been 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 organizations in the Union".

ENISA supports the European institutions, the Member States and the business community in addressing, responding to and especially in preventing network and information security problems. It does so through a series of activities across five areas identified in its strategy:

- Expertise: provision of information and expertise on key network and information security issues.
- Policy: support to policy making and implementation in the Union.
- Capacity: support for capacity building across the Union (e.g. through trainings, recommendations, awareness raising activities).
- Community: foster the network and information security community (e.g. support to the Computer Emergency Response Teams (CERTs), coordination of pan-European cyber exercises).
- Enabling (e.g. engagement with the stakeholders and international relations).

In doing so, ENISA will act "*without prejudice to the competences of the Member States*" regarding their national security[6] and in compliance with the right of initiative of the European Commission. In order to achieve its mission, several objectives and tasks[7] 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*" [8].

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 NIS capability development[9], resulting in a more agile and flexible approach to achieving its mission.

6 Article 1(2) of ENISA Regulation (EU) No 526/2013
7 Article 2 and 3 of ENISA Regulation (EU) No 526/2013
8 Article 1(2) of ENISA Regulation (EU) No 526/2013
9 Article 14 of ENISA Regulation (EU) No 526/2013

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 cybersecurity issues** in view of promoting a coherent EU approach to NIS;
- **Adding value through complementarity with Member States 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;
- **Competent EU institutions, agencies, and bodies** dealing with other aspects of NIS (Europol, European Defence Agency, European External Action Service, Sectoral agencies, etc.) with which the Agency will closely liaise;
- **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, from National NIS competent authorities, private sector and academia;
- **Supporting Public & Private Cooperation**, with a view to reducing the fragmentation of the Digital Single Market and support the development of digital security industry in Europe.

A stronger ENISA as of 2020

• **EU policy development and implementation**: proactively contributing to the development of policy in the area of network information security, as well as to other policy initiatives with cybersecurity elements in different sectors (e.g. energy, transport, finance); providing independent opinions and preparatory work for the development and the update of policy and law; supporting the EU policy and law in the areas of electronic communications, electronic identity and trust services, with a view to promoting an enhanced level of cybersecurity; assisting Member States in achieving a consistent approach on the implementation of the NIS Directive across borders and sectors, as well as in other relevant policies and laws; providing regular reporting on the state of implementation of the EU legal framework.

• **Capacity building**: contributing to the improvement of EU and national public authorities' capabilities and expertise, including on incident response and on the supervision of cybersecurity related regulatory measures; contributing to the establishment of Information Sharing and Analysis Centres (ISACS) in various sectors by providing best practices and guidance on available tools and procedures, as well as by appropriately addressing regulatory issues related to information sharing.

• **Knowledge and information, awareness raising**: becoming a key information hub of the EU for cybersecurity; promoting and sharing best practices and initiatives across the EU by pooling information on cybersecurity deriving from the EU and national institutions, agencies and bodies; making available advice, guidance and best practices on the security of critical infrastructures; in the aftermath of significant cross-border cybersecurity incidents, compiling reports with a view to providing guidance to businesses and citizens across the EU; regularly organising awareness raising activities in coordination with Member States authorities.

• **Market related tasks (standardisation, cybersecurity certification)**: performing a number of functions specifically supporting the internal market and cover a cybersecurity 'market observatory', by analysing relevant trends in the cybersecurity market to better match demand and supply, and by supporting the EU policy development in the ICT standardisation and ICT cybersecurity certification areas; with regard to standardisation in particular, facilitating the establishment and uptake of cybersecurity standards; executing the tasks foreseen in the context of the future framework for certification.

• **Research and innovation**: contributing its expertise by advising EU and national authorities on priority-setting in research and development, including in the context of the contractual public-private partnership on cybersecurity (cPPP); advising the new European Cybersecurity Research and Competence Centre on research under the next multi-annual financial framework; being involved, when asked to do so by the Commission, in the implementation of research and innovation EU funding programmes.

• **Operational cooperation and crisis management**: strengthening the existing preventive operational capabilities, in particular upgrading the pan-European cybersecurity exercises (Cyber Europe) by having them on a yearly basis; supporting the operational cooperation as secretariat of the CSIRTs Network (as per NIS Directive provisions) by ensuring, among others, the well-functioning of the CSIRTs Network IT infrastructure and communication channels and by ensuring a structured cooperation with CERT-EU, European Cybercrime Centre (EC3), EDA and other relevant EU bodies in line with the Commission proposal for the Cybersecurity Act[10].

• **Play a role in the EU cybersecurity blueprint** presented as part of this package and setting the Commission's recommendation to Member States for a coordinated response to large-scale cross-border cybersecurity incidents and crises at the EU level in line with the Commission proposal for the Cybersecurity Act; facilitating the cooperation e.g. at blueprint technical (CSIRTs) and operational level (Single Point of Contact), between individual Member States in dealing with emergency response by analysing and aggregating national situational reports based on information made available to the Agency on a voluntary basis by Member States and other entities.

• **Cybersecurity certification of ICT products and services**: European Cybersecurity Certification Framework for ICT products and services specifies the essential functions and tasks of ENISA in the field of cybersecurity certification. The draft foresees that ENISA prepares the European cybersecurity certification schemes, with the assistance, expert advice and close cooperation of the European Cybersecurity Certification Group. Upon the EU Commission’s request to prepare a scheme for specific ICT products and services, ENISA will work on the scheme in close cooperation with national certification supervisory authorities represented in the Group. The same may apply upon the request of the Member States or the Group.

[10] COM(2017)477

Section I. General context

Threat Landscape

2017 was the year in which incidents in the cyberthreat landscape have led to the definitive recognition of some omnipresent facts. We have gained unwavering evidence regarding monetization methods, attacks to democracies, cyber-war, transformation of malicious infrastructures and the dynamics within threat agent groups.

But 2017 has also brought successful operations against cyber-criminals. Law enforcement, governments and vendors have managed to shut down illegal dark markets, de-anonymize the Darknet and arrest cyber-criminals. Moreover, state-sponsored campaigns have been revealed and details of technologies deployed by nation states have been leaked. Mostly remarkable though is the manifestation of the cyberthreat landscape within framework programmes that are about to be established in the area of critical infrastructure protection: cyberthreats make up the basis for the development and implementation of red and blue teaming activities in financial sector across Europe.

But the cybersecurity community is still far from striking the balance between defenders and attackers. Although 2017 has reached records in security investments, it has also brought new records in cyber-attacks of all kinds, data breaches, and information loss. From this perspective, one may argue that there is a market failure in cyber-security; that is, the increased defence levels and expenses cannot successfully reduce levels of cyberthreat exposure.

Whether this is due to a segmented cyber-security market, lack of awareness or capabilities and skills, are topics of vivid discussions in the corresponding communities. Fact is however, that in 2017 we have seen extremely increased amount of information on cyber-security incidents, cyberthreats and related matters to deluge all kinds of media. This trend is indicative for the high level of interest assigned by media to cybersecurity issues.

In summary, the main trends in the 2017's cyberthreat landscape are:

- Complexity of attacks and sophistication of malicious actions in cyberspace continued increasing.
- Threat agent of all types have advanced in obfuscation (that is, hiding their trails).
- Malicious infrastructures continue their transformation towards multipurpose configurable functions including anonymization, encryption, detection and evasion.
- Monetization of cybercrime is becoming the main motive of threat agents, in particular cyber-criminals. They take advantage of anonymity offered by the use digital currencies.
- State-sponsored actors are one of the most omnipresent malicious agents in cyberspace. They are top concern of commercial and governmental defenders.
- Cyber-war is entering dynamically into the cyberspace creating increased concerns to critical infrastructure operators, especially in areas that suffer some sort of crises.
- Skills and capabilities are the main concerns for organisations. The extensive need for related training programmes and educational curricula remains almost unsatisfied.

All these trends are assessed and analysed by means of the content of the ENISA Threat Landscape 2017 (ETL 2017). Identified open issues leverage on these trends and propose policy, business and research/educational. They serve as recommendations and are taken into account in the future activities of ENISA and its stakeholders.

In 2017 the frequency and impact of serious incidents has grown. The proliferation of ransomware, for example, has reached a ca. 2.000% increase in 2017 and has drawn everyone's attention to the reality of cyber threats and their possible critical impacts and costs.

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.

Concluding, on top of a quite active cyber-crime scene, ETL has indicated that high profile (state-sponsored) attackers have advanced in analogy to the developments of the entire threat landscape: complexity, sophistication and advancements in capabilities have been observed for most of the threat agent groups. While the race between good and bad guys continues, advancements in obfuscation and masquerading of threat agents make it more difficult to understand who-is-who. This difficulty has led to an alerting phenomenon: the user community cannot differentiate between the bad and the good, thus loosing trust to commercial and even institutional players in cyber-space.

In the realm of all these developments, ENISA has identified numerous activities to cope with the trends of the cyberthreat landscape and increase knowledge and capability levels for various stakeholder groups.

Policy Initiatives

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

Whereas NIS has been set high in the EU political agenda notably in the European Cybersecurity Strategy (2013), the European Cyberdefence Policy Framework (2014) and in the European Digital Single Market (2015), ENISA will in the future, more than ever, need to accompany the efforts of Member States and Union institutions in reinforcing NIS across Europe. Above all, the recent adoption of the European directive of the European Parliament and the Council concerning measures to ensure a high common level of network and information security, further calls for enhanced commitment of ENISA in supporting a coherent approach towards NIS across Europe.

While ENISA should continue its well-established activities – from the support to the reinforcement of Member States' national capacities to the organization 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: contributing to the NIS technical and operational cooperation by actively supporting Member States' CSIRTs' cooperation within the European CSIRTs Network and the NIS Cooperation Group; also providing input and expertise into policy level collaboration between national competent authorities in the framework of the Cooperation Group, supporting the reinforcement of the NIS of Union institutions in strong 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 several European Union institutions are mandated to act in the area of cybersecurity (CERT-EU, 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 cybersecurity in Europe.

In this respect, the publication of the new EU cybersecurity package with its set of legislative and non-legislative measures, on 13th of September 2017, has identified ENISA as a key pillar of the EU's ambition towards the reinforcement of cybersecurity across Europe. The Strategy in particular foresees the strengthening and reinforcing ENISA:

- Section 2.1 addresses ENISA and the strengthening of the Agency. The permanent mandate is proposed.
- ENISA's role in the NIS Directive is acknowledged.
- An EU cyber security certification framework is proposed. It is proposed that ENISA would 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[11] and the new proposed Cybersecurity Act[12].

[11] 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

[12] 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

Section II. Multi-annual programming 2019 – 2021

Multi-annual programme

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

Priorities are completed with indications on

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

Annual outputs will derive from these priorities.

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

Multiannual priorities (2019-2021) for Objective 1.1. Improving the expertise related to NIS

Priorities

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

Guidelines

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

Added-value

- provide European-wide visibility to existing NIS expertise, in particular developed at national level;
- foster convergent understanding of NIS challenges across the EU NIS community as well as best practices to address them, by offering tailored, high quality and up-to-date analysis and recommendations;
- raise awareness of operators, European institutions and national public authorities on rising security challenges that should be taken into account at technical and policy levels;

- support its work under Activity 2 (Policy), 3 (Capacity) and 4 (Community) by advising on challenges that may influence EU NIS policy developments and implementation, national and European capacity building as well as crisis and CSIRT cooperation.

Multiannual priorities (2019-2021) for Objective 1.2. NIS threat landscape and analysis

Priorities

- carry out an annual EU threat landscape offering a general technical assessment of existing and anticipated threats and their root causes;
- produce annual analyses of national incident reports within the framework of the implementation of the Telecom package, eIDAS Regulation and the NIS Directive;
- in addition to the general threat assessment, focus as well on a specific dimension (e.g. sector or cross-sector threats in the context of the NIS Directive, or threats to existing technologies whose usage is increasing e.g. IPV6 and threats today underestimated which may increase in the future);
- establish dissemination channels for the information created (threat intelligence) and make it available to stakeholders. The delivered threat intelligence consists of both main and side products of the threat assessments (e.g. cyberthreats, threat agents, assets, mitigation controls, collected sources, other related items), put in context as appropriate.
- provide on a regular basis a concise overview on cyberthreats as they have materialised within incidents. Such information should provide an overview of the findings of available open source evidence in a neutral manner.

Guidelines

- seek synergies among national incident reports in its analyses mentioned above;
- ensure that the EU threat landscape benefits from relevant sources of information, in particular vendor reports, national threat assessments, researchers, media as well as information stemming from the CSIRTs network;
- seek to enhance visibility of these results to the EU NIS community by delivering generated material for various stakeholders in a coherent manner;

Added-value

- offer an EU-wide independent synthesis on technical threats of general interest for the EU, in particular in the context of the implementation of the NIS directive (operators of essential services, digital service providers);
- improve general awareness on threats of national and European public and private entities and bodies and foster mutual understanding by National Competent Authorities on current and future threats;
- establish a dialogue among relevant threat intelligence stakeholders in form of an interaction model, including a community and an interaction platform;
- support stakeholders in building capability in the area of threat intelligence/threat analysis; provide support in their activities and deliver threat analysis tailored to their needs.
- support other Activities by advising on threats that may influence EU NIS policy developments and implementation (Activity 2), by encouraging Member States' to develop national threat assessments and advising the Union institutions, bodies and agencies (hereinafter: "Union institutions") on threats to their security (Activity 3) as well as creating synergies with crisis and CSIRT cooperation such as by supporting cooperation on the development of threats taxonomies (e.g. incident taxonomies) (Activity 4);

Multiannual priorities (2019-2021) for Objective 1.3. Research & Development, Innovation

Priorities

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

Guidelines

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

Added-value

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

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

Multiannual priorities (2019-2021) 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, security certification, crisis cooperation, education and training, information hub) in view of ensuring coherence with the framework and principles agreed upon in the NIS directive;
- seek to identify when possible NIS challenges that may require policy developments at EU level;
- build upon this stocktaking and taking into accounts NIS challenges previously identified, offering NIS expert advice the European Commission and other relevant Union institutions on these policy developments;.

Guidelines

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

Added-value

- foster awareness of the EU NIS community on EU policy developments with a NIS dimension;
- foster the inclusion of 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 (2019-2021) 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 (legislations) with a NIS dimension, by allowing them to share national views and experiences and build upon those to draw consensual recommendations;
- focus on the NIS Directive in particular regarding requirements related to Operators of Essential Services (e.g. identification, security requirements, incident reporting) and on eIDAS Regulation as well as on NIS aspects of, GDPR (and more generally data protection) and the draft ePrivacy Regulation;

Guidelines

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

Added-value

- support Member States 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 the harmonized approach on implementation of EU policies and in particular legislations, even when mandatory harmonization of national approaches is not enforced, such as in the NIS Directive regarding OES;

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

Multiannual priorities (2019-2021) 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 rising of EU Member States' CSIRTs;
- develop a NIS national capacities metrics, building upon capacities foreseen in the NIS directive, allowing an assessment of the state of NIS capacity development with the EU;

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

Guidelines

- carry out a regular stocktaking of national NIS capacity initiatives with a view to identify trending developments in view of collecting and analysing different approaches and practices;
- liaise closely with national NIS competent authorities' experts to identify 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 of NIS capacities ranging from technical to organizational and policy ones;
- while creating a general NIS capacity metrics, seek in priority to identify main trends at the EU level and 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 to increase their impact (e.g. summer school, onsite trainings)

Added-value

- continue to support the development of national NIS capacities reinforcing the level of preparedness and response capacities of Member States thus contributing to the overall cybersecurity of NIS across the EU;
- foster sharing of best practices among Member States;
- indirectly 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 CEF) benefiting to the cooperation within the CSIRTs network and the development

Multiannual priorities (2019-2021) for Objective 3.2 Assist in the EU institutions' capacity building

Priorities

- representation by ENISA on the Steering Board of CERT-EU of the EU Agencies
- Cooperation with relevant EU agencies on initiatives covering NIS dimension related to their mission;
- in cooperation with CERT-EU, inform the European Commission and other relevant Union institutions, bodies and agencies on threats to NIS via the production of regular and punctual information notes;
- provide (upon request and in coordination with the institutions) capacity building support for trainings, awareness, and development of education material.

Guidelines

- Liaison with EU agencies on defining NIS requirements;
- capacity building through regular interactions (e.g. annual workshop)in cooperation with the ICT Advisory Committee of the EU Agencies ;
- partner with CERT-EU and institutions with strong NIS capabilities in view of supporting its actions under this objective;
- reinforce links between Union bodies and general awareness raising campaigns (e.g. through active engagement of European Union institutions and agencies in the ECSM).

Added-value

- support the development of NIS capacities of European Union institutions and agencies thus contributing to raising the level of the overall cybersecurity of NIS across the EU;
- foster sharing of best practices among Union agencies and better definition of NIS requirements to reduce duplication of efforts and to encourage more systemic approaches to NIS;
- complement CERT-EU's work on active cybersecurity for the EUIs and agencies through awareness raising and other proactive measures, by offering advice on the "prevention" dimension of NIS;

Multiannual priorities (2019-2021) for Objective 3.3 Support private sector capacity building

Priorities

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

Guidelines

- build upon existing work done at 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 size enterprises, NIS experts or non-experts) and adopt a holistic approach of NIS capacities ranging from technical/operational to organizational and policy capacities;
- with a view to supporting information sharing on NIS developments at European level, contribute to the functioning of ECSO as foreseen in Objective 1.3 and 2.1 and when wishing to interact with specific sectors, liaise with Member States primarily responsible for interacting with private stakeholders nationally;
- offer advice on how to improve private-private exchanges of information (e.g. via ISACs) and on an ad hoc basis and, without prejudice to 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 their NIS;
- support the development of the NIS of businesses across the EU and support national NIS competent authorities in their similar efforts towards private sector, thus contributing to raising the level of the overall cybersecurity of NIS across the EU;

Multiannual priorities (2019-2021) for Objective 3.4 Assist in improving general awareness

Priorities

- organize the European Cybersecurity Month (ECSM) and the European Cybersecurity Challenge (ECSC) with a view to making these events sustainable EU "rendez-vous" ;
- carry out regular stocktaking of national awareness raising initiatives;
- build upon this stocktaking and in liaison with the ECSM and ECSC, analyse and provide 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 volunteer national NIS competent authorities' experts on awareness raising and communication, responsible for the national dimension of the ECSM and ECSC;
- adopt a holistic approach to awareness raising and adapt its recommendations to specific target audiences, from the citizens to public authorities;
- explore ways of using adapted communication channels within the framework of the ECSM and ECSC;

Added-value

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

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

Multiannual priorities (2019-2021) for Objective 4.1 Cyber crisis cooperation

Priorities

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

Guidelines

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

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

Added-value

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

Multiannual priorities (2019-2021) 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, 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 advice, upon request, Member States' CSIRTs on projects to be proposed within the framework of future CEF call for projects;

Guidelines

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

Added-value

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

Activity 5 – Enabling. Reinforce ENISA's impact

Multiannual priorities (2019-2021) for Objective 5.1 Management and compliance

Priorities

- increase and improve the recruitment of new talents with the aim of achieving priorities laid out in the WP;

- Optimize internal procedures, by using modern IT applications in several Agency specialized areas
- develop internal management in view of supporting the development of ENISA's internal expertise as well as ensuring staff's well-being, personal development and professional commitment;
- ensure the responsible financial management of its resources within the financial and legal framework;
- guarantee a high level of transparency regarding its internal processes and working methods;

Guidelines

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

Added-value

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

Multiannual priorities (2019-2021) for Objective 5.2 Engagement with stakeholders and international relations

Priorities

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

Guidelines

- when provided by the WP, establish structured and, whenever relevant on a multiannual basis, dialogues with volunteer national Member States' experts in view of delivering its outputs (e.g. working groups such as on cyber crisis cooperation);
- rely upon national Member States when primarily responsible for national public private cooperation, in view of engaging with private sector;
- further develop tools and procedures to facilitate and make transparent involvement of all stakeholders in particular regarding the principles and modalities of the participation and consultation of national NIS competent authorities;

- build in priority upon the Network of Liaison Officers as main exchange point for ENISA and Member States' in view achieving these priorities;
- carry out regular in-depth evaluations in view of assessing mid-long term impact of its action in certain areas of expertise;

Added-value

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

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

The Agency developed key indicators to provide the metrics to measure against performance, results and impact of the Agency's outcome, output and impact. Detailed presentation of Key Performance Indicators (KPIs), Key Results Indicators (KRIs) and Key Impact Indicators (KII) is provided in Annex B.

Human and financial resource outlook for the years 2019-2021

Annex A1 provided the outlook of resources and contains a brief description on new tasks and efficiency gains.

Section III. Work Programme Year 2019

The ENISA Work Programme for the year 2019 follows the lay out presented in the multi-annual programming Section II. In this section objectives, results and indicators are identified in relation to each activity.

The Activities presented in this section follow the structure of the ENISA strategy. After a short description of the activity the objectives are presented. A short narrative is included, consisting of a description and added value of the activity, the main challenges for 2019 and link to the multi-annual objectives.

The main outputs/ actions in the specific year, for this case for 2019, are listed within each objective. For each objective there are several outputs defined.

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

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

For each activity there is an objective defined that covers the actions that the Agency is carrying out in order to respond to official 'Article 14 requests', named after the Article 14 of the ENISA regulation[13], which allows the MS and EU institutions to make direct requests to ENISA seeking assistance or advice on specific activities.

In the preparation of Work Programme 2019, ENISA is considering two scenarios. In detail, Scenario 1 uses the resources available in MFF 2014-2020 (COM(2013)519. Scenario 2 (which assumes that the new regulation will be in place by latest mid 2019), adds new tasks and activities using resources as proposed in the draft Cybersecurity Act COM (2017)477 and in alignment with the draft general budget of the European Union for the financial year 2019. Each Output is labelled accordingly as Scenario 1 or Scenario 2 Output. Activities labelled as Scenario 2 are only proposed to be delivered if the draft Cybersecurity Act is adopted.

[13] According to Regulation (EU) No 526/2013. When the Cybersecurity Act will be adopted, in case of Scenario 2, these objectives will be re-allocated, re-labelled based on the new legal framework and corresponding articles.

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

Objective 1.1. Improving the expertise related to Network and Information security

Output O.1.1.1 – Good practices for security of Internet of Things (Scenario 1)

IoT is at the core of operations for many Essential Service Operators as defined in the **NIS Directive**, especially considering recent initiatives towards Smart Infrastructures, Industry 4.0[14], 5G[15], Smart Grids[16], etc. With a great impact on citizens' safety, security and privacy, the IoT threat landscape is extremely complex. Therefore, it is important to understand what exactly needs to be secured and to implement specific security measures to protect the IoT from cyber threats.

Building on its previous work on IoT security, the Agency will identify and analyse existing IoT security practices and standards in the area of e.g. Industry 4.0 and Critical Information Infrastructures, consumer electronics, etc. taking into consideration existing national expertise and practices. The Agency will map the evolving threat landscape and compare these practices and standards and develop good practices for the security of the Internet of Things focusing on its impact on the overall supply chain and considering relevant interdependencies.

To satisfy these goals, 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[17], the Communication on Building strong cybersecurity for the EU[18], the Public Private Partnership (PPP) on cybersecurity[19], the 5G Infrastructure Public Private Partnership (5G PPP)[20], etc.).

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 consider defining e.g. IoT security requirements, maturity levels, procurement guidelines or other means to promote awareness and to ensure "security for safety". The Agency will also consider implementing online tools to visualize IoT security measures in order to further support stakeholders.

The Agency will also validate the results of the study (e.g. via joint workshops as the two organised with EUROPOL/EC3) with relevant national and EU initiatives (e.g. AIOTI, IIC) and interact with important digitised industries in EU and IoT stakeholders from the public sector (e.g. DG CNECT, JRC, EUROPOL/EC3), as well as from the private sector including operators, integrators and manufacturers.

This work item builds on previous work of ENISA in the area of IoT (WP2017-2018) and Smart Infrastructures (WP2015 – 2017).

---

[14] See https://ec.europa.eu/digital-single-market/en/fourth-industrial-revolution
[15] See https://ec.europa.eu/digital-single-market/en/towards-5g
[16] See https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters
[17] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2009:0278:FIN
[18] See http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN
[19] See https://ec.europa.eu/digital-single-market/en/news/commission-decision-establish-contractual-public-private-partnership-cybersecurity-cppp
[20] See https://5g-ppp.eu/

Output O.1.1.2 – Good practices for the security of Smart Cars (Scenario 1)

The automotive industry is undergoing a paradigm change towards connected and autonomous vehicles. Smart cars already available today provide connected, added-value features in order to enhance car users' experience or improve car safety. With this increased connectivity (that the emergence of 5G is expected to further promote) novel cybersecurity risks and threats arise and need to be managed. In light of the NIS Directive where of road authorities and intelligent transport systems are among the entities identified as Essential Service Operators in the road transport sub-sector, there is a growing call for smart cars security to be addressed.

The Agency will build on its previous work on smart cars[21] and will identify and analyse existing security practices and standards in the area of smart cars (e.g. UN-ECE dedicated TF on CYBER, ISO/SAE standardisation work) analysing the emerging notions of connectivity and autonomy. ENISA will review these practices and standards and highlight or suggest good practices and potential legislative action required for security of smart cars focused on safety and the issues of connectivity and autonomy, while mapping the emerging threat landscape.

Building on the previous initiative 'Europe on the Move' of May 2017, on 17 May 2018 the European Commission put forward a strategy to make Europe a world leader for automated and connected mobility. To assist the Commission and the member states in achieving these objectives the Agency will consider and contribute to existing EU policy and regulatory initiatives (the NIS Directive, the European strategy on Cooperative Intelligent Transport Systems[22], the C-ITS Platform of DG MOVE[23], the High Level Group GEAR 2030[24]), as well as the 3rd Mobility package[25] and the Communication on Connected and Automated Mobility (CAM). This agenda provides a common vision for developing and deploying key technologies, services and infrastructure. Among these actions, it is envisaged that the Commission will work towards the adoption of a Recommendation by the end of 2018 to be addressed to the Member States and industry actors. The Recommendation would pertain to the use of pioneer spectrum for 5G large-scale testing, cybersecurity issues and into a data governance framework that enables data sharing, in line with the initiatives of the 2018 Data Package. Moreover, the Agency will take into account industry initiatives such as the European Automotive Telecom Alliance (EATA) and the 5G Automotive Alliance.

The Agency will develop targeted smart cars case studies to identify risks and vulnerabilities, by defining appropriate attack scenarios, and providing relevant recommendations and good practices to ensure "security for safety" in regard to connected and autonomous vehicles. This work should support EC in the Recommendation deliverable listed in the Communication on CAM.

The Agency will examine the concept of information sharing initiatives among relevant stakeholders in the automotive sector. This stems from the relevant recommendations of the WP2016 ENISA study, as well as related industry guidelines, e.g. ACEA.

The Agency will also validate the results of the study (e.g. via joint workshops) with relevant national and EU initiatives (such as EATA and ERTICO) and interact with all important smart cars stakeholders from

[21] See https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars
[22] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0766
[23] See https://ec.europa.eu/transport/themes/its/c-its_en
[24] See https://ec.europa.eu/growth/content/high-level-group-gear-2030-report-on-automotive-competitiveness-and-sustainability_en
[25] See https://ec.europa.eu/transport/modes/road/news/2018-05-17-europe-on-the-move-3_en

public sector such as the relevant European Commission service, JRC, national road authorities, and from the private sector including automotive manufacturers, OEMs, etc.

This work item builds on previous work of ENISA in the area of Smart Cars, IoT, Smart Cities and Intelligent Public Transport (WP 2015 - 2017).

Output O.1.1.3 - Awareness raising on existing technical specifications for cryptographic algorithms (Scenario 1)

In the revised Cybersecurity strategy of the EU published in September[26], the European Commission highlights "[…] the lack of European capacity on assessing the encryption of products and services used by citizens, businesses and governments within the Digital Single Market. Strong encryption is the basis for secure digital identification systems that play a key role in effective cybersecurity […]". Furthermore, in Art 10 of its proposal for a regulation of the European parliament and of the Council on ENISA, the "EU Cybersecurity Agency", repealing Regulation (EU) 526/2013, of 13 Sept 2017 the European Commission is calling ENISA to *"…advise the Union and the Member States on research needs and priorities in the area of cybersecurity, with a view to enabling effective responses to current and emerging risks and threats, including with respect to new and emerging information and communications technologies, and to using risk-prevention technologies effective"*". One of the most important technologies that is satisfying the criteria of a security enhancing technology as well as privacy enhancing technology is encryption.

While acknowledging the importance of crypto technologies with regard to cyber security, particularly encryption is still a key area of national security, especially when it comes to the protection of sensitive governmental systems as well as critical information infrastructures. To harmonise both - market needs and MS responsibilities - it is essential to work together on sharing existing approaches, best practices and knowledge. In international standardisation, technical specifications for cryptographic algorithms already exist which should be considered at European level, too. Moreover, at the European level the so called SOGIS-MRA Crypto catalogue[27] is already a major achievement as a first comprehensive collection of cryptographic means agreed on by participating Member States' competent authorities.

Working closely with the Member States, ENISA will act as a catalyst to raise awareness on already existing cryptographic means based on a wider promotion of the SOGIS catalogue. Especially in light of the new EU certification framework where ENISA plays a significant role, ENISA will start in 2019 to discuss with the existing SOGIS crypto working group the possibilities of a long-term relationship and exchange. As a starting point, ENISA will participate in respective meetings of the group.

With regard to standardisation ENISA should facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT processes, products and services – and this includes cryptography.

ENISA could engage with ETSI groups concerned with cryptography – primarily TC Cyber and its QSC subgroup as well as TC ESI. ENISA could also promulgate the outputs of these groups by linking to them from its website. A similar arrangement could be in place for relevant CEN/CENELEC standards groups (primarily JTC-13 as it begins its work).

---

[26] 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

[27] https://www.sogis.org/uk/supporting_doc_en.html

Output O.1.1.4 - Good practices for the security of Healthcare services (Scenario 2)

Recent cybersecurity incidents have shown that the healthcare sector is one of the most vulnerable. Based on ENISA studies, the situation currently in the healthcare sector regarding cyber security has shown that the level of cybersecurity is low. For example, most hospitals don't have a Chief Information Security Officer, there is a lack of security policies, of access control mechanisms; hospitals are easy targets due to their interoperable systems and due to the high vulnerability of the legacy medical devices.

Newly adopted EU legislations have indicated that there has been a shift in priorities: the NIS Directive defines healthcare organisations as operators of essential services, Medical Devices Regulation[28] (MDR) includes obligatory safety and security provisions for medical devices as well as the EC Communication on enabling digital transformation of health and care in the Digital Single Market[29].

The Agency, based on previous experience, will support Healthcare organisations in enhancing their cyber security level by helping them to make the right decisions when procuring equipment and services supporting their internal systems. The Agency will identify existing vulnerabilities and risks on the Healthcare organisations' systems deriving also from medical devices. The Agency will map the evolving threat landscape and collect common practices for ensuring cyber security in these interoperable systems. The ultimate goal is to provide healthcare organisations with a list of security requirements and measures in order to take the informed decisions when procuring equipment and services. This is not linked to the certification topic.

To achieve these goals, the Agency will take into account existing national and EU policies and regulations, such as the requirements deriving from the NIS Directive and will not contradict and interfere with those provisions and international standards (like HIPPA and ISO 27799) as well as position papers from EC working groups (MDR working group and the eHealth Network).

The Agency will also validate the results of the study (e.g. via joint workshops) with relevant national and EU initiatives and interact with Healthcare organisations and policy makers (ASIP Sante in FR, SPMS in PT etc.), NIS competent authorities, as well as with experts from the private sector including operators, integrators and manufacturers. ENISA will offer experts the possibility to contribute to the work through informal expert groups.

This work builds on previous work of ENISA in the areas of Healthcare security (WP 2015), Smart Hospitals (WP 2016) and NIS Directive implementation (WP 2017).

Output O.1.1.5 – Good practices for the maritime security (ports security) (Scenario 2)

Ports serve a critical function in domestic and international supply chain activities by connecting sea and inland transport services. In the EU, sea ports play a significant role facilitating 90% of the EU's external trade in terms of weight and an additional 43% of internal market exchanges. In addition, ports in the EU constitute energy hubs for conventional and renewable energies, serve 400 million passengers annually and generate employment[30]. Ports are a Critical Information Infrastructure for water transport and identified as operators of essential services in the NIS Directive, where managing bodies of ports, including

[28] https://ec.europa.eu/growth/sectors/medical-devices/regulatory-framework_en
[29] https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering
[30] https://ec.europa.eu/transport/modes/maritime/ports/ports_en

their port facilities, and entities operating works and equipment contained within ports are all eligible to be classified as Operators of Essential Services.

The Agency will provide port authorities and service providers and developers with good security and resilience practices when designing, developing and deploying services in order to minimise the exposure of such network and services to all relevant cyber-threat categories. The good practices will consider both the current port ICT environment and the emerging trends in terms of business models and supporting ICT systems. ENISA will take stock of existing practices and standards and develop good practices with a focus on critical port services resilience and user safety, while analysing specific use cases to determine attack scenarios.

In this endeavour the Agency will take into account and contribute to existing EU policy and regulatory initiatives, such as the NIS Directive and will not contradict and interfere with those national provisions, and interact with key stakeholders from the public sector, such as DG MOVE and EMSA and from the private sector, such as managing bodies of ports, port facilities, water transport companies, operators of vessel traffic services and ICT product and service vendors to collect information and validate the study findings.

This work builds on previous work of ENISA in the areas of maritime (2011), intelligent transportation systems (WP 2015) and smart critical infrastructures (2016).

Objective 1.2. NIS Threat Landscape and Analysis

Output O.1.2.1 – Annual ENISA Threat Landscape (Scenario 1)

This report will provide an overview of current threats and their consequences. It contains tactical and strategic information about cyber-threats. It also refers to threat agents and attack vectors used. The ENISA Threat Landscape is hence a source of generic Cyber Threat Intelligence (CTI) by means of interrelated information objects. The contents of the report are based on an intensive information collection exercise, followed by analysis and consolidation of publicly available information on cyber threats, including annual incident reports.

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

The dissemination, concise presentation and online availability of cyberthreat intelligence will be in the focus in 2019. Available cyberthreat intelligence will be interlinked with other related ENISA results (see also chapter Multiannual priorities (2019-2021) for Objective 1.2. NIS threat landscape and analysis).

In this manner, ETL stakeholders will be in the position to access and interact with ENISA cyberthreat information on a permanent basis. In 2019, ENISA will continue the cooperation with CERT-EU in the area of Threat Landscaping. This effort will be carried out by means of information exchanges, use of CERT-EU services and organisation of common meetings/events. In carrying out this work, synergies with related experts (i.e. ENISA ETL Stakeholder Group) and vendors (through MoUs) will be maintained and expanded.

In 2019, ENISA will continue supporting the relevant Cyberthreat Intelligence stakeholder community by supporting CTI good practices and by providing an interaction platform. This is the main instrument of

mobilization of CTI stakeholders; it will be engaged in the dissemination of ENISA CTI information of all kinds (e.g. Info Note).

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

ENISA provides guidance on important NIS events and developments through Info Notes. As from 2018, the Agency will produce two distinct types of info note; 'CSIRT Info Notes' and 'General Info Notes'. This will be continued in 2019.

CSIRT Info Notes

CSIRT Info Notes cover incidents and/or vulnerabilities of EU dimension that are within the scope of activities of the CSIRTs Network. Such notes will only be published following the agreement of the CSIRTs Network whilst respecting its internal procedures.

General Info Notes

General info notes cover significant developments and announcements in the field of cyber security. General info notes are not a response to incidents or vulnerabilities but are rather explanatory notes, regarding - for example - events that reach a certain level of public and media attention. For General Info notes, ENISA will consult the CSIRTs Network but also other resources as appropriate.

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

Both types of Info Notes will be logically integrated with the cyber-threat information, building thus a single interconnected knowledge base.

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

Just as with ETL, ENISA will further continuously develop the dissemination efficiency of the procured cyber-threat information Info Notes. For this purpose, available dissemination channels will be used to enhance uptake among key stakeholder. In addition to the ENISA web site, in 2019 Info Notes will be disseminated via the ENISA ETL platform.

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

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

Current and foreseen activities in this area include:

- Incident notification in the telecom sector (Art. 13a telecom package); currently ENISA facilitates the activities of the informal Art. 13a Expert Group, keeping in touch with industry and collecting and processing the incidents for the Annual Incident Report. Further support is needed as the telecom package is currently under review. The new EU Electronic Communications Code (EECC) brings significant improvements to the security part along with the incident reporting framework.

- Incident notification for the trust service providers (Art. 19 eIDAS regulation): In 2019 ENISA will continue receiving from the competent authorities the annual incident reports, will analyse them and produce a consolidated, anonymised incident analysis report. In addition, the Agency will build upon lessons learnt from past incidents and recommend good practices to the Member States. It will also continue engaging with the competent authorities towards a harmonised implementation of this article and also engage with the private sector stakeholders to better understand the needs and challenges of the sector.
- Incident notification in the context of the NIS Directive: Further guidelines and support is needed from ENISA to facilitate a smooth implementation of the new provisions, availing where appropriate, of opportunities arising under the Connecting Europe Facility (CEF). More specifically ENISA can assist stakeholders in developing sector specific incident reporting frameworks and procedures, develop cross-border incident reporting frameworks, agree on the parameters and thresholds upon which an incident is considered significant as well as the ex-post analysis of the reported data, make inventories of suitable tools available etc. ENISA shall contribute to ensure the efficient flow of voluntary information at Member State's request and to establish common situational awareness in case of a large-scale cross-border incident.

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

Output O.1.2.4 – Regular technical reports on cybersecurity situation (Scenario 2)

As the frequency and magnitude of cybersecurity incidents in the EU increase, the EC recognised the need to improve shared situation awareness amongst EU and MS policy makers. In particular, the EC requested the following in the blueprint:

"As part of the regular cooperation at technical level to support Union situational awareness, ENISA should on a regular basis prepare the EU Cybersecurity Technical Situation Report on incidents and threats, based on publicly available information, its own analysis and reports shared with it by Member States' CSIRTs (on a voluntary basis) or NIS Directive Single Points of Contact, European Cybercrime Centre (EC3) at Europol and CERT - EU and where appropriate the European Union Intelligence Centre (INTCEN) at the European External Action Service (EEAS). The report should be made available to the relevant instances of the Council, the Commission, the HRVP and the CSIRTs Network".

The production of such situation reports will leverage many other existing and future ENISA WP activities.

For this particular output, ENISA will produce a summary report of all EU Cybersecurity Technical Situation Reports produced throughout the year. Pending implementation of the blueprint, the Agency will also organise a workshop with EU, MS and sectorial stakeholders to present the results and gather feedback on ways to improve the collection, analysis, presentation and distribution mechanisms of the EU Cybersecurity Technical Situation Reports.

In addition to the above, ENISA will create cyberthreat information reports on a quarterly basis. Such reports will be in par with the ENISA Info Note and are the intermediate reports towards the ENISA Threat Landscape, the end year cyberthreat intelligence report. Taken together and under the assumption that this information will be prepared in a structurally consistent manner, it will comprise a unique open source Cyberthreat Intelligence. It is expected that such an offering will significantly enhance the capabilities of

organisations with low cybersecurity maturity. And will contribute to a better understanding of the threat level and will be in the position to better protect themselves.

ENISA will also support the dissemination of CTI good practices. This will enable stakeholders to better adopt CTI in their business, vendors to create usable CTI offerings and tools and governmental organisations to better engage in the CTI brokerage. All this will enable CTI usage and will thus contribute to a more proper, more agile adaptation to the real cyberthreats.

Objective 1.3. Research & Development, Innovation

Output O.1.3.1 – Supporting cPPP in defining priorities for EU research & development (Scenario 1)

ENISA will continue providing analysis of the areas covered by the NIS Directive, the Cybersecurity Package, , the COM decision on cPPP and the outcomes of relevant Horizon2020 projects e.g. the CSA projects (cyberwatching, AEGIS and EU-Unity) and will aim to show where R&D activities funded in the context of H2020, CEF (Connecting Europe Facility), TRANSITS and GEANT would achieve the greatest impact. On cybersecurity aspects related to the General Data Protection Regulation, ENISA will work in conjunction with the respective Commission services. ENISA will monitor and analyse cybersecurity related directives and initiatives in various sectors (e.g. space, maritime, defence, transport, automotive) and assess the specific-threat landscape in these critical sectors.

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

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

Additionally, ENISA will continue supporting and advising the Commission and organisations in this area (e.g. ECSO), other agencies (e.g. EDA, ESA), industrial communities as well as in the Member States to meet their goals by bringing in its concrete NIS policy expertise. Relevant such contributions will also be made regarding the proposal on the creation of the Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre[31].

Objective 1.4. Response to Article 14 Requests under Expertise Activity[32]

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

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

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

[31] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN
[32] In case of Scenario 2, this objective will be re-allocated based on the new framework.

Although, by definition, it is not possible to accurately estimate the exact number or the output and outcome of these requests for 2018, the allocated resources are indicated in the Summary Section at the end.

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 Network and information Security		
Output O.1.1.1 –Good practices for security of Internet of Things (Scenario 1)	P: Good practices for security of Internet of Things, Q4 E: Validation cyber security workshop, Q3-Q4 E: Joint ENISA – Europol Conference on IoT Cyber Security, Q3-Q4 S: Support the EC, MS and IoT stakeholders in major EU initiatives, Q1-Q4	Engage 5 Industries using IoT and 5 IoT stakeholders from 5 EU MS in the preparation of the study (P) and/or validation workshop (E)
Output O.1.1.2 –Good practices for the security of Smart Cars (Scenario 1)	P: Good practices for the security of Smart Cars, Q4 E: Smart cars security workshop, Q3-Q4 S: Support the Commission, MS and automotive industry to holistically address cyber security of smart cars, Q1-Q4	Engage 5 automotive manufacturers and 5 automotive stakeholders from 5 EU MS in the preparation of the study, i.e. publication (P) and workshop (E)
Output O.1.1.3 – Awareness raising on existing technical specifications for cryptographic algorithms (Scenario 1)	S: Support work in the area of cryptography and participation in SOG-IS and ETSI related groups/meetings, Q1-Q4.	2 news items or dissemination materials published covering public documents and activities of the groups/meetings attended.
Output O.1.1.4 - Good practices for the security of Healthcare services (Scenario 2)	P: Procurement guidelines for cyber security in hospitals, Q3-Q4 S: Support the EC and the relevant MS healthcare organisations in EU policy initiatives (e.g. JASEHN WP 2018-2020), Q1-Q4 S: Support the EU healthcare organisations on identifying risks in their systems, Q1-Q4 E: Annual eHealth workshop including validation session of the relevant studies, Q3-Q4	Engage healthcare stakeholders from at least 12 EU MS in this activity, i.e. publication (P) and/or workshop (E) and/or support (S)
Output O.1.1.5 – Good practices for the maritime security (ports security) (Scenario 2)	P: Good practices for cyber security in the maritime sector, Q4 E: Maritime cyber security workshop, Q3-Q4 S: Support the Commission, MS and maritime industry to holistically address cyber security of the maritime sector, Q1-Q4	Engage 10 maritime sector stakeholders from 5 EU MS in the preparation of the study (P) and/or the workshop (E)
Objective 1.2. NIS Threats Landscape and Analysis		
Output O.1.2.1 – Annual ENISA Threat Landscape (Scenario 1)	P: Report and online information offering; report, Q4, information offering during the year.	Engage more than 10 MS in discussions and work related to the structure and content of ENISA Threat Landscape. More than 5.000 downloads of the ENISA Threat Landscape report.

	E: ENISA will organise the annual event on Cyberthreat Intelligence EU (CTI EU), Q3-Q4	Engagement of more than 80 CTI experts from industry, academia and Member States.
Output O.1.2.2 – Restricted and public Info notes on NIS (Scenario 1)	P: Info notes on NIS, Q1-Q4	Coverage of all major incidents relevant to EU NIS policy priorities. Expand coverage to all key ENISA stakeholder groups.
Output O.1.2.3 – Support Incident reporting activities in EU (Scenario 1)	P: Annual Incident Analysis Report for the Telecom Sector, Q4 E: Three workshops for the Art. 13a[33] working group P: Annual Incident Analysis Report for the Trust Service Providers, Q4 E: Two workshops for the Art. 19[34] meetings S: Support MS and the EC in implementing NISD incident reporting requirements. P: Good practices for further development of the NISD incident notification frameworks across EU, Q4, 2019 P: Short Position Paper - Analysis of a technical topic requested by the Art. 13a EG, Q4	More than 20 NRAs/EU MS contribute in preparation of the report (Art. 13a) (P) More than 10 SBs/EU MS contribute in preparation of the report (Art. 19) (P) Engage more than 10 MS in discussions and work related to implementing particularities of the NISD incident reporting framework (S).
Output O.1.2.4 – Regular technical reports on cybersecurity situation (Scenario 2)	P: Quarterly cyber threat information reports, Q4 E: Workshop with EU, MS and sectorial stakeholders to present the results and gather feedback on ways to improve the collection, analysis, presentation and distribution mechanisms of the EU Cybersecurity Technical Situation Reports, Q4.	Engage CTI stakeholders and CSIRTs community
Objective 1.3. Research & Development, Innovation		
Output O.1.3.1 – Supporting cPPP in defining priorities for EU Research & Development (Scenario 1)	S: Support for ECSO	No paper to be produced.
Objective 1.4. Response to Article 14 Requests under Expertise Activity		
Output O.1.4.1 – Response to Requests under Expertise Activity (Scenario 1)	S: Answers to requests.	

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

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 preparatory policy discussions in the area of certification of products and services (Scenario 1)

Taking due account of recent legislative and policy developments, including the draft "Cybersecurity Act" ENISA will continue working towards meeting preparatory requirements for certification framework for ICT security products and services by e.g. promoting mutual recognition or harmonisation of certification practices up to a certain level, in line with the proposed Act. Any planned activity in the area of cybersecurity certification will respect existing national efforts and interests as well as subsidiarity as it applies in the area of certification, while taking into consideration the ongoing legislative process.

ENISA will provide support for the Commission and the Member States in the policy area on certification of products and services within the scope of the approved Cybersecurity Act and for the purpose of better preparing for the new EU cybersecurity certification framework for products and services. Within this framework ENISA will enter the final year of preparations in anticipation of the coming into force of the Cybersecurity Act. ENISA will subsequently seek to stimulate the interaction and involvement of Member States' governments as well as public policy and industry stakeholders in the emerging EU certification framework. Transitioning from policy preparation to policy implementation in good cooperation with the Member States' governments is demanding for the Agency as it is conditional to final approval of the Cybersecurity Act.

ENISA will provide support for the organisation of the EU cybersecurity certification framework (organisational and IT systems), supporting the European Commission in its role in the European Cybersecurity Certification Group and analysing aspects of functional equivalence of existing certification schemes across the EU (at the MS as well as the EU level) with the emerging EU certification framework for the purpose of facilitating the transition to the new EU framework. ENISA will continue to interact with key stakeholders associated with the EU cybersecurity certification framework.

Objective 2.2. Supporting EU policy implementation

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

ENISA will continue its work on supporting public and private bodies in implementing the eIDAS Regulation by addressing technological aspects and building blocks for trust services. Aspects to be covered will be agreed with the EC and MS through the eIDAS experts group. Interacting with private sector actors will enhance the ablity of the Agency to make further meaningful contributions to this area. In implementing the Cybersecurity Act, ENISA will support the eID efforts of the MS and the Commission. Specific implementation guidelines and technical recommendations for whose approval the eIDAS expert group will be consulted will address operational aspects of Trust Service Providers, Conformity Assessment Bodies and Supervisory Authorities while accumulating the experience of best-practises and state-of the art progress, seeking to emphasise implementation and interoperability aspects. These recommendations will complement the existing knowledge base that ENISA created for the trust service providers. At the same time, ENISA will take account of recommendations and standards being developed by CEN/CENELEC, ETSI and the ISO and seek to avoid both duplication of work and potentially opposing approaches. In this regard, ENISA will support the EC in assessing the relevant standards by reviewing their meeting of requirements of the eIDAS Regulation. Furthermore, ENISA will continue to support the EC in the

implementation of qualified website authentication certificates, in particular by using them for their webpages. Other relevant areas include the non-qualified level of Trust services, mobile services etc.

Output O.2.2.2 – Supporting the implementation of the Work Programme of the Cooperation Group under the NIS Directive (Scenario 1)

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

The Agency can analyse specific issues identified in the second biennial Work Programme of the Cooperation Group (2018-2020), consult with Member States' competent authorities, and develop recommendations and suggestions that would allow Commission and Member States to take informed decision on NIS matters. It could be useful to use the work carried out on OES, DSPs and other services inter-dependencies as a reference for the NIS Cooperation Group Work Stream on cross-border dependencies.

ENISA will support the work of the Commission in resourcing capabilities on cybersecurity through CEF (specifically for for the national competent authorities under objective 4 and for OES and DSP under objective 2), in accordance with the objectives of the NIS Directive.

ENISA will also take stock of the lessons learnt from the first year's implementation of the NISD and recommend good practices to the Cooperation Group and the Commission concerning the Directive transposition process.

In addition, ENISA will continue its efforts supporting the Commission and MS with the overview of the NISD implementation and its evaluation by the Member States and the Commission.

Output O.2.2.3 – Assist MS in the implementation of OES and DSPs security requirements (Scenario 1)

Drawing from the experience of the NIS Cooperation Group, ENISA will assist MS in the implementation of OES and DSPs security requirements by building on its knowledge and expertise in the area of security requirements, identification criteria, security measures and notification requirements. The Agency will work closely with Member States to identify such cost effective practices and maturity security frameworks.

In deriving such a set of common mechanisms, sector-specific needs might be taken into account as these are likely to introduce different 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). ENISA will monitor the development of the NIS Directive implementation (across all sectors in the MS) and identify possible priorities and tasks for the involved actors.

However, the Agency will take note of such specific requirements as and when they are identified during the analysis phase and will then map them to the needs and requirements of DSPs and OES.

The Agency will also compare and validate the results with other relevant approaches in the area of Operators of Essential Services (e.g. C2M2, NICE-CMM) or the generic IT models (e.g. ISO 27001) and

interact with all important stakeholders from public as well as the private sector. In this line, online tools which map the security requirements with different approaches and standards will be developed.

The proper validation of the proposed practices would contribute to setting the basis for sufficient convergence across the EU MS. The existence of multiple legislation instruments (e.g GDPR and sector specific legislation) with different security requirements on OES and DSP requires a concerted effort from competent authorities vis-à-vis the supervision and the good governance practices. In this light, the Agency will take stock of existing initiatives addressing this problem and will bring together stakeholders from different security domains to discuss the findings.

Output O.2.2.4 – Supporting the Payment Services Directive (PSD) implementation (Scenario 1)

The second Payment Services Directive (PSD 2) will revolutionise the Finance sector and more specifically payments industry. It will affect everything from the way payments are done online, to what information is sent when making a payment. The transposition of the directive is bound to happen in January 2018.

ENISA will continue its support for European Banking Authority (EBA), European Central Bank (ECB) and relevant competent public and private stakeholders to develop guidelines and recommendations for implementing the directive and explore synergies with the NIS Directive.

In this context the Agency will help the relevant authorities with presenting the security requirements and incident reporting status for each MS on PSD II implementing the directive in with the use of a web tool.

This work item builds on previous work of ENISA in the area of supporting activities in the NIS directive (WP 2015 - 2017).

Output O.2.2.5 – Contribute to the EU policy in the area of privacy and data protection with policy input on security measures (Scenario 1)

Within the scope of security measures required by the legal framework on personal data protection and privacy as well as suitable provisions stemming from the draft Cybersecurity Act for the role of ENISA in this area, ENISA will continue promoting trust and security in digital services by means of technical analysis on the implementation of EU legislation addressing privacy and personal data protection. In particular, aspects concerning the technical implementation of the GDPR and of the forthcoming ePrivacy Regulation will be addressed. ENISA will support the implementation of the regulatory aspects related to cybersecurity by making available policy, technical and organisational advice to the Commission in the area of security of personal data and privacy confidentiality of communications for the purpose of implementing security measures. Moreover, ENISA analysis will discuss aspects of shaping technology according to GDPR and ePrivacy provisions, such as for example data security, data minimisation, anonymisation and pseudonymisation, privacy by design and by default, mobile applications as well as aspects of privacy standards.

ENISA will seek to bring together the data protection and privacy considerations on one hand with IT security considerations in the product and services certification area on the other. ENISA will liaise with stakeholders and policy makers as well as with competent authorities in the Member States and EU Institutions, to ensure that the network and information security dimension of data protection and privacy are considered in the EU while striving for synergies between privacy and security and assistance to key stakeholders, namely the Commission and competent EU Bodies.

Currently in its 7th edition, the Annual Privacy Forum (APF) – a conference that has grown to be cost-free for ENISA in the last 2 editions -- remains the instrument of choice to bring together key communities,

namely policy, academia and industry, in the broader area of privacy and data protection while focusing on privacy related application areas. Co-operation activities with European Data Protection Supervisor, the European Data Protection Board and national Data Protection Authorities will be further pursued.

Output O.2.2.6 – Guidelines for the European standardisation in the field of ICT security (Scenario 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 CSCG, observing relevant Technical and Conference programme Committees etc.). New requirements associated primarily with the implementation and secondly transposition of the EU legal instruments in place in the Member States will be taken into account, including aspects of the NIS Directive and the GDPR, as well as preparing for the coming into force of the draft ePrivacy Regulation, and the draft Cybersecurity Act, etc. This output will seek to analyse the gaps and provide guidelines for, in particular, the development or repositioning of standards, facilitating the promulgation and adoption of NIS standards. ENISA brings in this relationship its technical and organisation NIS know-how which can be further leveraged into standards in terms of extending or assessing them to render them more appropriate to stakeholders and more compliance with the prevailing regulatory framework. By bringing in 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 standards developing organisations (e.g. ETSI, CEN, CENELEC), as well as Commission services and Agencies with policy competence thereto as appropriate.

Output O.2.2.7 – Supporting the implementation of European Electronic Communications Code (Scenario 1)

The proposal for the European Electronic Communications Code (EECC) brings substantial improvements to the security component. Built on the general objectives such as ensuring a high-level of security of networks and services, adapting to technological changes and ensuring consistency with other regulatory initiatives (GDPR, NIS Directive), the EECC, once adopted, is expected to bring more harmonisation at EU level and several improvements as regards the security part, such as:

- broadening the scope to include also number-independent (Ni) interpersonal communications services (ICS) (also called OTTs),
- a comprehensive definition of security (focused on availability, integrity, confidentiality and authenticity of the data and services), that will result in more types of incidents being reported,
- clear criteria to be taken into account when notifying incidents (e.g. socio-economic impact).

After its approval, ENISA will provide support for Member States and the industry, so as to assure a proper and efficient implementation of the new requirements in the EECC. ENISA will engage its Article 13a Expert Group and the private sector in order to define guidelines and good practices that will facilitate the implementation process. ENISA will also further facilitate the coordination of Member States to avoid diverging national requirements that may create security risks and barriers to the internal market. ENISA will closely monitor the development of the EECC and identify tasks and priorities for the concerned actors accordingly.

Output O.2.2.8– Supporting the sectorial implementation of the NIS Directive (Scenario 2)

The key NIS Directive obligations are currently implemented horizontally across all NIS Directive sectors. The proposed measures, namely incident reporting, security requirements and criteria for identifying OES, cover the aspects which are common across all sectors. They aim at developing a baseline for all OES.

Sector specific initiatives will have to use the horizontal obligations of the NIS Directive and customise them to address the specific needs and requirements of each sector. It is extremely important, at this stage, to facilitate the sectorial implementation of the NISD in a consistent and coherent way. This way we ensure proper deployment of horizontal measures within the NISD.

In this outcome ENISA will identify for all NISD sectors relevant public and private initiatives at national and EU level and assess their maturity. The Agency, in close collaboration with the Cooperation Group (e.g. based on widely accepted criteria for the prioritisation of the criticality of essential services) and the expertise of ENISA in given sectors (e.g. health, transport), will select two NISD sectors in terms of sectorial implementation.

In that context ENISA will work with all relevant stakeholders, public and private, in each sector and subsector, to identify whether and how a customisation of the horizontal NISD measures could be done. The Agency will do that by taking under consideration the sectorial specifications, standards, and existing initiatives/schemes.

The Agency will use its expertise and knowledge developed within the NISD (WP 2016, WP 2017, and WP 2018) and other CIIP related activities done in the past.

The Agency will work within the framework of the cooperation group, with Member States' experts.

Output O.2.2.9 – Hands on tasks in the area of certification of products and services (Scenario 2)

Pursuant to having adopted the finally approved Cybersecurity Act and its component on certification, the Agency will support the Commission and the Member States by carrying out hands on tasks in this area for the purpose of assisting them in deploying the framework.

Transitioning from policy preparation to policy implementation is a demanding action for the Agency and it will include a framework for certification schemes, a support framework as well as structured interactions with the stakeholders' community and the tools required to carry out these functions.

Working in cooperation with MS certification supervisory authorities, the European Cybersecurity Certification Group and other key stakeholders, ENISA will set the stage for implementation by supporting the functional equivalence of existing certification schemes across the EU (at the MS as well as the EU level) with the emerging EU cybersecurity certification framework for the purpose of integrating existing schemes in the new EU framework in a flexible way. ENISA will continue working with stakeholders to collect, define and understand expectations they have from the EU cybersecurity certification framework. The Agency will implement an action plan in order to fulfil a role in the emerging EU cybersecurity certification framework for the purpose of quickly taking up the new tasks emanating from the Cybersecurity Act along with the Member States.

Practical aspects to be considered include but are not limited to identifying new areas in certification, recommendations on next steps to take at EU level, analysis of impact of certification for manufacturers, governments and end-users, recommendations on prioritisation of schemes, review of overlaps and gaps across proposed schemes etc. Areas for possible cybersecurity certification schemes include IoT, Consumer

Electronics and Cloud Computing, depending of course on requests received by the designated initiator i.e. MS and the Commission.[35] ENISA will carry out support activities in the area of certification and if needed, it will organise its own events in line with the finally approved Cybersecurity Act bringing together key stakeholders. There is also a certain degree of internal preparatory work in terms of IT infrastructure and organisational preparation including management of third party intellectual property rights that will need to be sorted out, to duly support the EU framework.

Objective 2.3. Response to Article 14 Requests under Policy Activity[36]

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

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

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 2018, the allocated resources are indicated in the Summary Section at the end.

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

Summary of Outputs in Activity 2 – Policy. Promote network and information security as an EU policy priority		
Outputs	**Type of output (P=publication, E=Event, S=Support)**	**Performance indicator**
Objective 2.1. Supporting EU policy development.		
Output O.2.1.1 – Support the preparatory policy discussions in the area of certification of products and services (Scenario 1)	P: An action Plan to implement the EU certification framework (business plan for ENISA), Q2 P: Transitioning existing certification schemes to the emerging EU certification framework, Q3 E: 2 workshops with stakeholders, Q1-Q3 E: Support the Commission in the ECCG	For all activities but the last one: More than 10 private companies and 10 EU MS representatives contribute to/participate in the activity For the last activity: in close cooperation with the Commission
Objective 2.2. Supporting EU policy implementation		
Output O.2.2.1 – Recommendations for technical implementations of the eIDAS Regulation (Scenario 1)	P: Recommendations to support the technical implementation of the eIDAS Regulation in Trust Services and/or eID, Q4. P: Recommendations to support the review of the application of the eIDAS Regulation in line with Article 49 of eIDAS, Q4. E: Trust Services Forum, Q2	Engaging at least 5 representatives from different bodies/MS in the validation of the recommendations. Review and acceptance by at least 10 stakeholders (trust service providers, conformity assessment bodies, and supervisory authorities) from at least 5 MS. More than 50 stakeholders participate in the activity

[35] ENISA acknowledges the maturity and suitability of the Commission driven Cloud certification initiative which it will use as indispensable input, upon receiving a suitable request in 2019.
[36] In case of Scenario 2, this objective will be re-allocated based on the new framework.

Output O.2.2.2 – Supporting the implementation of the Work Programme of the Cooperation Group under the NIS Directive (Scenario 1)	S: Support the Cooperation Group in assessing the implementation of the NISD, Q1-Q4 S: Support the work of the Cooperation Group by providing in due time advice and expertise on deliverables and good practices identified by the Group in the 2018-2020 Work Programme, Q1-Q4 E: A workshop related to the tasks of the NISD, Q2-Q4 S: Assist Cooperation Group with the update of existing "living documents" (e.g. security measures) Q1-Q4	Engaging at least 12 MS in ENISA's contributions to the implementation of the NIS Directive (S) 10 MS participate in the workshop/activity (E)
Output O.2.2.3 –Assist MS in the implementation of OES and DSPs Security requirements (Scenario 1)	P: Web tool for mapping the baseline security measures to existing international standards, Q1 P: Stock Taking of security requirements set by different legal frameworks on OES and DSPs, Q4 E: Two workshops with stakeholders from OES sectors, Q2-Q4 P: Web tool for mapping the dependencies' indicators to international standards, Q3 S: Support MS in assessing the implementation of security requirements of the NISD, Q3-Q4	Engage 12 MS in the stock taking of good practices for OES and DSPs (P) More than 10 MS and 15 OES participate in the workshops/activity. (E)
Output O.2.2.4 - Supporting the Payment Services Directive (PSD) implementation (Scenario 1)	P: Web tool presenting the security requirements and incident reporting status for each MS on PSD II, Q2 S: Support EBA, ECB and stakeholders of the finance sector in the implementation of the PSD2and its synergy with the NISD E: 2 workshops with relevant stakeholders (and EGFI, EBA) (Q2-Q4)	Engaging at least 12 Member States regulatory bodies in the workshops Engage at least 10 financial institutions in the workshops
Output O.2.2.5 – Contribute to EU policy in the area of privacy and data protection with policy input on security measures (Scenario 1)	E: 2 workshops with relevant stakeholders, Q1-Q4 P: Recommendations on shaping technology according to data protection and privacy provisions in consultation with competent EU Bodies and the Commission, Q4 P: Reinforcing trust and security in the area of electronic communications and online services, Q4 E: APF 2019, Q3	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/MS participate in the preparation of the recommendations. At least 5 representatives from different bodies/MS participate in the preparation of the recommendations. More than 60 participants from relevant communities
Output O.2.2.6 – Guidelines for the European standardisation in the field of ICT security (Scenario 1)	P: Guidance and gaps analysis for European standardisation in NIS, with reference to the legal framework, Q4.	Participation in drafting and review of the guidelines of at least 5 representatives of European Standard Developing Organizations (SDOs) and relevant services of the European Commission and/or Agencies
Output O.2.2.7 - Supporting the implementation of European Electronic Communications Code (EECC), (Scenario 1)	E: 2 workshops with public and private stakeholders S: Support the Commission, the competent authorities and private sector in proper and efficient implementation of European Electronic Communications Code	At least 10 MS and 5 providers participate in the activities/workshops related to the new EECC

O.2.2.8 - Supporting the sectorial implementation of the NIS Directive (Scenario 2)	P: NISD Sector Specific Initiatives, Q4 E: 2 Workshops with NISD Stakeholders, Q2, Q4. S: Supporting Commission, EU Agencies, MS and private sector in the sectorial implementation of two NISD sectors	Engage 12 MS and 10 OES organisation in NISD sector specific initiatives Engage 12 MS and 10 OES organisation in activities/workshops
O.2.2.9 – Hands on tasks in the area of certification of products and services (Scenario 2)	P: Action plan for an EU certification framework, Q4	Engage stakeholders from at least 15 EU MS
Objective 2.3. Response to Article 14 Requests under Policy		
Output O.2.3.1. Response to Requests under Policy Activity (Scenario 1)	S: Answers to requests.	

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

Objective 3.1. Assist Member States' capacity building

Output O.3.1.1 – Update and provide technical trainings for MS and EU bodies (Scenario 1)

In 2019 most of the activities in this area target at maintaining and extending the collection of good practice guidelines and trainings for CSIRT and other operational personnel. The Agency will support the development of Member States' national incident response preparedness by providing good practice guidance on key elements of NIS capacity building with a focus on CSIRT trainings and services in order to improve skills of CSIRT teams and their personnel. ENISA will further build upon successful work in the area of 'training methodologies and impact assessment'.

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

In 2019, ENISA will further enhance its methodology, seminars and trainings on: a) cyber crisis management and b) the organisation and management of exercises. This activity will build on the current developed material and infrastructure for onsite and online trainings on these subjects. In addition, this activity will cover the delivery of these trainings upon request.

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

The NIS Directive sets as priority for the MS to adopt a national NIS strategy and to monitor its implementation. Since 2017 all 28 MS have published a national NIS strategy. However, in order to align the objectives of the existing NCSS to the requirements of the NISD, many MS will update their current NCSS.

ENISA will continue assisting EU MS to develop their capabilities in the area of National Cyber Security Strategies (NCSS). The Agency, building on previous years' work in this area, will assist MS to deploy 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. Each year the Agency focuses on one of the objectives of the strategy (e.g., collaboration, CIIP, governance).

ENISA will this year, focus on a new objective trending in the NCSS: innovation and start-ups. This derives from the need for the private sector to have incentives to invest on cybersecurity. This is widely depicted in the EU National Cybersecurity strategies as the engagement of the private sector that will pave the way for a Digital Single Market in the EU and for a strong cybersecurity role at international level. ENISA will investigate the activities the MS take under this objective and examine best practices and new potential incentives.

ENISA will continue supporting MS in evaluating and assessing their NCSS, as well as, their NIS initiatives. The Agency will update its NCSS assessment methodology and will validate it with public and private stakeholders. Then ENISA will make this assessment methodology available to MS to use and remain at their disposal should they need assistance in implementing it.

Finally, ENISA will enhance the NCSS map with additional valuable information related to the NISD creating an Info Hub. As for the past 5 years, ENISA will organise the annual NCSS workshop focusing validating the findings of the study.

Output O.3.1.3 – Support EU MS in their incident response development (Scenario 1)

In 2019 ENISA will concentrate its efforts on assisting MS to support their incident response capabilities by providing an updated view on 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 their request, direct support to single Member States to assess and improve their incident response capabilities, including assistance in the preparatory phase of CEF proposals.

The main objectives of this output in 2019 is to help MS and another ENISA's incident response stakeholders, such as the EU institutions, bodies and agencies, to develop, extend and deploy their incident response capabilities and services in order to meet the ever growing challenges to secure their networks. Another objective of this output is to further develop and apply ENISA recommendations for CSIRT baseline capabilities and maturity framework. As a continuous effort, ENISA will continue supporting cross-border CSIRT community projects, tools development as well as the global dialog about common definitions and maturity framework in the incident response domain.

Output O.3.1.4 – Support EU MS in the development of ISACs for the NISD Sectors (Scenario 2)

For many years ENISA works closely with the main operators of essential services in the EU. It has set up several sectoral expert groups covering sectors such as maritime, finance and health.[37] Through this effort and based on this experience with sectors or sector-specific topics like ICS/SCADA, ENISA holds a unique position in the EU to fulfil a key role concerning EU focused ISACs. It is a natural role for ENISA and continuation of its activities in the last 10 years to coordinate, in conjunction with CEF funding, the further

[37] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services

development, implementation and continuation of EU ISACs in the next decade. ENISA is already cooperating with the Commission in developing the ISAC facilities manager concept arising from proposals to develop ISACs reference in the CEF Telecom 2018 Work Programme[38].

ENISA has been working on the topic of CIIP since 2010, so it would make sense to have a special role in Pan European sectorial ISAC. Some examples would include:

- EU Aviation ISAC: ENISA plays a key role in the (further) development of this ISAC. Its added value is mainly based on the network and the specific expertise in the sector (previous and existing studies). The Members consist of airlines and carriers. ENISA is an associate member.
- EU Energy ISAC: ENISA plays a key role in the development and professionalization of this ISAC. ENISA is a full member and is responsible for providing expertise through organizing webinars and educational sessions for its members. In September 2017, it hosted the ISAC meeting in Athens. The EE-ISAC members are preferably, and only, operators.
- EU Financial Institutions ISAC: This ISAC is the oldest and ENISA has been actively involved for many years. It supports the ISAC, for example by hosting the mailing list. ENISA's involvement is mainly to legitimize EU participation. ENISA is an observer.
- EU Rail ISAC: ENISA is facilitating the European Railway operators (infrastructure managers and railway undertakings) creating the European Rail ISAC. Currently more than 23 European stakeholders and the European Railway Agency (ERA) participate in the ISAC. ENISA offer experience and support.

The September 2017 Joint Communication states: "Some first steps have been taken in respect of specific critical sectors such as aviation, through the creation of EASA, and energy, by developing Information sharing and Analysis Centres. The Commission will contribute in full to this approach with support from ENISA, with an acceleration needed in particular with regard to sectors providing essential services as identified in the NIS directive".

ENISA will support MS with the creation of national ISACs through engaging all relevant stakeholders: national competent bodies, the private sector i.e. operators of essential services or manufacturers and other relevant bodies and through assisting, on request, the development of proposals, by Member State endorsed entities, for funding through CEF. ENISA will use the opportunity to continue promoting CEF resourcing under the Telecom Call (objective 2 supporting OES) to further support OES participating in the ISAC. ENISA will also explore the possibility of synergies across national ISACs (national ISAC to national ISAC) as well as across EU sectorial ones. This will help the private companies operating in numerous MS to have increased benefits from such a collaboration.

Objective 3.2. Support EU institutions' capacity building.

Output O.3.2.1. Representation of ENISA on the Steering Board of CERT-EU and coordination with other EU Agencies using the CERT-EU service (Scenario 1)

In December 2017, the operations of CERT-EU were formalised by way of a new Inter-institutional Arrangement. The Members of the Steering Board comprise the participating EU institutions and ENISA which participates as the representative of EU agencies that use the services of CERT-EU.

[38] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2018-cef-telecom-calls-proposals

In this context ENISA will actively participate in the Steering Board of CERT-EU, liaise with the EU Agencies on operational issues related to CERT-EU's activities in particular through the ICTAC (ICT Advisory Committee) of the EU agencies and generally to ensure that the viewpoints of the Agencies are adequately represented. ENISA will also report in to the CERT-EU Steering Board on the evolution of Services required by the Agencies.

Output O.3.2.2. Cooperation with relevant union bodies on initiatives covering NIS dimension related to their missions (Scenario 1)

Already since 2017, ENISA has increased its cooperation efforts with a number of EU bodies. Notable examples are the collaboration with CERT-EU in the context of the WannaCry incident as well as the cooperation in the context of CyCon between Cyber Europe, Cyber Coalition and Locked Shields, and its contribution for the preparation of the table top exercise conducted in the context of the Estonian Presidency.

In this context, in 2019 ENISA will intensify its cooperation efforts and liaise with the relevant EU Bodies[39] (including EASA, CERT-EU, EDA – including civil/ defense cooperation – etc.).

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 cyber security knowledge and skills to help protect their digital lives. Aspects like cybersecurity culture and insurance will be further 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 Member States.

Output O.3.3.1 – European Cyber Security Challenges (Scenario 1)

Both the growing need for IT security professionals and skills shortage are widely acknowledged. To help solve this, ENISA is supporting national cybersecurity competitions for students, security professionals and even non-IT professionals, with the goal to find cyber talents and encourage all of them to pursue a career in cybersecurity.

Thus, in order to promote capacity building and awareness in NIS among youngsters and future cyber security experts in the EU MS, ENISA will continue to promote and advise EU MS on running national 'Cyber Security Challenge' competitions.

The Agency will also continue to support the planning and development of the European Cyber Security Challenge 2019 final. The goal for 2019 will be to further increase the interest in this type of events by promoting excellence in the form of cyber competitions

[39] Memorandum of Understanding between The European Union Agency for Network and Information Security (ENISA), The European Defence Agency (EDA), Europol's European Cybercrime Centre (EC3), The Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU), available at: https://www.eda.europa.eu/docs/default-source/documents/mou---eda-enisa-cert-eu-ec3---23-05-18.pdf

Output O.3.3.2 – European Cyber Security Month deployment (Scenario 1)

The metrics built into the ECSM- European Cyber Security Month have shown an increased number of participants, and a better engagement level from year to year. This was made possible with the support of a vibrant community. In 2019, ENISA will continue reaching out to Member States and citizen alike. Previously proposed pillars remain: support a multi-stakeholder governance approach; encouraging common public-private activities; assess the impact of activities, optimising and adapting to new challenges as appropriate.

Output O.3.3.3 – Support EU MS in cybersecurity skills development (Scenario 2)

In 2019, ENISA will promote a series of new activities in the area of cyber security skill development which will focus on identifying current national and EU wide initiatives. The main output of this activity will be a database of existing services and programs in the EU that aim to enhance cyber security skills among EU citizens, in general, and cyber security experts, in particular. The 2019 stocktaking exercise will cover academia, public institutions and private companies. As part of this program, a skill development scheme and maturity model will be defined, by taking into account existing and similar frameworks and initiatives.

Objective 3.4. Response to Article 14 Requests under Capacity Activity[40]

Output O.3.4.1 – Response to Requests under Capacity Activity (Scenario 1)

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

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 2018, the allocated resources are indicated in the Summary Section at the end.

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

Summary of Outputs in Activity 3 – Capacity. Support Europe maintaining state-of-the-art network and information security capacities		
Outputs	**Type of output (P=publication, E=Event, S=Support)**	**Performance indicator**
Objective 3.1. Assist Member States' capacity building		
Output O.3.1.1 - Update and provide technical trainings for MS and EU bodies (Scenario 1)	P: Update of existing operational training material and customization to the needs of an NISD Sector (details on operational category can be found on ENISA training website), Q4 P: Delivery of a training session of the NISD Sector customized training material mentioned above. S: TRANSITs (European CSIRT training event) support	At least one training material updated to support operational practices of CSIRTs in Europe. At least one NISD critical sector covered in the training session. Support at least 3 TRANSITs events.

[40] In case of Scenario 2, this objective will be re-allocated based on the new framework.

Output O.3.1.2 – Support EU MS in the development and assessment of NCSS (Scenario 1)	P: Good practices in innovation on cyber security under the NCSS, Q3- Q4 S: Developing an Info Hub for NCSS in MS (Tool), Q3-Q4 S: Support MS in the deployment of an NCSS assessment methodology E: Workshop with EU MS on NCSS development, Q2-Q4	Engage stakeholders from at least 5 EU MS in using the NCSS assessment methodology (S) Engage stakeholders (national competent authorities or private sector) from at least 12 EU MS in this activity/workshop (P and E).
Output O.3.1.3 – Support EU MS in their incident response development (Scenario 1)	P: Supporting development of CSIRTs capabilities in Europe, Q4 P: CSIRT online Inventory update – European interactive map of CSIRTs, Q2 & Q4 P: ENISA CSIRT maturity framework review, Q4 S: Continue activities and involvement in CSIRT structures (e.g. FIRST, TF-CSIRT-TI, NATO NCIRC, GFCE including CEF MeliCERTes project), Q1-Q4	Engage or support at least 5 CSIRTs in the development or improving of incident response capabilities in Europe Two CSIRT inventory updates During 2019, support or advisory provided at least for two CSIRTs to enhance their team's maturity. ENISA supports at least 2 international CSIRT initiatives in community fora like FIRST, TF-CSIRT-TI or GFCE.
Output O.3.1.4 – Support EU MS in the development of ISACs for the NISD Sectors (Scenario 2)	P: A toolkit for creating an EU ISAC undertaken in conjunction with CEF ISACs Facilities manager, Q4 S: Support relevant public and private stakeholders in establishing EU ISACs using the CEF funding opportunities, Q1-Q4. S: Support the Commission and facilitate alignment of the CEF EU level sectoral ISACs Facilities Manager's tasks with work on ISACs development, Q2-Q4	Engage at least 12 organisations representing at least 3 sectors from at least 8 MS in this activity (P)
Objective 3.2. Support EU institutions' capacity building		
Output O.3.2.1 – Representation of ENISA on the Steering Board of CERT-EU and coordination with other EU Agencies using the CERT-EU service (Scenario 1)	S: Attending CERT-EU SB meetings S: Liaison with EU agencies using CERT-EU services notably through ICTAC	Consultation with EU Agencies and representing their views at CERT-EU SB level.
Output O.3.2.2 - Cooperation with relevant union bodies on initiatives covering NIS dimension related to their missions (Scenario 1)	P: Report on the cooperation activities with relevant union bodies, Q4	Engage the relevant EU stakeholders (including EASA, CERT-EU, EDA – including civil/ defence cooperation – etc.)
Objective 3.3. Assist in improving private sector capacity building and general awareness		
Output O.3.3.1 – Cyber Security Challenges (Scenario 1)	S: European Cyber Security Challenge support, Q1-Q4 E: Q2-Q3: 'Award workshop' for winners of the European Cyber Security Challenge 2019 (ENISA promotes best of the best)	At least two additional EU MS organise national cyber security challenges in 2019 and participate in the European Cyber Security Challenge Final.
Output O.3.3.2 – European Cyber Security Month deployment (Scenario 1)	S: ECSM support, Q1-Q4 P: ECSM evaluation report, Q4	All 28 EU MSs and at least 10 partners and representatives from different bodies/MS participate in/support ECSM 2018 (private and public sectors).

Output O.3.3.3 - Support EU MS in cybersecurity skills development (Scenario 2)	P: Q4, Stocktaking of existing services and programs in the EU that aim to enhance cyber security skills among EU citizens, in general, and cyber security experts	Engage at least 15 organisations representing academia, public institutions and private companies from at least 10 MS
Objective 3.4. Response to Article 14 Requests under Capacity Activity		
Output O.3.4.1 - Response to Requests under Capacity Activity (Scenario 1)	S: Answers to requests.	

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

Objective 4.1. Cyber crisis cooperation

Output O.4.1.1 – Planning of Cyber Europe 2020 and Cyber SOPEx (Scenario 1)

In 2020, ENISA will organise the fifth pan-European cyber exercise, Cyber Europe 2020 (CE2020). In 2019 ENISA will prepare the plan of CE2020. This exercise will closely follow up and build upon the lessons learned and actions from previous exercises, such as CE2018.

CE2020 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, Single Point of Contacts and Competent Authorities set up under the NIS Directive, including focusing on one or more of the essential sectors. Also there will be designs to exercise the various aspects of the Cyber Crisis Collaboration Blueprint. Depending on the availability of resources in 2020 ENISA will also enhance the observers role (introduced in 2018) striving to make best use of observers.

The high-level exercise program brief will include the strategic dimensions of the exercise will be prepared based on the lessons learned from CE2018, to drive the whole planning process. The exercise brief will be given for comments and approval to ENISA's Management Board after consultation with the MS Cooperation Group and the CSIRTs Network set up under the NIS Directive. Following this ENISA will assemble group of planners from the participating countries to work closely towards developing a detailed exercise plan (ExPlan) in 2019. ENISA will involve the group of planners in the relevant planning steps and take into account their input towards a consented plan. The exercise planning will avoid overlaps with other major related activities.

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

Finally, in 2019 ENISA will organise the Cyber SOPEx exercise (formerly known as EuroSOPEx) 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 in between them. As in previous years the exercise will be planned with the support of representatives from the involved organisations. The exercise is expected again to have as high-level goals to raise awareness of cooperation procedures, train participants in using the cooperation infrastructures, such as the communication and information sharing and ultimately contribute to increase trust within the CSIRTs Network. Guidance should be found in the CSIRTs Network on planning the exercise. There will not be any private entities involved in this exercise.

Output O.4.1.2 – Support activities for Cyber Exercises (Scenario 1)

Since 2014 ENISA started the development of the Cyber Exercise Platform (CEP). CEP hosts a number of services that ENISA offers to the Member States and EU Institutions, such as: exercise organisation and management, exercise playground with technical incidents, map of exercises and hosting the exercise development community. In the interests of efficiency, ENISA will seek to align the CEP with the MeliCERTes facility so that Cyber Exercises can be integrated in the main operational co-operation platform under the CSIRTs Network.

In addition, new content and exercise incident challenges and material will be developed in order to keep up the interest of the stakeholders and make CEP a central tool in cyber security exercising for all stakeholders. The CEP platform opens new opportunities for ENISA to enlarge the user base and thus offer to the operational cyber security communities opportunities to exercise and gain experience and knowledge. One way to develop such exercise incident material will be through the engagement of the experts' community.

Finally, following up on possible requests for support by competent authorities, EU bodies and other relevant organisations to plan and setup Technical Cyber Exercises (CTEx), or other types of exercises, utilising the technical incidents and the gaming infrastructure in the Cyber Exercise Platform (CEP).

Output O.4.1.3 – Support activities for Cyber Crisis Management (Scenario 1)

Since 2015, ENISA offers the secretariat to the MS developing EU-level standard cooperation procedures, which formed the basis of the CSIRTs Network SOPs. ENISA will continue to support Member States in the implementation of the Cyber Crisis collaboration blueprint. In particular, ENISA will further support the maintenance of the CISRTs Network SOPs.

The 2016 Communication "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry" encouraged Member States to make the most out of the NIS Directive cooperation mechanisms and to enhance cross-border cooperation related to preparedness for a large-scale cyber incident.

The 2017 blueprint called for the establishment of "*practical implementation guidelines as regards the integration of their national crisis management and cybersecurity entities and procedures into existing EU crises management mechanisms, namely the IPCR and EEAS CRM. In particular, Member States should ensure that appropriate structures are in place to enable the efficient flow of information between their national crisis management authorities and their representatives at EU level in the context of EU crisis mechanisms*".

In this light, ENISA will support individual Member States in setting up, improving and testing their own cyber crisis management frameworks in order to ensure a smooth adoption of the blueprint and to foster synergies in crisis management practices across Member States. ENISA will support the cross-border cooperation between Member States, relevant authorities, and facilitate the engagement with the crisis management framework at national and EU level. Activities offered will range from remote trainings on crisis management and public affairs handling, on-site workshops, document revision and table-top exercises, including opportunities in CE2020 for testing national crisis management structures.

Last, building upon the after action report from Cyber Europe 2018 and in an effort to improve crisis management practices at sectorial level, ENISA will draft a report on cyber crisis management practices in the aviation sector.

Output O.4.1.4 – Supporting the implementation of the information hub (Scenario 2)

Decision-supporting intelligence in the cybersecurity domain is scarce, despite today's security information overload[41]. ENISA is at the crossroads of most if not all public-private, cross-sector cybersecurity communities in Europe, from the technical to the strategic level. As indicated in the EC Communication on Building strong cybersecurity for the EU[42], ENISA serves as "the focal point for information and knowledge in the cybersecurity community". As a result, ENISA is in a unique position to leverage its network to gather information, process it and foster timely, tailored and highly relevant situational awareness to support decision-making in both the public and the private European sectors, as recommended by the EC in the blueprint:

"As part of the regular cooperation at technical level to support Union situational awareness, ENISA should on a regular basis prepare the EU Cybersecurity Technical Situation Report on incidents and threats, based on publicly available information, its own analysis and reports shared with it by Member States' CSIRTs (on a voluntary basis) or NIS Directive Single Points of Contact, European Cybercrime Centre (EC3) at Europol and CERT - EU and where appropriate the European Union Intelligence Centre (INTCEN) at the European External Action Service (EEAS). The report should be made available to the relevant instances of the Council, the Commission, the HRVP and the CSIRTs Network".

In order to support the drafting of these reports and process meaningfully the massive amounts of inputs they require, ENISA has developed in 2018 a prototype to perform automatic classification of documents as well as simple automatic generation of reports by applying Natural Language Processing and Machine Learning techniques. This prototype is the first brick of a toolset meant to assist in the development of EU Cybersecurity Situation reports, supporting a steady increase and offering guarantees in terms of production time, quality and consistency.

For this particular output, ENISA will leverage the experience gained in drafting EU Cybersecurity Technical Situation Reports with the prototype to further develop the Natural Language Processing features in order for the tool to transition from paragraph-based proposals to the production of meaningful sentences. Similarly, this experience will be leveraged to further develop the Machine Learning algorithms of the prototype to allow for a significant increase in number and type of information sources.

Output O.4.1.5 – Supporting the implementation of the cyber crisis collaboration blueprint (Scenario 2)

ENISA will support EU Institutions in the implementation of the Cyber Crisis collaboration blueprint. As specified in the blueprint: *"The EU Cybersecurity Crisis Response Framework should in particular identify the relevant […]EU institutions […]at all necessary levels - technical, operational, strategic/political and develop, where necessary, standard operating procedures that define the way in which these cooperate within the context of EU crisis management mechanisms. Emphasis should be placed on enabling the exchange of information without undue delay and coordinating the response during large-scale cybersecurity incidents and crises."*

[41] Scott J., Spaniel D. *CISO Solution Fatigue Overcoming the Challenges of Cybersecurity Solution Overload*, Hewlett Packard, Institute for Critical Infrastructure Technology http://icitech.org/wp-content/uploads/2016/06/CISO-Solution-Fatigue.pdf

[42] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN

In particular, ENISA will assist the Commission and the Member States in further developing bilateral and multilateral procedures for cyber crisis cooperation with:

- DG Connect
- the European Cybercrime Centre at Europol (Europol/EC3)
- the EU Intelligence Analysis Centre (INTCEN)
- the EU Military Staff Intelligence Directorate (EUMS INT) and Situation Room (SITROOM) working together as SIAC (the Single Intelligence Analysis Capacity)
- the EU Hybrid Fusion Cell (based in INTCEN)
- the Computer Emergency Response Team for the EU Institutions (CERT-EU)
- the Emergency Response Coordination Centre in the European Commission
- and possibly the Cybersecurity Emergency Response Fund.

ENISA will drive working groups to initiate or further develop these procedures in the context of the blueprint, from defining emergency directories and update processes to structuring cooperation activities during crises. This is what the Blueprint calls as priorities.

ENISA will assist Member States to engage EU Cybersecurity Crisis Response Framework with National Cybersecurity Crisis Response Frameworks.

Furthermore, upon request or emerging needs, ENISA will organise workshops and/or table-top exercises to validate that these procedures allow for the exchange of information without undue delay, prior to their use either in real life or in larger exercises such as Cyber Europe.

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 (Scenario 1)

ENISA will continue its support to the Commission and Member States in the implementation of the NIS Directive, in particular in the area of CSIRTs. As part of this activity, ENISA will continue its tasks as the secretariat of the CSIRTs Network and actively support its functioning by suggesting ways to improve cooperation and trust building among CSIRTs. The agency will also support this cooperation by developing and providing guidance and good practices in the area of operational community efforts, such as on information exchange and secure communication, on request by the members of the 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 own work programme (action plan -midterm goals and objectives).

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 testing and use of the Common Service Platform (CSP) co-operation mechanism for CSIRTs, known as MeliCERTes of the Cybersecurity DSI.

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

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

Output O.4.2.2 – Support the fight against cybercrime and collaboration between CSIRTs and law enforcement (Scenario 1)

In 2019, ENISA will continue supporting the cooperation between the CSIRT and the law enforcement communities and the extensions that this collaboration may have to the judiciary. ENISA will continue its effort to support the EU wide objective on fight against cybercrime and continue liaising with various stakeholders at EU (e.g. Europol and possibly Eurojust), as well as with select stakeholders at Member States level.

In particular, in 2019 ENISA will collect input from key stakeholders and prepare a roadmap to further enhance the cooperation between the CSIRTs and the law enforcement along with their interaction with the judiciary. The roadmap will not necessarily be made public; it is likely to be distributed instead to select stakeholders. In addition, ENISA will co-organise together with Europol/EC3 the annual workshop for national and governmental CSIRTs and their LEA counterparts.

Output O.4.2.3 – Supporting the implementation and development of MeliCERTes platform (Scenario 1)

By the end of 2019, ENISA will take over the central component of MeliCERTes, which is destined to be the primary collaboration platform between participating Member States CSIRTs and which is oriented to enlarge EU MS preparedness, cooperation and coordination to effectively respond to emerging cyberthreats as well as to cross-border incidents. The Agency will also work together with the Commission to define (a) the extent of support for the implementation of MeliCERTes running in the CSIRTs premises and (b) the support for the maintenance of the underlying codebase of the MeliCERTes system. Based on this work, we will establish corresponding procedures and SLAs for the support and work with the Commission to ensure that the code base is correctly supported. In particular ENISA with the endorsement of the Commission will lead on the development and finalisation of a sustainable governance arrangement for MeliCERTes with the enabling legal requirements for the participating Member States. ENISA also will support the work of the Commission in resourcing capabilities on cybersecurity through CEF calls in accordance with the objectives of the NIS Directive, including assistance in the preparatory phase of CEF proposals related with the support of MeliCERTes platform.

Due to the sensitivity of the data and the level of trust required by our stakeholders, special care and diligence is needed in order to correctly plan, deploy, administrate and maintain the different systems related with MeliCERTes platform, therefore high standards of security must be reached in order to provide internal and external secure operation capabilities, continuous integration of the software and support to users.

During 2019, ENISA will deploy different systems and processes with the aim of being able to support, maintain and develop the platform and related activities, including collaboration, involvement and alignment on Cyber Exercises and on the CSIRTs Network.

Objective 4.3. Response to Article 14 Requests under Community Activity[43]

Output O.4.3.1 – Response to Requests under Community Building Activity (Scenario 1)

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

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 2018, the allocated resources are indicated in the Summary Section at the end.

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

Summary of Outputs in Activity 4 – Community. Foster the emerging European network and information security community		
Outputs	**Type of output (P=publication, E=Event, S=Support)**	**Performance indicator**
Objective 4.1. Cyber crisis cooperation		
Output O.4.1.1 – Planning of Cyber Europe 2020 and Cyber SOPEx (Scenario 1)	P: CE2020 Exercise Plan (restricted), Q4 E: Exercise planning events, Q2 & Q3 E: Cyber SOPEx 2019,	At least 80% EU/ EFTA Member States and countries confirm their support for Cyber Europe 2020 At least 25 CSIRTs Network (CNW) member teams confirm their support for Cyber SOPEx 2019
Output O.4.1.2 – Support activities for Cyber Exercises (Scenario 1)	S: Support for the maintenance and further development of the Cyber Exercise Platform, with a view towards its alignment with the MeliCERTes facility, Q4	At least 4 CSIRTs from different Member States use CEP in alignment with MeliCERTes for exercise related activities
Output O.4.1.3 – Support activities for Cyber Crisis Management (Scenario 1)	P: Report on Good Practices in Cyber Crisis Cooperation and Management in Aviation, Q4	At least 5 stakeholders of the Aviation sector from EU MS consulted.
Output O.4.1.4 – Supporting the implementation of the information hub (Scenario 2)	S: Support for other EU Agencies having a role in cybersecurity.	Established communication procedures with all affected agencies and EU bodies having a role in cybersecurity.
Output O.4.1.5 – Supporting the implementation of the cyber crisis collaboration blueprint (Scenario 2)	P: Q4 Supporting the implementation of the Cyber Crisis collaboration blueprint	At least 5 stakeholders from EU MS consulted.
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 (Scenario 1)	S: Provide CSIRTs Network Secretariat support (e.g. logistics, organisation of the meeting, agenda management, meeting minutes; conference calls infrastructure; working groups support; facilitate adhoc operational	Engage all 28 MS designated MS CSIRTs and CERT-EU in the activities described in the Network work programme (action plan midterm goals and objectives)

[43] In case of Scenario 2, this objective will be re-allocated based on the new framework.

	cooperation e.g. support CNW operations during cross border incident or crisis) E: Network meetings' organisation and support (minimum 1 event and maximum 3 events) P: Q1-Q4: Facilitate preparation of the next evaluation report for the cooperation group S: Q1-Q4, CSIRTs Network active support (e.g. communication support; maintaining and improving available means for communication in line with decisions in the CSIRTs Network – e.g. outcome of Working Groups' effort. P: Q1-Q4, Continue improving CSIRTs Network Cooperation Portal functionalities and security. E: Trust building exercise (co-located with the regular CSIRTs Network meeting) P: Q4 Further support for CNW specific information exchange and secure communication issues (according to the CSIRTs Network Action plan) S: Active Secretariat support and engagement during annual Cyber SOPEx 2019 exercise of the CSIRTs Network according to the CNW SOPs. S: CSIRT maturity assessment and peer review support for members of the CSIRTs Network.	90% of MS standing CSIRT representatives and CERT-EU participated in CSIRTs Network regular meetings. Support CNW Chair in preparation of the next evaluation report for the cooperation group Provide at least conference call facility for the need of the CSIRTs Network operations. At least two penetration tests and necessary security and functionality improvements made to the Cooperation Portal. At least one team building event organised during regular CSIRTs Network Meeting At least four communication checks done to test CNW communication channels readiness. Provide active support to the facilitator of the exercise during execution according to SOPs. Assist at least one CSIRTs Network member with the maturity assessment and peer review
Output O.4.2.2 – Support the fight against cybercrime and collaboration between CSIRTs and law enforcement (Scenario 1)	P: Roadmap to further enhance the cooperation between the CSIRTs and law enforcement and their interaction with the judiciary (distribution to selected stakeholders, not for publication) E: Q3, annual ENISA/EC3 workshop for national and governmental CSIRTs and their LEA counterparts	At least 5 MS CSIRT representatives, 5 MS law enforcement representatives, 2 MS judiciary representatives and EC3 participate in the preparation of the roadmap At least 15 MS participate in ENISA/EC3 annual workshop
Output O.4.2.3 - Supporting the implementation and development of MeliCERTes platform (Scenario 1)	P: Q4 Takeover of the central component of MeliCERTes: Project management support and technical assistance to the Commission, encompassing assistance with procurement as appropriate in respect of the acquisition of MeliCERTes. P: Q4 Agree responsibilities of the Agency for (a) level of support for remote components of the system and (b) management of the code base	Engage the Member State authorities on strategy and resourcing and also the CSIRTs Network members for technical and operational support.
Objective 4.3. Response to Article 14 Requests under Community Activity		
Output O.4.3.1. Response to Requests under Community Building Activity (Scenario 1)	S: Answers to requests.	

Activity 5 – Enabling. Reinforce ENISA's impact

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, the, Management Board Secretariat will continue the administration of the Management Board meetings and the administrative correspondence that takes place between meetings, including the management of the MB Portal. In 2019, MB Secretariat will continue to support the Management Board (MB) and the Executive Board in their functions by providing secretariat assistance.

In relation to the MB, following the applicable rules, one or two (Scenario 2) ordinary meetings will be organised during 2019 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 **Resources Department** (RD) oversees a variety of programs, projects and services relating to the overall management of the Agency, supporting the Executive Director Decision is areas as personnel, finance, communications, press, purchasing, technology, facilities management, health, safety, security, protocol, liaison with local authorities, etc.

The aim of the RD is to provide this assurance and at the same time provide the best level of efficiency and use of the resources that are made available for the Agency. This also includes coordination with the European Commission Internal Audit Service, European Court of Auditors, European Ombudsman, European Commission European Anti-Fraud Office, EU DG HR, EU DG BUDGE, DG CNECT, etc. All internal policies related to transparency, anti-fraud policy, whistle-blowers protection, declarations of interests, etc. are addressed within this activity.

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

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

The Core Operations Department (COD) coordinates the delivery of the core activities of the agency. As such, the main role of the Core Operations Department is to deliver activities A1-A4 of this work programme. The Core Operations Department also includes the Policy Office and the Public Affairs team and the support of the PSG and NLO network is also carried out within COD.

Policy Office

Through the Policy office, the Agency initiates and further develops strategic cooperation with relevant stakeholders active in cybersecurity community. For instance, the Agency engages in policy and strategy discussions with political and policy decision makers (by participating or organizing e.g. MEP Breakfasts).

Furthermore the Agency engages and further develops strategic relationships with e.g. specific industry sectors at decision making level, and identifies the strategic issues on cybersecurity. Some of the results of these activities of the Policy Office are published as opinion papers on ENISA webpage. Besides these activities, more details of the activities delivered by Policy Office and Public Affairs team are detailed in Objective 5.2 Engagement with stakeholders and international activities.

Quality management is part of the Policy Office. The Agency implements a Quality Management System (QMS) to support its regulatory and strategic goals by means of a quality management approach. The methodology is based on the Plan-Do-Check-Act (PDCA) cycle, documented in a dedicated SOPs and applied accordingly. Planning activities of the Agency, including Single Programming Document preparation and Work Programme coordination are part of Policy Office list of tasks.

Public Affairs Team

The Public Affairs Team (PAT) is responsible for coordinating all activities with the media and press, including press releases, news items and interviews. The PAT team also plays a major role in supporting events attended by the Agency, ensuring that ENISA is well represented from a public affairs perspective, that appropriate publicity material is available and, where appropriate, that booths are arranged and supported.

Internal control

ENISA is aiming implement the new COSO framework 2013 as well as its new requirements in order to be align with the European Commission.

The exercise will include the adoption of this framework by the Management Board as well as the assessment of the compliance of these Internal Controls.

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

IT

ENISA has launched a project that will run during the second half of 2018 in order to assess information security risks and determine missing or out of date IT operational procedures. The project will provide a roadmap and the changes needed in order to mitigate the identified risks. IT Advisory Committee has decided that data the development of a datacentre recovery site is absolutely necessary in order to enhance the IT service availability.

By end of 2019 it is expected that all business applications will be securely available on the most widely used mobile devices. By this timeframe the platform consolidation should be complete and mature, with adequate, flexible and advance reporting and monitoring tools. Is expected that 2018 will consolidate the support technology in the Agency with modern, adequate and flexible business applications.

IT is supporting the implementation of a Stakeholders Relationship Management application that will support the overall stakeholder's management, communications and internal information sharing. This application also involves an effective event management platform and internal case management to be used as service internal client support for requests.

Task	Objective	Level of completion 2019	Level of completion 2020	Level of completion 2021
Keep ENISA systems safe from cybersecurity incidents (from exterior) – prevent and react to threats	Security	100%	100%	100%
Percentage of IT managed servers patched at deadline (24h after released from supplier)	Security	100%	100%	100%
Exchange server availability	Efficiency	95%	98%	98%
Availability of internal applications	Availability	95%	95%	95%
Help desk, reply with success to all service requests	Efficiency	95%	99%	99%

Finance, Accounting and Procurement

The key objective is to ensure the compliance of the financial resources management within the applicable rules, and in particular with the principle of sound financial management (namely the principles of effectiveness, efficiency and economy) as set down in the Financial Regulation. The Accounting principles are followed in order to ensure that financial statements are presented in a manner that is relevant, reliable, comparable and understandable. Furthermore, the Agency continues its good practice to close accounts and process payments within the time frame.

The Agency continues the deployment of tools used to simplify and automate its work in the area of Budget, Finance and Procurement. Further development of in-house systems is expected in the future years to improve the utilization of resources, to have a better overview of all financial and procurement processes, to provide better reporting and a high level transparency. Internal policies will be revised to ensure that they are up to date with the Financial Regulation and Procurement rules, but also to implement a clear guidance for internal use and optimise the available resources.

By mid-2019 an analysis will be made on the cost efficiency of outsourcing activities versus services received. The aim is to reduce costs and streamline processes in order to achieve a high support level towards ENISA. The Unit strives to maintain low budget transfers during the year, having planned and justified carry overs.

Task	Objective	Level of completion 2019	Level of completion 2020	Level of completion 2021
Budget Implementation (Committed appropriations of the year)	Efficiency and Sound Financial Management	99%	99%	99%
Payments against appropriations of the year (C1 funds)	Efficiency and Sound Financial Management	85%	90%	90%
Payments against appropriations carried over from year N-1 (C8 funds)	Efficiency and Sound Financial Management	93%	95%	95%
Payments made within Financial Regulation timeframe	Efficiency and Sound Financial Management	98%	98%	98%
Planned Procurement Activities versus actual implementation of the year	Efficiency and Sound Financial Management	70%	70%	90%

Human Resources

The ultimate goal of HR is to attract, select, develop and retain highly qualified staff, to put in place optimal organisational structures, to promote a safe working environment, to create a culture that reflects ENISA's vision and values in which staff can give their best in achieving the organisation's objectives. By offering a broad array of services (Recruitment, Performance management, L&D, Career management, Working

conditions, Social rights, etc.) HR's objective is to deliver a successful day-to-day management of ENISA statutory staff and external staff (e.g. trainees) in compliance with the Staff Regulations/CEOS. Additionally, investment and efforts are focusing on several projects such as the acquisition of an E-Recruitment tool, the development in closed collaboration with the European Commission's services of SYSPER, the implication of the new GDPR Regulation on HR matters, the security's upgrade and rationalisation of personnel files management, etc.

2019 might see ENISA growing with additional resources to fulfil its new mandate, having in mind the full compliance achieved in 2018 of the agreed 5% staff reduction[44]. Most of the staff would be allocated to operational needs with some allocation of staff to ensure sufficient capacity for the Agency's enabling. It would also imply from an HR perspective to take a strategic approach to its workforce requirements, with an emphasis on attracting, selecting, developing and rewarding staff based on a Talent Management approach.

Task	Objective	Level of completion 2019	Level of completion 2020	Level of completion 2021
Efficient management of selection procedures	Reduction of time to hire (*in line with EU HR standard definition it is the time between the closure date for applications and the signature of the reserve list by the ED)*	5 months	5 months	5 months
Turnover of staff	Reduce the turnover ratio of statutory staff (TA and CA)	<15%	<15%	<15%
Staff's Performance Management	Implementation and monitoring of the appraisal and reclassification exercises (launching and closing the exercises)	100%	100%	100%
Staff Survey	Participation of staff in the staff survey	65%	70%	75%

Legal affairs, data protection and information security coordination

Legal Affairs

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

Data Protection Compliance tasks and Data protection Office

The main tasks of the Data Protection Officer (DPO) include[45]:

- Inform and advise ENISA of its obligations as provided in the applicable legal provisions for the protection of personal data 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 and the applicable legal framework for data protection.

[44] The Agency reduced its staffing in 2018 in full compliance with the Art.27 of Interinstitutional Agreement of 02 December 2013 (2013/C 373/01) on 5% staff cut.

[45] The tasks of the DPO are mandated in the applicable legal framework for data protection at ENISA, i.e. Regulation (EC) 45/2001 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. Note that this Regulation is currently under revision See relevant Commission's proposal in: http://ec.europa.eu/newsroom/document.cfm?doc_id=41158. There has been an agreement by the co-legislators with regard to the revised Regulation but the final number and text are not yet made available. This part should be updated once the revised Regulation is officially published.

- Monitor the implementation and application of the applicable legal framework for the protection of personal data at ENISA, including the requirements for data security, information of data subjects and their requests in exercising their rights..
- Monitor the documentation, notification and communication of personal data in the context of ENISA's operations.
- Act as ENISA's contact point for EDPS on issues related to the processing of personal data; co-operate and consult with EPDS whenever needed.

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 to develop and implement information security policies, standards, guidelines and baselines that seek to secure the confidentiality, integrity and availability of the information systems of the Agency. The ISO is instrumental in incident handling and incident response and security event monitoring. The ISO also leads the security training for the Agency's staff and he provides security guidance on all IT projects, including the evaluation and recommendation of technical controls. In 2019 the ISO will contribute to such goals as:

- Developing assurance frameworks to demonstrate ongoing improvement of the information security management system. This includes:
  - developing KPIs
- Monitoring and reporting the following to IT Advisory Commitee;
  - KPI results
  - Incidents identified and managed
  - Non-Compliances with policy identified and addressed
- Improving the security posture of ENISA by planning penetration tests and vulnerability assessments
- Advising on security policies and updating existing ones in line with the evolution of threats and risks
- Improving the internal security training for ENISA staff
- Implementing new systems and tools that can support improvements on Information Security.

Objective 5.2. Engagement with stakeholders and international activities

Stakeholders communication and dissemination activities

In 2019, ENISA will continue its efforts to improve its focus on key activities and engage the higher possible number of stakeholders. This includes the various groups of stakeholders that count with institutional, academia, industry, citizens, etc. In its engagement with the stakeholders, the Agency is guided by principles as balanced representation, openness, transparency and inclusiveness.

Dissemination and Outreach

The Agency will continue developing various tools and channels including the web site and with strong emphases in social media. Dissemination activities are the responsibility of the Stakeholders Communication team that will seek the appropriate level of outreach activities to take ENISA´s work to all interested and to provide added value to Europe.

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

several actors in Europe. ENISA is consistent of this fact and will work with all interested to reach the Citizens that require information about the work that is developed by the Agency.

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

Area	Metric	Increase Relative to Previous Year		
		2019	2020	2021
Volume of media material published by the agency	Number of press communications published	30%	30%	30%
Number of social media items	Number of social media items published	50%	40%	40%
Number of social media followers	Number of social media followers	30%	25%	25%
Number of corporate events	Number of corporate events	10%	40%	10%
Website traffic	Number of page views/visits/unique visitors/returning visitors	20%	30%	30%

Internal communications

Stakeholders' communications comprise the internal and external stakeholders. From an internal perspective the team is responsible to support the internal communication activities aim to keep all those working within the Agency informed and to enable both management and staff to fulfil their responsibilities effectively and efficiently. A strong corporate culture improves staff engagement and ultimately the implementation of the work program. It is envisaged to do an annual review of this Strategy to ensure that it is kept up to date and appropriate for the Agency.

Task	Objective	Level of completion		
		2019	2020	2021
Maintain staff informed on ENISA Activities (internal communications)	20 staff meetings per year	90%	100%	100%
Team building activities	Events with participation of all staff	2	2	2

Permanent Stakeholders Group

In 2019, ENISA will continue to support the PSG and will aim to reinforce the contribution of the Permanent Stakeholders Group (PSG) to the ENISA Work Programme.

The Permanent Stakeholders' Group (PSG) is composed of "nominated members" and members appointed "ad personam". The total number of members is 33 and they come from all over Europe. These members constitute a multidisciplinary group deriving from industry, academia, and consumer organisations and are selected upon the basis of their own specific expertise and personal merits. Three (3) "nominated members" represent national regulatory authorities, data protection and law enforcement authorities.

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

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

National Liaison Officer Network

ENISA in 2017 has kicked off various activities aiming at strengthening the cooperation with its National Liaison Officers' (NLO) Network. These activities were continued and were further elaborated in 2018. NLOs are key actors for the Agency's daily work and they warrant the interaction with select public sector entities in the MS while they provide assurance in terms of outreach, effective liaison with the MS and dissemination of ENISA deliverables.

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

- NLO meetings to discuss possible improvements in the collaboration with ENISA and input on selected ENISA projects. Improvements aim at leveraging on the NLO network for the dissemination of ENISA's work to the EU Member States and EFTA countries.
- The members of the NLO network will continue to receive information on ENISA deliverables, upcoming ENISA project related tenders, news, working groups entailing requests for identification of experts in the MS, vacancy notices, and events organised by ENISA or where the Agency contributes to (for example co-organiser, etc.) as well as time-critical information.
- The Agency maintaining and sharing with the NLO network information on all relevant ENISA projects and activities (e.g. unit responsible for the project, relevant tender results, etc.) while maintaining and expanding as appropriate online resources available.

Additionally, guidelines provided by the Management Board on missions, objectives and functioning of the NLO network will guide the development of this important tool for ENISA 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 OECD, ICANN, IGF in so far as these groups are discussing items related to our work programme or strategy.

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

List of Outputs in work programme 2019

As explained in the introduction, this document covers two scenarios, depending on the adoption and publication of the Cybersecurity Act. To allow smooth transition to the new activities, this work programme covers both scenarios and activities are labelled accordingly.

Activities labelled as Scenario 1 are using the resources available in MFF 2014-2020 COM(2013)519, and are to be delivered independent of the adoption process of the Cybersecurity Act.

Activities labelled as Scenario 2 are only proposed to be delivered if the draft Cybersecurity Act is adopted and published and the resources proposed in the Draft General Budget of the European Union for the financial year 2019[46] are becoming available.

This section summarizes in "List of Outputs in work programme 2019", the Outputs for the two scenarios: First list covers the Scenario 1 Outputs, to be delivered independent of the adoption of the Cybersecurity Act, while second list includes the new Outputs to be delivered as soon as the Cybersecurity Act is published in the official Journal.

List of Outputs in work programme 2019, Scenario 1

Activity 1 - Expertise. Anticipate and support Europe in facing emerging network and information security challenges
Objective 1.1. Improving the expertise related to Network and Information security
Output O.1.1.1 - Good practices for security of Internet of Things (Scenario 1)
Output O.1.1.2 - Good practices for the security of Smart Cars (Scenario 1)
Output O.1.1.3 - Awareness raising on existing technical specifications for cryptographic algorithms (Scenario 1)
Objective 1.2. NIS Threat Landscape and Analysis
Output O.1.2.1 - Annual ENISA Threat Landscape (Scenario 1)
Output O.1.2.2 - Restricted and public Info notes on NIS (Scenario 1)
Output O.1.2.3 - Support incident reporting activities in the EU (Scenario 1)
Objective 1.3. Research & Development, Innovation
Output O.1.3.1 - Supporting cPPP in defining priorities for EU research & development (Scenario 1)
Objective 1.4. Response to Article 14 Requests under Expertise Activity
Output O.1.4.1 - Response to Requests under Expertise Activity (Scenario 1)
Activity 2 - Policy. Promote network and information security as an EU policy priority
Objective 2.1. Supporting EU policy development
Output O.2.1.1 - Support the preparatory policy discussions in the area of certification of products and services (Scenario 1)
Objective 2.2. Supporting EU policy implementation
Output O.2.2.1 - Recommendations supporting implementation of the eIDAS Regulation (Scenario 1)
Output O.2.2.2 - Supporting the Implementation of the Work Programme of the Cooperation Group under the NIS Directive (Scenario 1)
Output O.2.2.3 – Assist MS in the implementation of OES and DSPs baseline Security requirements(Scenario 1)
Output O.2.2.4 - Supporting the Payment Services Directive (PSD) implementation (Scenario 1)
Output O.2.2.5 - Contribute to the EU policy in the area of privacy and data protection with policy input on security measures (Scenario 1)
Output O.2.2.6 - Guidelines for the European standardisation in the field of ICT security (Scenario 1)
Output O.2.2.7 - Supporting the implementation of European Electronic Communications Code (Scenario 1)

[46] Draft General Budget of the European Union for the financial year 2019, available at: https://eur-lex.europa.eu/budget/data/DB/2019/en/SEC03.pdf , and COM(2018)600 of May 2018 with breakout for Agencies available at: http://ec.europa.eu/budget/library/biblio/documents/2019/WD%20III%20Agency_web.pdf
The budget contribution is subject to final adoption of the EU budget.

Objective 2.3. Response to Article 14 Requests under Policy Activity
Output O.2.3.1 - Response to Requests under Policy Activity (Scenario 1)
Activity 3 - Capacity. Support Europe maintaining state-of-the-art network and information security capacities
Objective 3.1. Assist Member States' capacity building
Output O.3.1.1 - Update and provide technical trainings for MS and EU bodies (Scenario 1)
Output O.3.1.2 - Support EU MS in the development and assessment of NCSS (Scenario 1)
Output O.3.1.3 - Support EU MS in their Incident Response Development (Scenario 1)
Objective 3.2. Support EU institutions' capacity building
Output O.3.2.1. Representation of ENISA on the Steering Board of CERT-EU and coordination with other EU Agencies using the CERT-EU service (Scenario 1)
Output O.3.2.2. Cooperation with relevant union bodies on initiatives covering NIS dimension related to their missions (Scenario 1)
Objective 3.3. Assist in improving private sector capacity building and general awareness
Output O.3.3.1 - European Cyber Security Challenges (Scenario 1)
Output O.3.3.2 - European Cyber Security Month deployment (Scenario 1)
Objective 3.4. Response to Article 14 Requests under Capacity Activity
Output O.3.4.1 - Response to Requests under Capacity Activity (Scenario 1)
Activity 4 - Community. Foster the emerging European network and information security community
Objective 4.1. Cyber crisis cooperation
Output O.4.1.1 - Planning of Cyber Europe 2020 and Cyber SOPEx (Scenario 1)
Output O.4.1.2 - Support activities for Cyber Exercises (Scenario 1)
Output O.4.1.3 - Support activities for Cyber Crisis Management (Scenario 1)
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 (Scenario 1)
Output O.4.2.2 - Support the fight against cybercrime and collaboration between CSIRTs and law enforcement (Scenario 1)
Output O.4.2.3 - Supporting the implementation and development of MeliCERTes platform (Scenario 1)
Objective 4.3. Response to Article 14 Requests under Community Activity
Output O.4.3.1 - Response to Requests under Community Building Activity (Scenario 1)

List of Outputs in work programme 2019 Scenario 2, when Cybersecurity Act enters into force

Activity 1 - Expertise. Anticipate and support Europe in facing emerging network and information security challenges
Objective 1.1. Improving the expertise related to Network and Information security
Output O.1.1.1 - Good practices for security of Internet of Things (Scenario 1)
Output O.1.1.2 - Good practices for the security of Smart Cars (Scenario 1)
Output O.1.1.3 - Awareness raising on existing technical specifications for cryptographic algorithms (Scenario 1)
Output O.1.1.4 - Good practices for the security of Healthcare services (Scenario 2)
Output O.1.1.5 - Good practices for the maritime security (ports security) (Scenario 2)
Objective 1.2. NIS Threat Landscape and Analysis
Output O.1.2.1 - Annual ENISA Threat Landscape (Scenario 1)
Output O.1.2.2 - Restricted and public Info notes on NIS (Scenario 1)
Output O.1.2.3 - Support incident reporting activities in the EU (Scenario 1)
Output O.1.2.4 - Regular technical reports on cybersecurity situation (Scenario 2)
Objective 1.3. Research & Development, Innovation
Output O.1.3.1 - Supporting cPPP in defining priorities for EU research & development (Scenario 1)
Objective 1.4. Response to Article 14 Requests under Expertise Activity
Output O.1.4.1 - Response to Requests under Expertise Activity (Scenario 1)

Activity 2 - Policy. Promote network and information security as an EU policy priority
Objective 2.1. Supporting EU policy development
Output O.2.1.1 - Support the preparatory policy discussions in the area of certification of products and services (Scenario 1)
Objective 2.2. Supporting EU policy implementation
Output O.2.2.1 - Recommendations supporting implementation of the eIDAS Regulation (Scenario 1)
Output O.2.2.2 - Supporting the Implementation of the Work Programme of the Cooperation Group under the NIS Directive (Scenario 1)
Output O.2.2.3 – Assist MS in the implementation of OES and DSPs baseline Security requirements(Scenario 1)
Output O.2.2.4 - Supporting the Payment Services Directive (PSD) implementation (Scenario 1)
Output O.2.2.5 - Contribute to the EU policy in the area of privacy and data protection with policy input on security measures (Scenario 1)
Output O.2.2.6 - Guidelines for the European standardisation in the field of ICT security (Scenario 1)
Output O.2.2.7 - Supporting the implementation of European Electronic Communications Code (Scenario 1)
Output O.2.2.8 - Supporting the sectorial implementation of the NIS Directive (Scenario 2)
Output O.2.2.9 - Hands on tasks in the area of certification of products and services (Scenario 2)
Objective 2.3. Response to Article 14 Requests under Policy Activity
Output O.2.3.1 - Response to Requests under Policy Activity (Scenario 1)
Activity 3 - Capacity. Support Europe maintaining state-of-the-art network and information security capacities
Objective 3.1. Assist Member States' capacity building
Output O.3.1.1 - Update and provide technical trainings for MS and EU bodies (Scenario 1)
Output O.3.1.2 - Support EU MS in the development and assessment of NCSS (Scenario 1)
Output O.3.1.3 - Support EU MS in their Incident Response Development (Scenario 1)
Output O.3.1.4 - Support EU MS in the development of ISACs for the NISD Sectors (Scenario 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 coordination with other EU Agencies using the CERT-EU service (Scenario 1)
Output O.3.2.2. Cooperation with relevant union bodies on initiatives covering NIS dimension related to their missions (Scenario 1)
Objective 3.3. Assist in improving private sector capacity building and general awareness
Output O.3.3.1 - European Cyber Security Challenges (Scenario 1)
Output O.3.3.2 - European Cyber Security Month deployment (Scenario 1)
Output O.3.3.3 - Support EU MS in cybersecurity skills development (Scenario 2)
Objective 3.4. Response to Article 14 Requests under Capacity Activity
Output O.3.4.1 - Response to Requests under Capacity Activity (Scenario 1)
Activity 4 - Community. Foster the emerging European network and information security community
Objective 4.1. Cyber crisis cooperation
Output O.4.1.1 - Planning of Cyber Europe 2020 and Cyber SOPEx (Scenario 1)
Output O.4.1.2 - Support activities for Cyber Exercises (Scenario 1)
Output O.4.1.3 - Support activities for Cyber Crisis Management (Scenario 1)
Output O.4.1.4 -Supporting the implementation of the Information hub (Scenario 2)
Output O.4.1.5 -Supporting the implementation of the Cyber Crisis collaboration blueprint (Scenario 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 (Scenario 1)
Output O.4.2.2 - Support the fight against cybercrime and collaboration between CSIRTs and and law enforcement (Scenario 1)
Output O.4.2.3 - Supporting the implementation and development of MeliCERTes platform (Scenario 1)
Objective 4.3. Response to Article 14 Requests under Community Activity
Output O.4.3.1 - Response to Requests under Community Building Activity (Scenario 1)

Annexes A

A.1 Annex I: Resource allocation per Activity 2019 – 2021

Sections A.1.1 and A.1.2 of this Annex presents the evolution of past and current situation as well as the outlook in a chart the distribution of resources proposed for 2019, while Section A.1.3 provides allocation per activities.

Overview of the past and current situation.

WP 2019 is following the COM guidelines and MB decisions. The Work Programme is structured following the objectives and the priorities of the Agency as described in the ENISA strategy.

Regarding ENISA's budget, the variations between the years 2017 and 2018 is neutral. The budget remained with the same amount aligned with COM communications.

In 2018, a slight increase in the title II was adopted. In 2019, the budget of Title III was optimized in order to increase the budget in operations.

As already presented, in the preparation of Work Programme 2019, ENISA is considering two scenarios. In detail, Scenario 1, uses the resources available in MFF 2014-2020 (COM(2013)519). Scenario 2, (which assumes new regulation in place by latest mid 2019), adds new tasks and activities as proposed in the Cybersecurity Act COM (2017)477, using resources planned in the Draft General Budget of the European Union for the financial year 2019[47]..

In case of the European Commission's proposal for ENISA's new mandate COM(2017) 477 Final, all Titles will be increased in order to deliver the proposals of the new mandate.

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

Resource programming for the years 2019-2021

The distribution of budget and resources for 2019 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. of this document.

Following the publication of the NIS Directive (NISD), the Agency is re-allocating budget and resources to the new tasks/activities provisioned for the Agency in the Directive. Another area which will probably require more budget / resources is the Cybersecurity Public Private partnership (cPPP). However, the

[47] Draft General Budget of the European Union for the financial year 2019, available at: https://eur-lex.europa.eu/budget/data/DB/2019/en/SEC03.pdf , and COM(2018)600 of May 2018 with breakout for Agencies available at:
http://ec.europa.eu/budget/library/biblio/documents/2019/WD%20III%20Agency_web.pdf
The budget contribution is subject to final adoption of the EU budget.

impact on the ENISA work programme has not yet been quantified. This will be updated in future versions as any other relevant change in the ENISA scope and tasks.

The Resources Department already optimised all its resources. Improvements in order to gain in effectiveness and efficiency were developed. ENISA perform an internal check in relevance and optimization of workflows, procedures and rules, to seek optimization 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 work-related documents and transactions represents a huge improvement and cost savings in all processes of the Agency.

Moreover, the Resources Department applies a strict policy on ratio between Administrative support and Coordination staff and Operational staff as methodology set by the European Commission and benchmarking exercise within the institutions and EU agencies. In 2017, only 20,24 % of Administrative support and Coordination staff were populating the Agency having in mid that the benchmarking of the EU commission accept level up to 25% of this group.

Job Type	2017	2016
Total Administrative support and Coordination	**20,24 %**	**19,04 %**
Administrative support	16.67 %	15.47 %
Coordination	3.57 %	3.57 %
Total Operational	**65.48 %**	**66.66 %**
Top operational coordination	7.14 %	7.14 %
General Operational	58.33 %	59.52 %
Total Neutral	**14.29 %**	**14.29 %**
Finance and Control	14.29 %	14.29 %

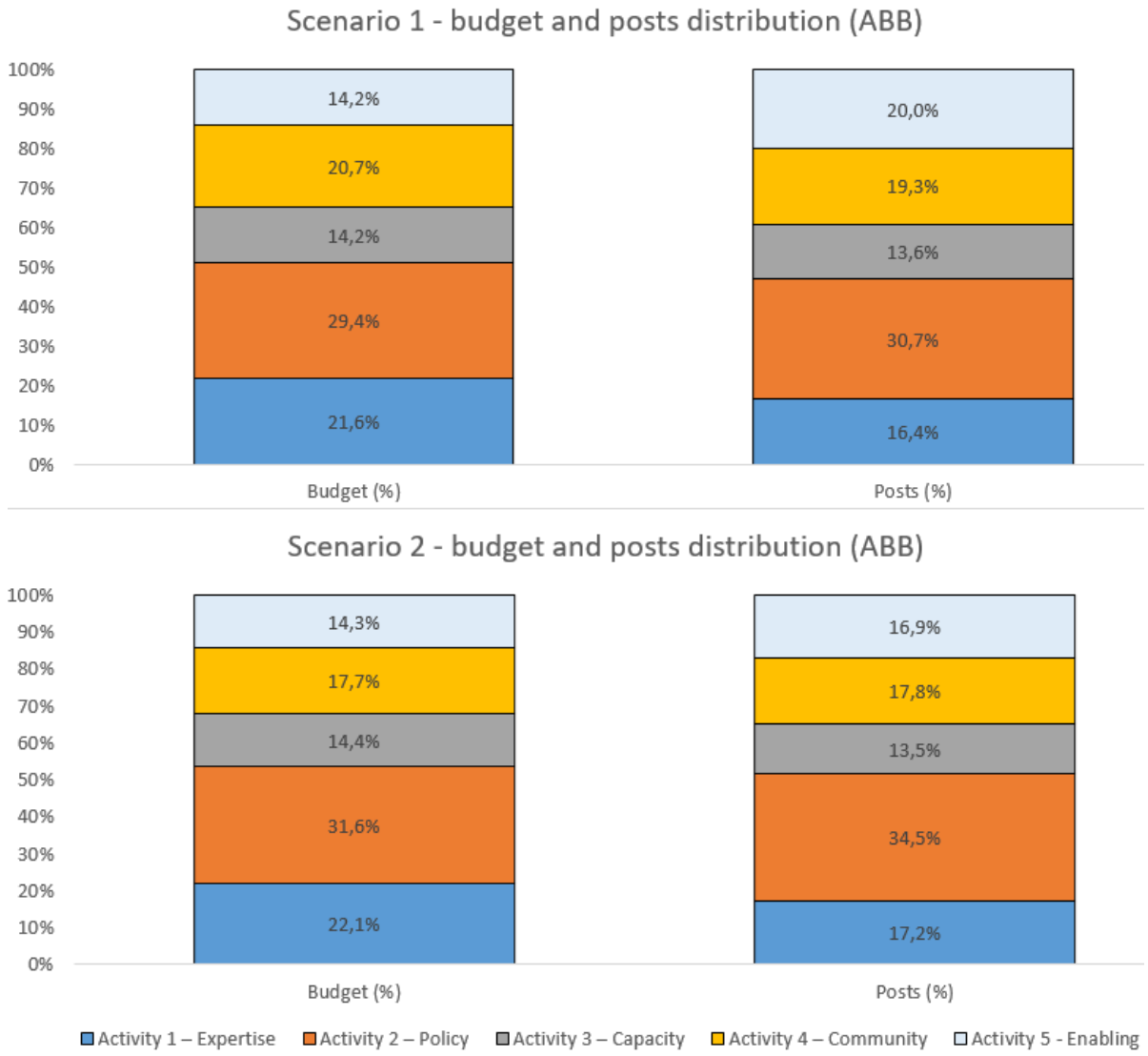
In addition, this version of the work programme takes account of the prioritisation exercise carried out during the consultation with the Management Board. Certain activities had to be removed from the work programme as there are not enough resources for the year 2018. Such de-prioritise activities are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

- Activities to support a Digital Single Market for high quality NIS products and services
- Support the assessment of existing policies/procedures/practices on NIS within EU institutions
- Planning and organisation of EuroSOPEx 2018.

For years 2019-2021, the Agency will gradually increase the share of the activity 2, Policy if more resources become available.

The budget and resources allocations within the summary tables and Annexes in **Scenario 1** are in line with the COM(2013)519. The budget and resources allocations within the summary tables and Annexes in **Scenario 2** are in line with the proposed additional resources and budget in the Draft General Budget of the European Union for the financial year 2019[48].

[48] Draft General Budget of the European Union for the financial year 2019, available at: https://eur-lex.europa.eu/budget/data/DB/2019/en/SEC03.pdf , and COM(2018)600 of May 2018 with breakout for Agencies available at:
http://ec.europa.eu/budget/library/biblio/documents/2019/WD%20III%20Agency_web.pdf
The budget contribution is subject to final adoption of the EU budget.



Overview of activities budget and resources

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

To improve better estimation of resources needed for each ENISA activity, we need to split the budget forecast in Direct and Indirect budget. The following assumptions are used in the simplified ABB methodology:

- **Direct** Budget is the cost estimate of each **Operational** activity (listed in Activities A1 to A5) in terms of goods and services procured.
- **Indirect** Budget is the cost estimate of salaries, mission costs and overhead costs, attributable to each **Operational or Compliance** activity. The indirect budget is re-distributed against direct budget in all Activities.

- **Compliance** posts from Activity A5 Enabling are redistributed to Core Activities - A1 to A4, and **operational** posts of the Activity A5.
- Total ABB posts (FTEs) are the sum of all the posts from all activities (A1 to A5) after the re-distribution.

The table below presents the allocation of financial and human resources to Activities of the Agency based on the above ABB methodology. Furthermore, as already explained:

- Scenario 1 is in line with the COM(2013)519,
- while Scenario 2 is in line with proposed additional resources and budget in the Draft General Budget of the European Union for the financial year 2019[49].

• **Scenario 1**	**Total ABB budget (€)**	**Total ABB posts (FTEs)**
Activity 1 - Expertise. Anticipate and support Europe in facing emerging network and information security challenges	2.509.254,13	13,58
Activity 2 - Policy. Promote network and information security an EU policy priority	3.421.710,18	25,50
Activity 3 - Capacity. Support Europe in maintaining state-of-the-art network and information security capacities	1.647.490,08	11,32
Activity 4 - Community. Foster the emerging European Network and Information Security Community	2.407.870,12	16,00
Activity 5 - Enabling. Reinforce ENISA's impact	1.652.559,29	16,60
Total	**11.638.883,80**	**83,00**

Scenario 2	**Total ABB budget (€)**	**Total ABB posts (FTEs)**
Activity 1 - Expertise. Anticipate and support Europe in facing emerging network and information security challenges	3.647.622,13	16,37
Activity 2 - Policy. Promote network and information security an EU policy priority	5.213.953,99	32,74
Activity 3 - Capacity. Support Europe in maintaining state-of-the-art network and information security capacities	2.381.682,69	12,86
Activity 4 - Community. Foster the emerging European Network and Information Security Community	2.918.097,70	16,95
Activity 5 - Enabling. Reinforce ENISA's impact	2.361.915,49	16,08
Total	16.523.272,00	**95,00**

[49] Draft General Budget of the European Union for the financial year 2019, available at: https://eur-lex.europa.eu/budget/data/DB/2019/en/SEC03.pdf , and COM(2018)600 of May 2018 with breakout for Agencies available at:
http://ec.europa.eu/budget/library/biblio/documents/2019/WD%20III%20Agency_web.pdf
The budget contribution is subject to final adoption of the EU budget.

A.2 Annex II: Human and Financial Resources 2019-2021

Expenditure overview.

Expenditure	2018		2019 Scenario 1		2019 Scenario 2		2020		2021	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1	6.386.500,00	6.386.500,00	7.133.782,80	7.133.782,80	9.477.948,32	9.477.948,32	12.038.000,00	12.038.000,00	13.343.500,00	13.343.500,00
Title 2	1.687.500,00	1.687.500,00	1.604.101,00	1.604.101,00	2.297.000,00	2.297.000,00	2.886.000,00	2.886.000,00	3.114.000,00	3.114.000,00
Title 3	3.354.126,00	3.354.126,00	2.901.000,00	2.901.000,00	4.748.323,68	4.748.323,68	6.851.310,20	6.851.310,20	6.957.777,60	6.957.777,60
Total expenditure	**11.428.126,00**	**11.428.126,00**	**11.638.883,80**	**11.638.883,80**	**16.523.272,00**	**16.523.272,00**	**21.775.310,20**	**21.775.310,20**	**23.415.277,60**	**23.415.277,60**

The tables below show the commitments and payment appropriations based on the same structure for the next years.

Commitment appropriations Scenario 1

EXPENDITURE	Executed Budget 2017 (31/12/17)	Budget 2018	Draft Budget 2019 (Scenario 1)		VAR 2019 / 2018	Envisaged in 2020	Envisaged in 2021
			Agency request	Budget Forecast	(Scenario 1)		
Title 1 : Staff Expenditure	**6.398.429**	**6.386.500**	**7.133.783**	**7.133.783**	**12%**	**12.038.000**	**13.343.500**
11 Staff in active employment	**4.674.964**	**5.186.400**	**6.093.783**	**6.093.783**	**17%**	**10.181.000**	**11.295.000**
- of which establishment plan posts							
- of which external personnel							
12 Recruitment expenditure	**175.432**	**261.100**	***365.000***	***365.000***	**40%**	**445.000**	**342.000**
13 Socio-medical services and training	**169.989**	**190.000**	**65.000**	**65.000**	**-66%**	**250.000**	**305.000**
14 Temporary assistance	**1.378.044**	**749.000**	**610.000**	**610.000**	**-19%**	**1.162.000**	**1.401.500**
Title 2: Building, equipment and miscellaneous expenditure	**1.600.312**	**1.687.500**	**1.604.101**	**1.604.101**	**-5%**	**2.886.000**	**3.114.000**
20 Building and associated costs	**868.135**	**1.000.500**	**923.000**	**923.000**	**-8%**	**1.180.000**	**1.234.000**
21 Movable property and associated costs	**25.435**	**60.000**	**32.000**	**32.000**	**-47%**	**99.000**	**99.000**
22 Current administrative expenditure	**83.027**	**62.000**	**75.500**	**75.500**	**22%**	**176.000**	**201.000**
23 ICT	**623.715**	**565.000**	**573.601**	**573.601**	**2%**	**1.431.000**	**1.580.000**
Title 3 : Operational expenditure	**3.176.484**	**3.375.000**	**2.901.000**	**2.901.000**	**-14%**	**6.851.310**	**6.957.778**
30 Activities related to meetings and missions	**943.055**	**715.000**	**716.000**	**716.000**	**0%**	**1.410.000**	**1.410.000**
32 Horizontal operational activities	**569.390**	**660.000**	**215.000**	**215.000**	**-67%**	**998.310**	**1.048.778**
36 Core operational activities	**1.664.038**	**1.979.126**	**1.970.000**	**1.970.000**	**0%**	**4.443.000**	**4.499.000**
TOTAL EXPENDITURE	**11.175.225**	**11.428.126,00**	**11.638.884**	**11.638.884**	**2%**	**21.775.310**	**23.415.278**

Payments appropriations Scenario 1

EXPENDITURE	Payments appropriations						
	Executed Budget 2017 (31/12/17)	Budget 2018	Draft Budget 2019 (Scenario 1)		VAR 2019 / 2018 (Scenario 1)	Envisaged in 2020	Envisaged in 2021
			Agency request	Budget Forecast			
Title 1 : Staff Expenditure	**6.398.429**	**6.386.500**	**7.133.783**	**7.133.783**	**12%**	**12.038.000**	**13.343.500**
11 Staff in active employment	4.674.964	5.186.400	6.093.783	6.093.783	**17%**	**10.181.000**	**11.295.000**
- of which establishment plan posts							
- of which external personnel							
12 Recruitment expenditure	175.432	261.100	***365.000***	***365.000***	**40%**	**445.000**	**342.000**
13 Socio-medical services and training	169.989	190.000	**65.000**	**65.000**	**-66%**	**250.000**	**305.000**
14 Temporary assistance	1.378.044	749.000	**610.000**	**610.000**	**-19%**	**1.162.000**	**1.401.500**
Title 2: Building, equipment and miscellaneous expenditure	**1.600.312**	**1.687.500**	**1.604.101**	**1.604.101**	**-5%**	**2.886.000**	**3.114.000**
20 Building and associated costs	868.135	1.000.500	**923.000**	**923.000**	**-8%**	**1.180.000**	**1.234.000**
21 Movable property and associated costs	25.435	60.000	**32.000**	**32.000**	**-47%**	**99.000**	**99.000**
22 Current administrative expenditure	83.027	62.000	**75.500**	**75.500**	**22%**	**176.000**	**201.000**
23 ICT	623.715	565.000	**573.601**	**573.601**	**2%**	**1.431.000**	**1.580.000**
Title 3 : Operational expenditure	**3.176.484**	**3.375.000**	**2.901.000**	**2.901.000**	**-14%**	**6.851.310**	**6.957.778**
30 Activities related to meetings and missions	943.055	715.000	**716.000**	**716.000**	**0%**	**1.410.000**	**1.410.000**
32 Horizontal operational activities	569.390	660.000	**215.000**	**215.000**	**-67%**	**998.310**	**1.048.778**
36 Core operational activities	1.664.038	1.979.126	**1.970.000**	**1.970.000**	**0%**	**4.443.000**	**4.499.000**
TOTAL EXPENDITURE	**11.175.225**	11.428.126	**11.638.884**	**11.638.884**	**2%**	**21.775.310**	**23.415.278**

Table 2.a – Revenue Overview Scenario 1

Revenues	2017	2018	2019 (Scenario 1)	2020	2021
	Revenues estimated by the agency including Amending Budget	Revenues estimated by the agency	Revenues estimated by the agency	Revenues estimated by the agency	Revenues estimated by the agency
EU contribution	10.322.000	10.529.000	10.739.000	20.646.000	22.480.000
Other revenue	853.225	899.126	899.884	1.129.310	1.167.278
Total revenues	**11.175.225**	**11.428.126**	**11.638.884**	**21.775.310**	**23.415.278**

REVENUES	2017	2018	2019 (Scenario 1)	VAR 2019 /2018	Envisaged 2020	Envisaged 2021
	Executed Budget	Revenues estimated by the agency	As requested by the agency			
1 REVENUE FROM FEES AND CHARGES						
2. EU CONTRIBUTION	**10.322.000**	**10.529.000**	**10.739.000**	**2%**	**20.646.000**	**22.248.000**
of which Administrative (Title 1 and Title 2)						
of which Operational (Title 3)						
of which assigned revenues deriving from previous years' surpluses						
3 THIRD COUNTRIES CONTRIBUTION (incl. EFTA and candidate countries)	**252.977**	**248.626**	**259.884**	**5%**	**489.310**	**527.278**
of which EFTA	252.977	248.626	259.884	**5%**	**489.310**	527.278
of which Candidate Countries						
4 OTHER CONTRIBUTIONS	**566.261**	**640.000**	**640.000**	**0%**	**640.000**	**640.000**
of which delegation agreement, ad hoc grants						
5 ADMINISTRATIVE OPERATIONS	**33.986**	**10.500**	**0**		**0**	**0**
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT						
7 CORRECTION OF BUDGETARY IMBALANCES						
TOTAL REVENUES	**11.175.225**	**11.428.126,00**	**11.638.884**	**2%**	**21.775.310**	**23.415.278**

Commitment appropriations Scenario 2

EXPENDITURE	Commitment appropriations					
	Executed Budget 2017 (31/12/17)	Budget 2018	Envisaged in 2019 (Scenario 2)	VAR 2019 / 2018	Envisaged in 2020	Envisaged in 2021
Title 1 : Staff Expenditure	6.398.429	6.386.500	9.477.948,32	33%	12.038.000	13.343.500
11 Staff in active employment	4.674.964	5.186.400	6.794.000,00	14%	10.181.000	11.295.000
- of which establishment plan posts						
- of which external personnel						
12 Recruitment expenditure	175.432	261.100	971.948,32	166%	445.000	342.000
13 Socio-medical services and training	169.989	190.000	325.000,00	400%	250.000	305.000
14 Temporary assistance	1.378.044	749.000	1.387.000,00	93%	1.162.000	1.401.500
Title 2: Building, equipment and miscellaneous expenditure	1.600.312	1.687.500	2.297.000,00	43%	2.886.000	3.114.000
20 Building and associated costs	868.135	1.000.500	1.100.000,00	19%	1.180.000	1.234.000
21 Movable property and associated costs	25.435	60.000	58.000,00	81%	99.000	99.000
22 Current administrative expenditure	83.027	62.000	104.000,00	38%	176.000	201.000
23 ICT	623.715	565.000	1.035.000,00	80%	1.431.000	1.580.000
Title 3: Operational expenditure	3.176.484	3.375.000	4.748.323,68	64%	6.851.310	6.957.778
30 Activities related to meetings and missions	943.055	715.000	1.043.323,68	46%	1.410.000	1.410.000
32 Horizontal operational activities	569.390	660.000	405.000,00	88%	998.310	1.048.778
36 Core operational activities	1.664.038	1.979.126	3.300.000,00	68%	4.443.000	4.499.000
TOTAL EXPENDITURE	11.175.225	11.428.126	16.523.272,00	42%	21.775.310	23.415.278

Payments appropriations Scenario 2

EXPENDITURE	Payment appropriations					
	Executed Budget 2017 (31/12/17)	Budget 2018	Envisaged in 2019 (Scenario 2)	VAR 2019 / 2018 (Scenario 2)	Envisaged in 2020	Envisaged in 2021
Title 1 : Staff Expenditure	6.398.429	6.386.500	9.477.948,32	48%	12.038.000	13.343.500
11 Staff in active employment	4.674.964	5.186.400	6.794.000,00	14%	10.181.000	11.295.000
- of which establishment plan posts						
- of which external personnel						
12 Recruitment expenditure	175.432	261.100	971.948,32	272%	445.000	342.000
13 Socio-medical services and training	169.989	190.000	325.000,00	71%	250.000	305.000
14 Temporary assistance	1.378.044	749.000	1.387.000,00	93%	1.162.000	1.401.500
Title 2: Building, equipment and miscellaneous expenditure	1.600.312	1.687.500	2.297.000	36%	2.886.000	3.114.000
20 Building and associated costs	868.135	1.000.500	1.100.000	10%	1.180.000	1.234.000
21 Movable property and associated costs	25.435	60.000	58.000	-3%	99.000	99.000
22 Current administrative expenditure	83.027	62.000	104.000	68%	176.000	201.000
23 ICT	623.715	565.000	1.035.000	83%	1.431.000	1.580.000
Title 3: Operational expenditure	3.176.484	3.375.000	4.748.323,68	42%	6.851.310	6.957.778
30 Activities related to meetings and missions	943.055	715.000	1.043.323,68	46%	1.410.000	1.410.000
32 Horizontal operational activities	569.390	660.000	405.000,00	-39%	998.310	1.048.778
36 Core operational activities	1.664.038	1.979.126	3.300.000,00	67%	4.443.000	4.499.000
TOTAL EXPENDITURE	11.175.225	11.428.126	16.523.272,00	44%	21.775.310	23.415.278

Table 2.b – Revenue Overview Scenario 2

Revenues	2017	2018	2019 (Scenario 2)	2020	2021
	Revenues estimated by the agency including Amending Budget	Revenues estimated by the agency	Revenues estimated by the agency	Revenues estimated by the agency	Revenues estimated by the agency
EU contribution	10.322.000	10.529.000	15.510.000,00	20.646.000	22.480.000
Other revenue	853.225	899.126	1.013.272,00	1.129.310	1.167.278
Total revenues	**11.175.225**	**11.428.126**	**16.523.272,00**	**21.775.310**	**23.415.278**

REVENUES	2017	2018	2019 (Scenario 2)	VAR 2019 /2018	Envisaged 2020	Envisaged 2021
	Executed Budget	Revenues estimated by the agency	As requested by the agency			
1 REVENUE FROM FEES AND CHARGES						
2. EU CONTRIBUTION	10.322.000	10.529.000	15.510.000,00	47%	20.646.000	22.248.000
of which Administrative (Title 1 and Title 2)						
of which Operational (Title 3)						
of which assigned revenues deriving from previous years' surpluses						
3 THIRD COUNTRIES CONTRIBUTION (incl. EFTA and candidate countries)	252.977	248.626	373.272,00	50%	489.310	527.278
of which EFTA	252.977	248.626	373.272,00	50%	489.310	527.278
of which Candidate Countries						
4 OTHER CONTRIBUTIONS	566.261	640.000	640.000,00	0%	640.000	640.000
of which delegation agreement, ad hoc grants						
5 ADMINISTRATIVE OPERATIONS	33.986	10.500	-		0	0
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT						
7 CORRECTION OF BUDGETARY IMBALANCES						
TOTAL REVENUES	11.175.225	11.428.126,00	16.523.272,00	45%	21.775.310	23.415.278

Table 3 – Budget outturn and cancellation of appropriations. Calculation of budget outturn

Budget Outturn	2015	2016	2017
Revenue actually received (+)	10.069.280	11.034.366	11.223.387
Payments made C1 (-)	9.395.559	9.860.775	9.901.545
Carry-over of appropriation (-)	674.521	1.176.717	1.376.731
Cancellation of appropriations carried over (+)	80.675	38.616	90.916
Adjustment for carry over of assigned revenue appropriations from previous year (+)	800	3.127	49.519
Exchange rate differences (+/-)	278	-180	-12
Adjustment for negative balance from previous year (-)			
TOTAL	**80.397**	**38.436**	**85.535**

Cancellation of appropriations

- Cancellation of Commitment Appropriations

  No commitment appropriations were cancelled.

  In 2017, ENISA demonstrates a commitment rate of 99,99 %, of C1 appropriation of the year at the year-end (31/12. The consumption of the 2017 Budget at year-end shows the capacity of the Agency to fully implement its annual appropriations. The same commitment rate achieved in 2010, 2011, 2012, 2013, 2014, 2015, 2016 and 2017, is maintained for an eight year in a row. The payment rate reached 88,19 % and the amount carried forward to 2018 is 1.411.440,51 EUR, representing 13,30 % of total C1 appropriations 2017.

- 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 2016 to 2017.)

  The appropriations of 2016 carried over to 2017 were utilised at a rate of 90,61 % (automatic carry-overs) which indicates a satisfactory capability of estimation of needs. From the amount of EUR 968 198,32 carried forward, the amount of EUR 90 916,34 was cancelled, due to the fact that the estimated expenditure deviated from the actual paid amount. This cancellation represent 0,87 % of the total budget.

A.3 Annex III: Human Resources – Quantitative

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

Staff population		Authorised under EU budget 2016	Actually filled as of 31 12.2016	Authorised under EU budget for year 2017	Actually filled as of 31.12.2017	In draft budget for year 2018	Envisaged in 2019 Scenario 1	Envisaged in 2019 Scenario 2	Envisaged in 2020	Envisaged in 2021
Officials	AD									
	AST									
	AST/SC									
TA	AD	34	28	34	29	34	34	43	51	57
	AST	14	15	14	13	13	13	16	18	19
	AST/SC									
Total		**48**	**43**	**48**	**42**	**47**	**47**	**59**	**69**	**76**
CA GFIV		16	12	28	17	28	28	28	28	28
CA GF III		15	12	2	11	5	2	2	2	2
CA GF II		1	0	0	0	0	0	0	0	0
CA GFI		1	1	0	1	0	0	0	0	0
Total CA		**33**	**25**	**30**	**29**	**33**	**30**	**30**	**33**	**33**
SNE		**3**	**1**	**6**	**3**	**3**	**6**	**9**	**12**	**12**
Structural service providers										
TOTAL		**84**	**69**	**84**	**74**	**83**	**83**	**98**	**114**	**121**
External staff for occasional replacement						5	5	5	5	5

Note: For 2017 Extra 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 – Multi-annual staff policy plan year 2019 – 2021

Category and grade	Establishment plan in EU Budget 2017		Filled as of 31/12/2017		Modifications in year 2018 in application of flexibility rule		Establishment plan in voted EU Budget 2018		Modifications in year 2018 in application of flexibility rule		Establishment plan 2019 (scenario 1)		Establishment plan 2019 (scenario 2)	Establishment plan 2020		Establishment plan 2021	
	Off.	TA	Off.	TA	Off.	TA	Off.	TA	Off.	TA	Off.	TA	TA	Off.	TA	Off.	TA
AD 16																	
AD 15		1		1				1				1	1		1		1
AD 14																	
AD 13																	
AD 12		3		3				3				3	6		6		6
AD 11																	
AD 10		5		2				5				5	5		5		5
AD 9		10		3				10				10	12		12		12
AD 8		15		8				15				15	19		21		21
AD 7				1											3		6
AD 6				10											3		6
AD 5				1													
Total AD	**0**	**34**		**29**				**34**				**34**	**43**		**51**		**57**
AST 11																	
AST 10																	
AST 9																	
AST 8																	
AST 7		2		1				2				2	3		4		5
AST 6		5		1				5				5	7		8		8
AST 5		5		2				5				5	5		5		5
AST 4		2		5				1				1	1		1		1
AST 3				4													
AST 2																	
AST 1																	
Total AST	**0**	**14**		**13**				**13**				**13**	**16**		**18**		**19**
AST/SC1																	
AST/SC2																	
AST/SC3																	
AST/SC4																	
AST/SC5																	
AST/SC6																	
Total AST/SC																	
TOTAL		**48**		**42**				**47**				**47**	**59**		**69**		**76**

Note: 1 AST post has been planned for the 5% staff cut in 2018.

A.4 Annex IV: Human Resources - Qualitative

A. Recruitment policy

Statutory Staff

The Agency continues to enhance the management of selection procedure with a focus on improving time to hire, developing good practices in recruitment (e.g. Conflict of Interest assessment for candidates being recruited in line with Articles 11 and 11a of the SR/Art. 11 and 81 of CEAOS) and streamlining processes. The acquisition of a modern e-recruitment tool from another EU Agency would definitively help.

The Agency is also investing in the development of an HR strategic approach focusing on competency-based interview's questions, tailor-made training for Selection Board Members, alignment of competencies across the organisation per job profile, targeted recruitment procedures for specialised profiles, transversal recruitment procedures where reserve lists could be used for filling vacant positions across all Departments/Units, specific dissemination of ENISA's job vacancies, etc.

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-AD10, 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 five 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 (two years, renewable once for a maximum one year) to be allocated depending on business needs or any other human resources constraints (a.i. 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 six months to a maximum of four 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 six months to a maximum of twelve months.

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

B. Appraisal of performance and reclassification/promotions

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

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

Table 1 - Reclassification of temporary staff/promotion of officials

Category and grade	Staff in activity at 1.01.Year 2016		How many staff members were promoted / reclassified in Year 2017		Average number of years in grade of reclassified/ promoted staff members
	officials	TA	officials	TA	
AD 16					
AD 15		1			
AD 14					
AD 13					
AD 12		3			
AD 11					
AD 10		3			
AD 9		4			
AD 8		4			
AD 7		2			
AD 6		12		1	3
AD 5		1			
Total AD					
AST 11					
AST 10					
AST 9					
AST 8					
AST 7		1			
AST 6		1			
AST 5		2			
AST 4		5		1	8
AST 3		6		1	2
AST 2					
AST 1					
Total AST					
AST/SC1					
AST/SC2					
AST/SC3					
AST/SC4					
AST/SC5					
AST/SC6					
Total AST/SC					
Total		**45**			

Table 2 - Reclassification of contract staff

Function Group	Grade	Staff in activity at 1.01.Year 2016	How many staff members were reclassified in Year 2017	Average number of years in grade of reclassified staff members
CA IV	14	3		
	13	6	1	2
CA III	10	1		
	9	5	1	5
	8	5		
CA II	6	1		
CA I	2	1		
Total		**22**		

C. 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 while in 2017, one mobility was organised.

D. Learning and Development

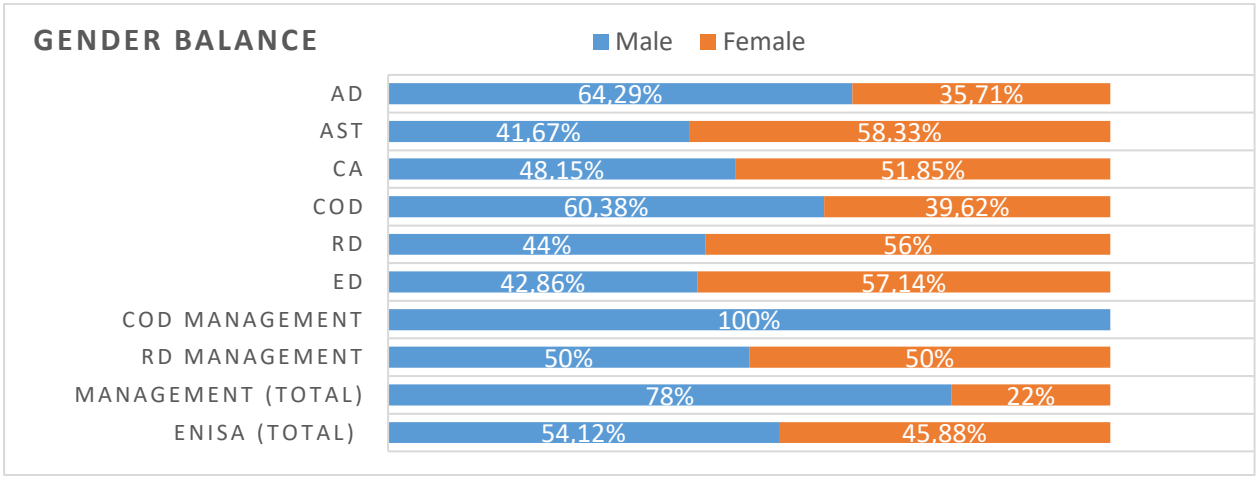
The Agency is striving for excellence in the approach to developing staff. In order to make the most out of its internal expertise and to develop mechanisms to retain staff, the organisation is focusing on offering a wide range of Learning and Development Opportunities including mandatory trainings (e.g. Ethics and Integrity, harassment prevention, etc.), various workshops and Team Building events, on-line courses, access to EU-Learn, etc.

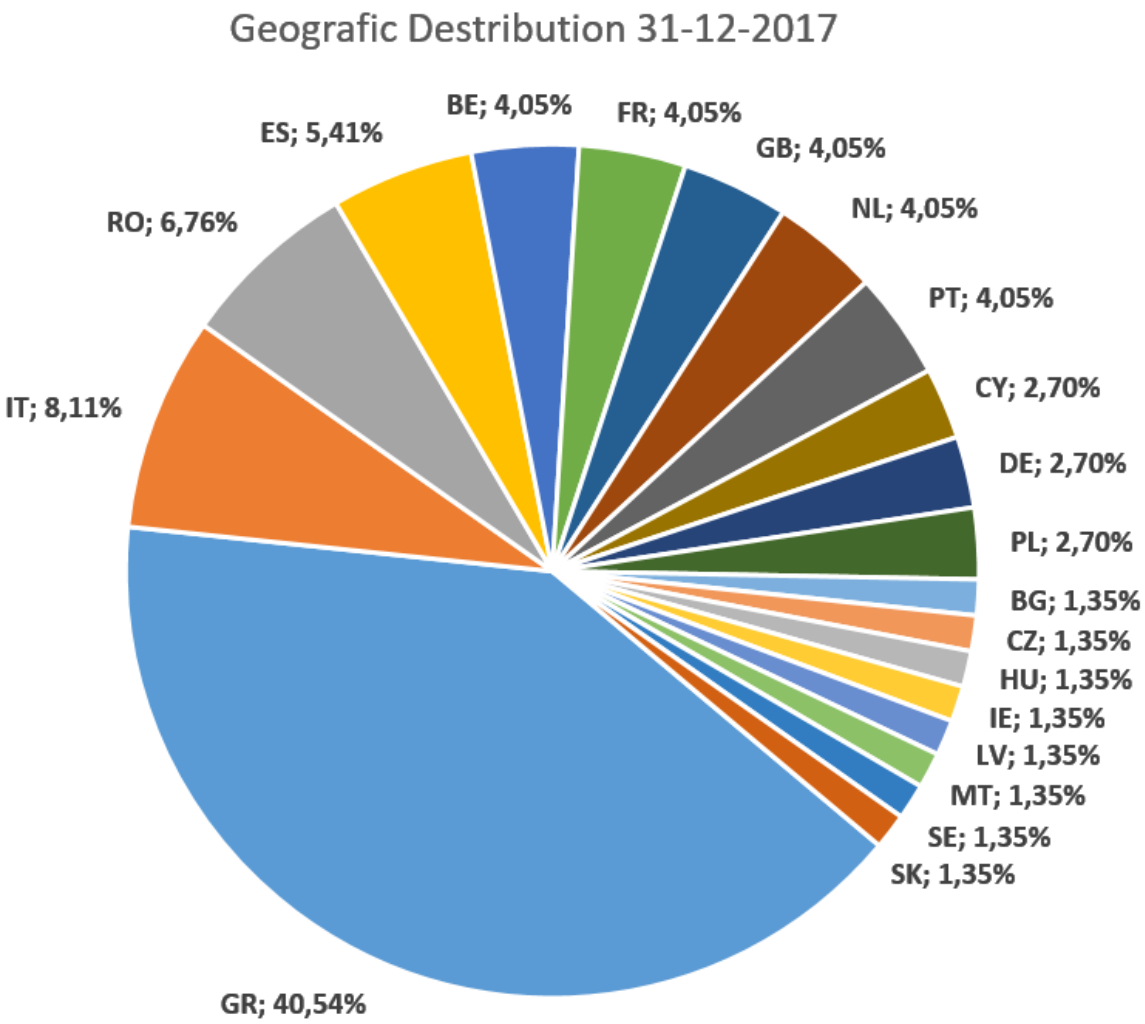
E. Gender and geographical balance

As of 31/12/2017 ENISA counts with 74 Staff members (42 TA's from which 29 AD's and 13 AST's), 29 CA's and 3 SNE's.

The overall gender balance among ENISA staff shows a male prevalence that 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. In line with the European Commission's objective to achieve 40% female representation in managerial positions, the Agency nominated in 2016 and 2017 a French woman as Head of HR and a Swedish woman as Head of Finances and Procurement.

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. The overall gender balance per grade and per operational unit can be find below:





F. Schooling

A European School is located in Heraklion and is used by Staff members of ENISA. For school year 2017-2018 2 pupils attended primary and 3 pupils attended 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 2017-2018, 20 pupils attended nursery and kindergarten and 19 pupils attended 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.

A.5 Annex V: Buildings

ENISA is currently negotiating a reduction in space rented in Heraklion and an increase in the space rented in Athens. It is expected that the relevant contracts will be negotiated and concluded in order to accommodate all ENISA staff in a suitable work environment.

A.6 Annex VI: Privileges and immunities

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

A.7 Annex VII: Evaluations

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

Also, external consultant has been contracted to carry annual ex post evaluation of core operational activities. The scope of the evaluation focusses on ENISA's core operational activities, with an estimated expenditure above 30.000 EUR. The overall objective of the annual evaluations is to evaluate the effectiveness, efficiency, added value, utility, coordination and coherence.

A.8 Annex VIII: Risks Year 2019

The Self Risk Assessment was performed by the Internal Audit Service in 2016. Three areas were proposed for the three next years: Stakeholders' Involvement in the Production of Deliverables in ENISA (done in 2017), Human Resources (2018), Information and Communication Technology (2019).

A.9 Annex IX: Procurement plan Year 2019

2019 WP Procurement Planning — Preliminary budget breakdown	Direct budget (in EUR) Scenario 1	Direct budget (in EUR) Scenario 2	Procurement (tender) procedure required	Launch Dates	All other expenditure
Activity 1 — Expertise. Anticipate and support Europe in facing emerging network and information security challenges	557.500,00	937.500,00	TBA	Q1-Q4	TBA
Activity 2 — Policy. Make network and information security an EU policy priority	621.500,00	1.441.500,00	TBA	Q1-Q4	TBA
Activity 3 — Capacity. Support Europe in setting up state-of-the-art network and information security capacities	325.000,00	600.000,00	TBA	Q1-Q4	TBA
Activity 4 — Community. Make the European network and information security community a reality	496.000,00	521.000,00	TBA	Q1-Q4	TBA
Activity 5 — Enabling. Reinforce ENISA's impact					
Objective 5.1. Management and Compliance	116.000,00	195.285,17	TBA	Q1-Q4	TBA
Objective 5.2. Engagement with stakeholders and International relations	210.000,00	355.000,00	TBA	Q1-Q4	TBA
Total A1-A5	**2.326.000,00**	**4.050.285,17**			

2019 WP Procurement Planning	Direct budget (in EUR) (Scenario 1)	Direct budget (in EUR) (Scenario 2)	Procurement (tender) procedure required Scenario 1	Procurement (tender) procedure required Scenario 2	Launch Dates	All other expenditure (Scenario 1)	All other expenditure (Scenario 2)
Activity 1 - Expertise. Anticipate and support Europe in facing emerging network and information security challenges	495.000,00	850.000,00	315.000	570.000	Q1-Q4	180.000,00	280.000,00
Activity 2 - Policy. Promote network and information security an EU policy priority	675.000,00	1.215.000,00	220.000	510.000	Q1-Q4	455.000,00	705.000,00
Activity 3 - Capacity. Support Europe in maintaining state-of-the-art network and information security capacities	325.000,00	555.000,00	230.000	380.000	Q1-Q4	95.000,00	175.000,00
Activity 4 - Community. Foster the emerging European Network and Information Security Community	475.000,00	680.000,00	250.000	390.000	Q1-Q4	225.000,00	290.000,00
Activity 5 - Enabling. Reinforce ENISA's impact	326.000,00	550.393,68	229.000	441.000	Q1-Q4	97.000,00	109.393,68
Total A1-A5	**2.296.000,00**	**3.850.393,68**	**1.244.000,00**	**2.291.000,00**	Q1-Q4	**1.052.000,00**	**1.559.393,68**

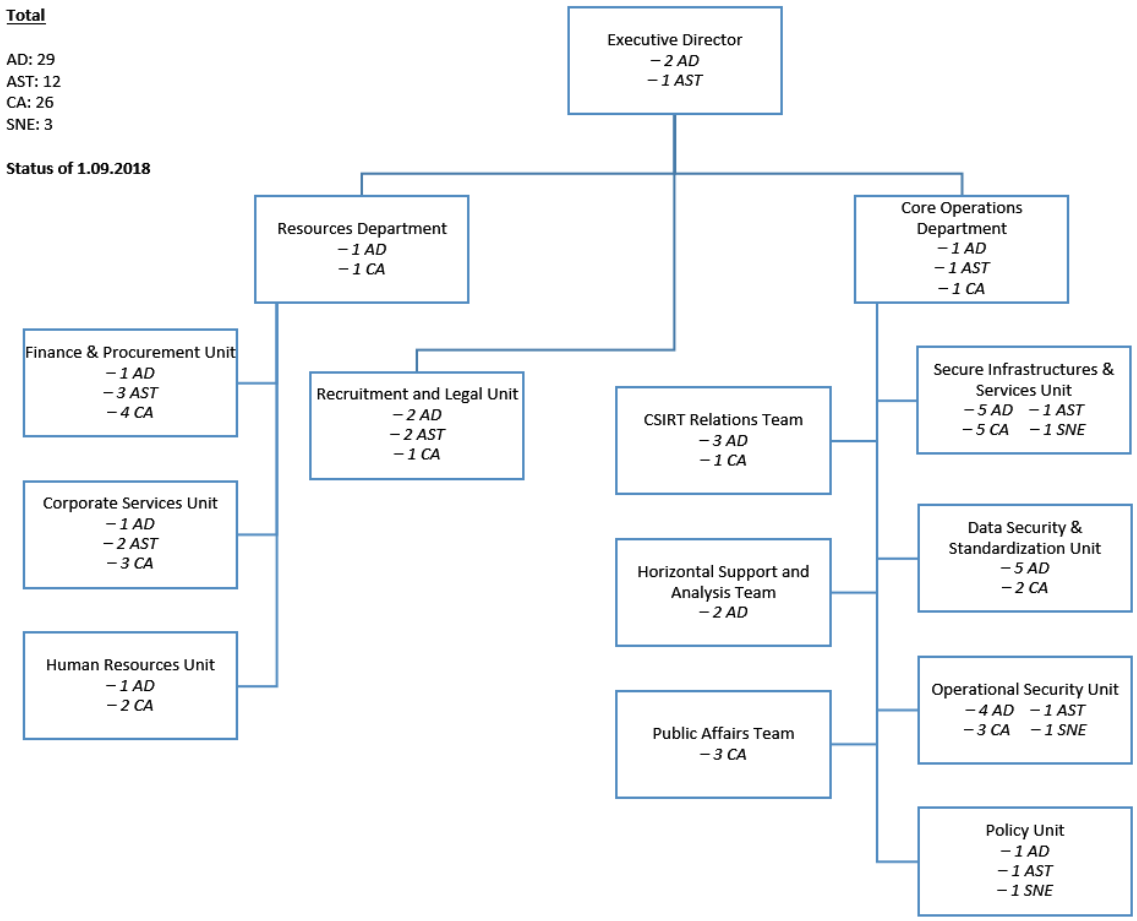
A.10 Annex X: ENISA Organisation

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

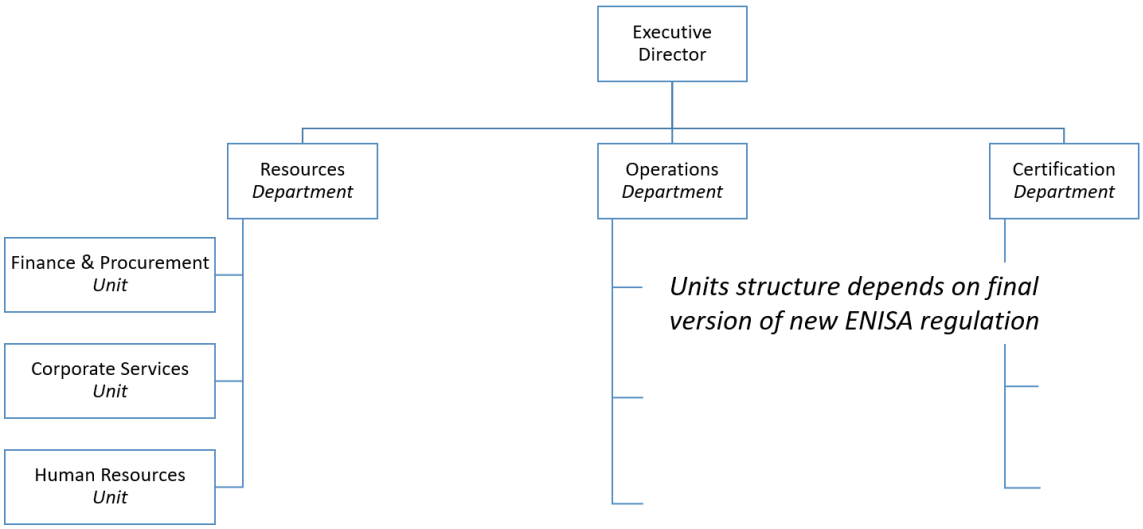
- A Management Board**:** The Management Board is ensuring that the Agency carries out its tasks under conditions which enables it to serve in accordance with the founding Regulation.
- An Executive Board**:** The Executive Board is preparing decisions to be adopted by the Management Board on administrative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

ENISA's organization for Scenario 1 is presented below in detail, while for Scenario 2 the structure of the departments is still to be detailed on the final outcome of the proposed ENISA regulation.

Scenario 1.



Scenario 2.

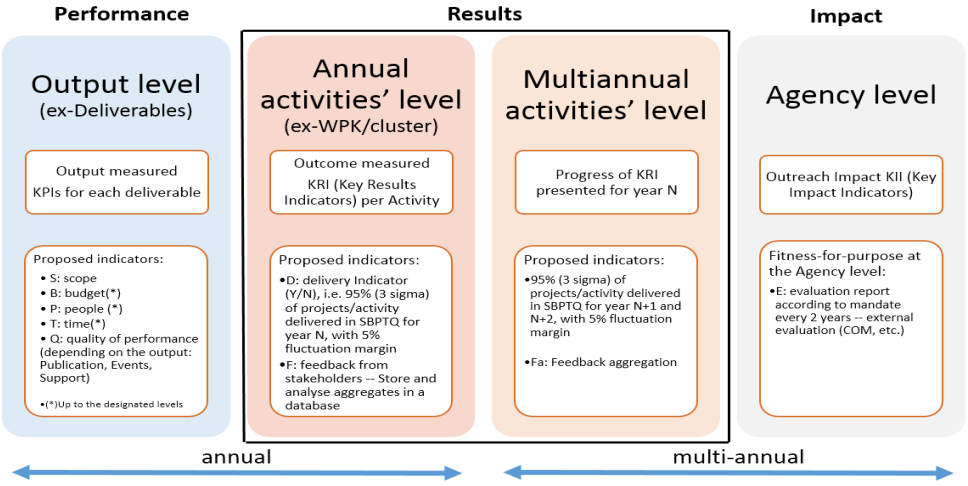


Annex B: Summarizing the Key Indicators for the multi-annual activities

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

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

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



Key indicators at ENISA seek to measure:

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

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

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

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

a. Delivery indicator aiming at delivery of at least 95% against work program planning. This is equivalent to a 3σ (3 Sigma) organisation (reaching between 93.3% and 99,3%); clearly the Agency has historically proven its operational ability to deliver at much higher level, meeting 6σ (6 Sigma) specification requirements (at 99,99%). However allowing for a 3 Sigma level meets the above-mentioned deviation rate of ±5%.[50] The criteria used, being scope, budget, people, time and quality, they all refer to the proper execution of the project leading up to the production of output. This evaluation is done at the end of the project within ENISA.

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

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

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

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

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

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

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

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

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

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

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

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

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

Annex C: List of Acronyms

ABB: Activity Based Budgeting
APF: Annual Privacy Forum
BEREC: Body of European Regulators of Electronic Communications
cPPP: Cyber Security Public-Private Partnership
CE2016: Cyber Europe 2016
CEF: Connecting Europe Facility
CEP: Cyber Exercises Platform
CERT-EU: Computer Emergency Response Team for the EU Institutions, Bodies and Agencies
CEN: European Committee for Standardization
CENELEC: European Committee for Electrotechnical Standardization
CIIP: Critical Information Infrastructure Protection
CSCG: ETSI CEN-CENELEC Cyber Security Coordination Group
CSIRT: Computer Security Incidents Response Teams
CSSU: Corporate Stakeholders and Services Unit
COD: Core Operational Department
COM: European Commission
CSS: Cyber Security Strategy
CNW: CSIRTs Network
DG: EC Directorate-General
DG CONNECT: EC Directorate-General CONNECT
DPA: Data Protection Authorities
DPO: Data Protection Officer
DSM: Digital Single Market
E: Event, type of output i.e. conference, workshop, and seminar
EB: ENISA Executive Board
EC3: European Cybercrime Centre, Europol
ECA: European Court of Auditors
ECSM: European Cyber Security Month
ECSO: European Cyber Security Organisation
ED: Executive Director
EDO: Executive Directors Office
EDPS: European Data Protection Supervisor
eID: electronic Identity
eIDAS: Regulation on electronic identification and trusted services for electronic transactions in the internal market
ETSI: European Telecommunications Standards Institute
EU: European Union
FAP: Finance, Accounting and Procurement
FIRST: Forum of Incident Response and Security Teams
FM: Facilities Management
FTE: Full Time Equivalents
KGI: Key Goal Indicator
H2020: Horizon 2020
HoD: Head of Department
HR: Human Resources
IAS: Internal Audit Service
ICC & IAC: Internal Control Coordination and Internal Audit Capability
ICS/SCADA: Industrial Control Systems/Supervisory Control and Data Acquisition
ICT: Information and Communication Technologies
IS: Information Systems
ISP: Internet Service Providers
IXP: Internet exchange point
KII: Key Impact Indicator
KPI: Key Performance Indicator
LEA: Law Enforcement Agency
MFF: Multi Annual Financial framework
M2M: Machine to Machine
MB: Management Board
MS: Member State
NAPAC: National Public Authority Representatives Committee
NCSS: National Cyber Security Strategies
NIS: Network and Information Security
NISD: NIS Directive
NLO: National Liaison Officer
NRA: National Regulatory Authority
O: Output
OES: Operators of Essential Services
P: Publication, type of output covering papers, reports, studies
PDCA: Plan-Do-Check-Act
PETs: Privacy Enhancing Technologies
PPP: Public Private Partnership
PSG: Permanent Stakeholders Group
Q: Quarter
QMS: Quality Management System
R&D: Research and Development
S: Support activity, type of output
SB: Supervisory Body
SCADA: Supervisory Control and Data Acquisition
SDO: Standard Developing Organization
SME: Small and Medium Enterprise
SO: Strategic Objectives
SOP: Standard Operating Procedure
SRAD: Stakeholder Relations and Administration Department
TF-CSIRT: Task Force of Computer Security Incidents Response Teams
TLR: Traffic Light Rating
TRANSITS: Computer Security and Incident Response Team (CSIRT) personnel trainings
TSP: Trust Service Provider
US: United States of America
WP: Work programme

Annex D: List of Policy References

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

Year	Reference	Policy/legislation reference. Complete title and link
2017		
	2017 Cybersecurity Strategy	JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN/2017/0450 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN
	Cybersecurity Act, Proposed ENISA regulation	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
	Council Conclusions on 2017 Cybersecurity Strategy	Council Conclusions of 20 November 2017 on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU -- http://www.consilium.europa.eu/media/31666/st14435en17.pdf
2016		
	The NIS Directive	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30, available at: ELI: http://data.europa.eu/eli/dir/2016/1148/oj
	COM communication 0410/2016 on cPPP	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0410
	COM decision C(2016)4400 on cPPP	COMMISSION DECISION of 5.7.2016 on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation, Brussels, 5.7.2016, C(2016) 4400 final, available at (including link to the Annex): https://ec.europa.eu/digital-single-market/en/news/commission-decision-establish-contractual-public-private-partnership-cybersecurity-cppp
	Joint Communication on countering hybrid threats	JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats a European Union response, JOIN/2016/018 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018
	General Data Protection Regulation (GDPR)	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88, available at: http://data.europa.eu/eli/reg/2016/679/oj
	LEA DP Directive	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131, available at: http://data.europa.eu/eli/dir/2016/680/oj
	PNR Directive	Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132–149, available at: ELI: http://data.europa.eu/eli/dir/2016/681/oj
2015		
	Digital Single Market Strategy for Europe (DSM)	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital

		Single Market Strategy for Europe, COM/2015/0192 final, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX:52015DC0192
	Payment Services Directive	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), OJ L 337, 23.12.2015, p. 35–127, available at: http://data.europa.eu/eli/dir/2015/2366/oj
	The European Agenda on Security	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, The European Agenda on Security, COM/2015/0185 final, available at:http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2015:0185:FIN
2014		
	eIDAS Regulation	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73–114, available at: http://data.europa.eu/eli/reg/2014/910/oj
	Communication on Thriving Data Driven Economy	Towards a thriving data-driven economy, COM(2014) 442 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the regions, July, 2014, available at: https://ec.europa.eu/digital-agenda/en/news/communication-data-driven-economy
2013		
	Council Conclusions on the Cybersecurity Strategy	Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, agreed by the General Affairs Council on 25 June 2013, http://register.consilium.europa.eu/pdf/en/13/st12/st12109.en13.pdf
	Cybersecurity Strategy of the EU	JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667
	ENISA Regulation	Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the The EU Cybersecurity Agency(ENISA) and repealing Regulation (EC) No 460/2004, OJ L 165, 18.6.2013, p. 41–58, available at: http://data.europa.eu/eli/reg/2013/526/oj
	Directive on attacks against information systems	Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14.8.2013, p. 8–14, available at: http://data.europa.eu/eli/dir/2013/40/oj
	Framework Financial Regulation	Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council, OJ L 328, 7.12.2013, p. 42–68, http://data.europa.eu/eli/reg_del/2013/1271/oj
	COM Regulation 611/2013 on the measures applicable to the notification of personal data breaches	Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, OJ L 173, 26.6.2013, p. 2–8, available at: http://data.europa.eu/eli/reg/2013/611/oj
2012		
	Action Plan for an innovative and competitive Security Industry	Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee regarding an Action Plan for an innovative and competitive Security Industry, COM(2012) 417 final
	European cloud computing strategy	The Communication COM(2012)529 'Unleashing the potential of cloud computing in Europe', adopted on 27 September 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF
	EP resolution on CIIP	European Parliament resolution of 12 June 2012 on critical information infrastructure protection – achievements and next steps: towards global cyber-security (2011/2284(INI)), available at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167
2011		
	Council conclusions on CIIP	Council conclusions on Critical Information Infrastructure Protection "Achievements and next steps:

		towards global cyber-security" (CIIP), 2011, Adoption of Council conclusions, available at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010299%202011%20INIT
	COM Communication on CIIP (old – focus up to 2013)	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection, 'Achievements and next steps: towards global cyber-security', Brussels, 31.3.2011, COM(2011) 163 final available at: http://ec.europa.eu/transparency/regdoc/rep/1/2011/EN/1-2011-163-EN-F1-1.Pdf
	EU LISA regulation	Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 286, 1.11.2011, p. 1–17, Version consolidated, after amendments, available here: http://data.europa.eu/eli/reg/2011/1077/2015-07-20
	Single Market Act	Single Market Act – Twelve levers to boost growth and strengthen confidence "Working Together To Create New Growth", COM(2011)206 Final
	Telecom Ministerial Conference on CIIP	Telecom Ministerial Conference on CIIP organised by the Presidency in Balatonfüred, Hungary, 14-15 April 2011
2010		
	Internal Security Strategy for the European Union	An internal security strategy for the European Union (6870/10), http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/113055.pdf
	Digital Agenda	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe, COM/2010/0245 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010DC0245&from=EN
2009		
	COM communication on IoT	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Internet of Things : an action plan for Europe, COM/2009/0278 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2009:0278:FIN
	Council Resolution of December 2009 on NIS	Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security, OJ C 321, 29.12.2009, p. 1–4, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009G1229(01)
2002		
	Framework Directive 2002/21/EC as amended	Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.4.2002, p. 33–50, consolidated version, after amendments, available at: http://data.europa.eu/eli/dir/2002/21/2009-12-19
	ePrivacy Directive 2002/58/EC as amended	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201 , 31/07/2002 P. 0037 – 0047, Consolidated version, after amendments, available at: http://data.europa.eu/eli/dir/2002/58/2009-12-19

ENISA

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

Athens Office

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

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