EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA PROGRAMMING DOCUMENT 2019-2021

Including multiannual planning, work programme 2019 and multiannual staff planning

Amendments

JUNE 2019

ABOUT ENISA

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

CONTACT

For media enquiries about this paper, please use press@enisa.europa.eu.

LEGAL NOTICE

This publication presents the ENISA Programming Document 2019-2021 as approved by Management Board in Decision No MB/2019/03. The Programming Document 2019-2021 is adopted as set out in the Annex 1 of this decision with the following remarks:

(1) The implementation of the outputs listed as Scenario 1 in the Programming Document 2019-2021 shall be launched as planned in the annual budgetary cycle;

(2) The implementation of the outputs listed as Scenario 2 in the Programming Document 2019-2021 shall be launched only after the approval of the draft Cybersecurity Act.

(3) After the draft Cybersecurity Act is adopted, the Management Board shall assess whether the Programming Document 2019-2021 should be amended.

The Management Board may amend Work Programme 2019 at any time.

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

COPYRIGHT NOTICE

TP-AH-19-101-EN-N ISBN: 978-92-9204-301-8 ISSN: 2467-4176 DOI: 10.2824/98700

TABLE OF CONTENTS

FOREWORD BY THE EXECUTIVE DIRECTOR

While preparing the 2019 work programme we are working in a context of many expectations and positive prospects. ENISA welcomes the new proposed cybersecurity act which provides for a strengthened ENISA with additional resources and staff. In addition to this, ENISA welcomes the 2017 cybersecurity package of legislative and non-legislative cybersecurity measures. ENISA also looks forward to the new permanent mandate, for the additional resources and additional budget to contribute to the new tasks provided for 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 the global challenges. Many EU MSs will benefit from a joint approach and EU institutions and EU bodies such as ENISA can help to foster effective EU cooperation, maximising 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 EU 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 in filling posts. The problem is here and is likely to stay. The global shortage of cybersecurity professionals is estimated to rise to two million by 2019 ([3]). The ENISA *Threat landscape report 2016* acknowledges the skills shortage ([4]) and recommends engagements in the areas of cybersecurity 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 provides for 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 demands of private stakeholders as well as those of the MSs. The prospect for the market can be significant as the

([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]) Chant, I., IEEE, The Institute, *The cybersecurity talent shortage is here, and it is 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]) Kauflin, J., *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,*Threat landscape report 2016*, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

EU can improve its position in internal market purchasing (private as well as through public procurement) and become a reference point to meet the challenge posed by global competition.

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

An agile ENISA, preparing for the future!

In the context of the Cybersecurity Act ([5]), 2019 marks the year that ENISA steps into a new future. ENISA is prepared and looks forward to adapting and capitalising on the opportunities of the new Regulation. The strengthened and permanent mandate and the new roles that are foreseen for ENISA lay the groundwork for an ambitious and pragmatic contribution to the cybersecurity of the EU. Encouraged by the prospect of a renewed and reinforced mandate, ENISA is ready to take on this opportunity and continue working towards a more cyber secure Union.

This document presents the amended Work programme of the agency for 2019, which takes account of the new budget and resources assigned to ENISA by the voted budget for 2019 ([6]) and the Cybersecurity Act.

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

Udo Helmbrecht
Executive Director

(5) The proposed Cybersecurity Act has been politically agreed between the European Parliament, the Council and the Commission and awaits the formal approval of the co-legislature. The agreed text is available here: https://data.consilium.europa.eu/doc/document/ST-15786-2018-INIT/en/pdf

Proposal for a Regulation of the European Parliament and of the Council, submitted by the Commission on 13 September 2017, on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) No 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act') (COM(2017) 477 final).

(6) General budget of the EU for the financial year 2019, Section 3 Commission, pages L67/885 for Union budget contribution and L67/1963 for authorized posts allocation under the Union budget. Available here: https://eur-lex.europa.eu/budget/data/General/2019/en/SEC03.pdf

MISSION STATEMENT

ENISA was set up in 2004 to contribute to the overall goal of ensuring a high level of NIS within the EU and acts as a centre of expertise dedicated to enhancing NIS in the EU and supporting the capacity building of Member States.

The mission of ENISA has been to contribute to securing Europe's information society by raising 'awareness of network and information security [(NIS)] and to develop and promote a culture, of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organisations in the Union' ([7]).

ENISA carries out its operations under an annual and multiannual work programme containing all of its planned activities drawn up by the executive director and adopted by the MB.

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

- Expertise: information, knowledge and skill on key NIS issues.
- Policy: support policymaking and implementation in the EU.
- Capacity: support capacity building across the EU (e.g. through training, recommendations and awareness-raising activities).
- Community: promote the NIS community (e.g. support computer emergency response teams (CERTs), coordination of pan-European cyber exercises).
- Enabling (e.g. engagement with stakeholders and furthering of international relations).

In doing so, ENISA will act 'without prejudice to the competence of the Member States regarding network and information security and ... to activities concerning public security, defence, national security' ([8]) and in compliance with the right of initiative of the European Commission. In order to achieve its mission, several objectives and tasks ([9]) have been assigned to ENISA.

In line with these objectives and tasks, ENISA carries out its operations under an annual and multiannual work programme containing all of its planned activities drawn up by the executive director and adopted by the 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. ENISA also provides the EU institutions, bodies and agencies (hereinafter: 'European Union institutions') and the Member States with a mechanism allowing them to call upon its services to support their NIS capability development ([10]), resulting in a more agile and flexible approach to achieving its mission.

Principles

In implementing its strategy, ENISA action is guided by the following principles.

- **Affirming itself as main point of reference of the EU on cybersecurity issues** to promote a consistent EU approach to NIS.

[7] Article 1(1) of ENISA Regulation (EU) No 526/2013: https://publications.europa.eu/en/publication-detail/-/publication/a227aef3-d802-11e2-bfa7-01aa75ed71a1/language-en
[8] Article 1(2) of ENISA Regulation (EU) No 526/2013
[9] Article 2 and 3 of ENISA Regulation (EU) No 526/2013
[10] Article 14 of ENISA Regulation (EU) No 526/2013

- **Adding value through complementarity with MS authorities and NIS experts** (primarily those competent in cybersecurity matters). ENISA will reinforce these communication channels via the development of sustainable cooperation in its various domains of competence.
- **Working closely with competent EU institutions** dealing with other aspects of NIS (the European Union Agency for Law-Enforcement Cooperation (Europol), the European Defence Agency (EDA), the European External Action Service (EEAS), sectorial agencies, etc.).
- **Achieving results by leveraging relevant stakeholder communities**, allowing ENISA to strengthen its knowledge of national NIS developments and facilitate the involvement of NIS experts in its activities, from NIS national competent authorities, the 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 the 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 NIS, as well as to other policy initiatives with cybersecurity elements in different sectors (e.g. energy, transport and finance).
- Providing independent opinions and preparatory work for the development and the update of policy and law.
- Supporting 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 NISD 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 authority 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 information on best practice 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 practice and initiatives across the EU by pooling information on cybersecurity deriving from the EU and national institutions, agencies and bodies.
- Making advice, guidance and information on critical-infrastructure security best practice available.
- In the aftermath of significant cross-border cybersecurity incidents, compiling reports with a view to providing guidance to businesses and people across the EU.
- Regularly organising awareness-raising activities in coordination with MS authorities.

Market-related tasks (standardisation, cybersecurity certification)

- Performing a number of functions specifically supporting the internal market and e.g. to provide a cybersecurity ‘market observatory’ by analysing relevant trends in the cybersecurity market to better match demand and supply and by supporting EU policy development in ICT standardisation and ICT cybersecurity certification areas.

- With regard to standardisation in particular, facilitating the establishment and uptake of cybersecurity standards.
- Executing the tasks provided for in the context of the future framework for cybersecurity certification.

Research and innovation (R & I)

- Contributing its expertise by advising EU and national authorities on priority setting in research and development (R & D), 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 (R & I) EU funding programmes.

Operational cooperation and crisis management

- Strengthening the existing preventive operational capabilities, in particular upgrading the pan-European cybersecurity exercises (Cyber Europe).
- Supporting operational cooperation as secretariat of the computer-security and incident-response team (CSIRTs Network) (as per NISD provisions) by ensuring, among other things, the good functioning of the CSIRTs Network IT infrastructure and communication channels and by ensuring structured cooperation with CERT-EU, the European Cybercrime Centre (EC3), EDA and other relevant EU institutions in line with the Commission proposal for the cybersecurity act ([11]).

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 EU level in line with the Commission proposal for the cybersecurity act.
- Facilitating cooperation e.g. at blueprint technical (CSIRT) 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 ENISA on a voluntary basis by Member States and other entities.

Cybersecurity certification of ICT products and services

- The European cybersecurity-certification framework for ICT products and services specifies the essential functions and tasks of ENISA in cybersecurity certification. The draft sets out 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.

[11] COM(2017)477

1. GENERAL CONTEXT

THREAT LANDSCAPE

The cyberthreat landscape continues to evolve. Assessed changes are indicative for the potential of developments both at the attacker and defender sides. Those changes had as source discrete developments in motives and tactics of the most important threat agent groups, namely cyber-criminals and state-sponsored actors. Monetization motives have contributed to the appearance of crypto-miners in the top threats. State-sponsored activities have led to the assumption that there is a shift towards reducing the use of complex malicious software and infrastructures and going towards low profile social engineering attacks.

Developments have been achieved from the side of defenders too. Through the emergence of active defence, threat agent profiling has led to a more efficient identification of attack practices and malicious artefacts, leading thus to more efficient defence techniques and attribution rates. Initial successes through the combination of cyberthreat intelligence (CTI) and traditional intelligence have been achieved. This is a clear indication about the need to open cyberthreat intelligence to other related disciplines with the aim to increase quality of assessments and attribution. Finally, defenders have increased the levels of training to compensate skill shortage in the area of cyberthreat intelligence. The vivid interest of stakeholders in such trainings is a clear indicator for their appetite in building capabilities and skills.

Through the emergence of active defence, threat agent profiling has led to a more efficient identification of attack practices and malicious artefacts.

Recent political activities have underlined the emergence of various, quite novel developments in the perceived role of cyberspace for society and national security. Cyber-diplomacy, cyber-defence and cyber-war regulation have dominated the headlines. These developments, when transposed to actions, are expected to bring new requirements and new use cases for cyberthreat intelligence. Equally, through these developments, existing structures and processes in the area of cyberspace governance will undergo a considerable revision. These changes will affect international, European and Member States bodies. It is expected that threat actors are going to adapt their activities towards these changes, affecting thus the cyberthreat landscape in the years to come.

In summary, the main trends in cyberthreat landscape are:

- Mail and phishing messages have become the primary malware infection vector.
- Exploit Kits have lost their importance in the cyberthreat landscape.
- Cryptominers have become an important monetization vector for cyber-criminals.
- State-sponsored agents increasingly target banks by using attack-vectors utilised in cyber-crime.
- Skill and capability building are the main focus of defenders. Public organisations struggle with staff retention due to strong competition with industry in attracting cybersecurity talents.
- The technical orientation of most cyberthreat intelligence produced is considered an obstacle towards awareness raising at the level of security and executive management.
- Cyberthreat intelligence needs to respond to increasingly automated attacks through novel approaches to utilization of automated tools and skills.
- The emergence of IoT environments will remain a concern due to missing protection mechanisms in low-end IoT devices and services. The need for generic IoT protection architectures/good practices will remain pressing.
- The absence of cyberthreat intelligence solutions for low-capability organisations/end-users needs to be addressed by vendors and governments.

All these trends are included in the content of the ENISA Threat Landscape 2018[12].
In the context of all these developments, ENISA has identified numerous activities to cope with the trends of the cyber-threat landscape and increase knowledge and capability levels for various stakeholder groups.

1.1 POLICY INITIATIVES

Since its establishment in 2004 the EU NIS agency, ENISA, has actively contributed to: raising awareness of NIS challenges in Europe, the development of Member State NIS capacities and the reinforcement of the cooperation of Member States and other NIS stakeholders.

NIS has been set high in the EU political agenda (notably in the European cybersecurity strategy (2013), the European cyber defence policy framework (2014) and in the European digital single market (2015)). ENISA will need to accompany the efforts of Member States and EU institutions in reinforcing NIS across Europe. Above all, the recent adoption of the European directive on measures to ensure a high common level of NIS further calls for ENISA to enhance its commitment to supporting a consistent approach towards NIS across Europe.

While ENISA should continue its well-established activities (from the support to the reinforcement of MS national capacities to the organisation of cyber-crisis exercises) the adoption of the NISD will require ENISA to develop further areas of action to accompany the evolution of NIS in Europe. ENISA will play a key role in: contributing to the NIS technical and operational cooperation by actively supporting MS CSIRT cooperation within the European CSIRTs Network and the NIS Cooperation Group; providing input and expertise for policy-level collaboration between national competent authorities as part of the cooperation group; supporting the reinforcement EU institution NIS 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 digital single market (DSM) and more generally of economic growth in Europe, including the development of NIS and related ICT industries in Europe.

While several EU institutions are mandated to act in the area of cybersecurity (CERT-EU, Europol, the EDA, the EEAS, etc.) ENISA aims to be the key point of reference for strategic analysis and advice on NIS issues. ENISA seeks to engage with other stakeholders (in particular the private sector) to use its experience and expertise to support them in their activities and to engage them in the EU effort to ensure a significant improvement of the state of cybersecurity in Europe.

The publication of the new EU cybersecurity package with its set of legislative and non-legislative measures (13 September 2017) has identified ENISA as a key pillar of the EU's ambition towards the reinforcement of cybersecurity across Europe. The strategy provides for the strengthening and reinforcing of ENISA.

- Section 2.1 addresses ENISA and its strengthening: it proposes a permanent mandate.
- It acknowledges ENISA's role in the NISD.
- It proposes an EU cybersecurity-certification framework: ENISA is to develop certification schemes and provide secretariat assistance to the EU cybersecurity-certification group. It envisages frameworks for:
    - critical high-risk applications,
    - widely deployed digital products and services,

[12] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

- low-cost digital devices.

ENISA welcomes the renewed cybersecurity strategy ([13]) and the new cybersecurity act ([14]).

[13] 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

[14] The proposed Cybersecurity Act has been politically agreed between the European Parliament, the Council and the Commission and awaits the formal approval of the co-legislature. The agreed text is available here: https://data.consilium.europa.eu/doc/document/ST-15786-2018-INIT/en/pdf

2. MULTIANNUAL PROGRAMMING 2019-2021

MULTIANNUAL PROGRAMME

This section reflects midterm priorities to guide the activities of ENISA for the next 3 years.

Priorities are supplemented with indications on the following.

- Guidelines to underpin ENISA's implementation of the multiannual and annual programming document.
- The expected added value of ENISA's work in achieving these priorities.

Annual outputs will derive from these priorities.

ENISA PRIORITIES

Priorities are supplemented with indications on the following.
- Guidelines to underpin ENISA's implementation of the multiannual and annual programming document.
-The expected added value of ENISA's work in achieving these priorities.

Activity 1 — Expertise. Anticipate and support Europe in facing emerging network and information-security (NIS) 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 software-related issues (e.g. mobile), interpersonal-communications services (ICS)/ supervisory control and data acquisition (SCADA), smart infrastructures and the internet of things (IoT).

Guidelines

- Collate and analyse in priority available expertise provided by national NIS competent authorities, closely liaise with them to support stocktaking activity and, when undertaking analyses and making recommendations, offer the opportunity to voluntary experts (from these authorities as well as from other relevant stakeholders) to take part in its work.
- Focus on challenges of significant added value for the EU NIS community and on the impact that aspects of those challenges may have on the functioning of critical economic and societal functions with the EU, as provided for in the NISD (e.g. expertise relevant to operators of essential services (OES)).
- Take a holistic approach encompassing the technical, organisational, regulatory and policy dimensions of NIS as well as different relevant approaches, including the user perspective and work whenever possible on a multiannual basis to deepen the understanding of identified issues.

Added value

- Provide European-wide visibility to existing NIS expertise, in particular that developed at national level.

- Foster convergent understanding of NIS challenges across the EU NIS community as well as of best practices to address them, by offering tailored, high-quality and up-to-date analyses and recommendations.
- Raise awareness of OES, European institutions and national public authorities of emerging 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 analyses, offering a general technical assessment of existing and anticipated threats and their root causes.
- Produce annual analyses of national incident reports according to the implementation of the telecom package, electronic identification and trust services for electronic transactions in the internal market (eIDAS) regulation[15] and the NISD.
- In addition to the general threat assessment, focus also on a specific dimension (e.g. sector or cross-sector threats in the context of the NISD, or threats to existing technologies whose usage is increasing e.g. internet protocol version 6 (IPv6) and threats whose risk is today underestimated but may increase in the future).
- Establish dissemination channels for the information created (threat intelligence) and make it available to stakeholders. The delivered threat intelligence is to consist of both main and side products of the threat assessments (e.g. cyber threats, threat agents, assets, mitigation controls, collected sources, other related items), put in context as appropriate.
- Provide a concise cyber-threat overview on a regular basis as they materialise 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 the ENISA analyses mentioned above.
- Ensure that the EU threat-landscape analyses benefit from relevant sources of information, in particular vendor reports, national threat assessments, research, media as well as information stemming from the CSIRTs network.
- Seek to enhance the visibility of these results to the EU NIS community by delivering generated material for various stakeholders in a consistent manner.

Added value

- Offer an EU-wide independent synthesis of technical threats of general interest for the EU, in particular in the context of the implementation of the NISD (e.g. OES, digital service providers).
- Improve general threat awareness of national and EU public and private entities and foster mutual understanding by national competent authorities on current and future threats.
- Establish a dialogue among relevant threat-intelligence stakeholders in the 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 analyses tailored to their needs.

([15]) Regulation (EU) No 910/2014

- 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 EU institutions on threats to their security (Activity 3) as well as creating synergies with crisis and CSIRT cooperation such as by supporting cooperation on the development of threat taxonomies (e.g. incident taxonomies) (Activity 4).

Multiannual priorities (2019-2021) for Objective 1.3. Research, development and innovation (RDI)

Priorities

- Support Member States and the European Commission in setting out EU R & D priorities within the context of the European contractual public-private partnership (cPPP) and the European Cyber Security Organisation (ECSO).

Guidelines

- Provide the secretariat of the national public authorities committee of ECSO: national public authority representatives committee (NAPAC).
- Support cooperation among national public authorities on R & D definition issues and, when relevant, liaise with other stakeholders represented within ECSO.
- Participate, whenever possible and upon request, in chosen ECSO working groups.

Added value

- Contribute to the smooth functioning and impact of the cPPP and seek to avoid duplication of efforts of EU institutions and Member States on research, development and innovation (RDI).
- 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 those related to the establishment of a functioning digital single market.

Activity 2 — Policy. Promote network and information security (NIS) as an EU policy priority

Multiannual priorities (2019-2021) for Objective 2.1. Supporting EU policy development

Priorities

- Carry out a regularly updated stocktake 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 sectorial 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) to ensure consistency with the framework and principles agreed upon in the NISD.
- Seek to identify, when possible, NIS challenges that may require policy development at EU level.
- Build upon this stocktaking and taking into accounts NIS challenges previously identified, offering NIS expert advice to the European Commission and other relevant EU institutions on these policy developments.

Guidelines

- Closely liaise with the European Commission to establish an up-to-date stocktake of ongoing and future initiatives.
- Benefit from the work undertaken in Objective 1 on NIS challenges and threats to advise on possible new policy developments.
- Foster dialogue among and with national NIS competent authority experts and other relevant stakeholders to develop in-depth and high-quality expertise to advise on EU policy developments.
- Ensure consistency of work on DSM-related policy developments with work undertaken under ECSO and, when relevant, contribute to that work according to its responsibilities with ECSO.
- Regularly inform national NIS competent authorities on policy via the cooperation group established by the NISD 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 consistency between future sectorial policy initiatives including regulations with the framework and principles agreed upon by the Member States and the European Parliament in the NISD, 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 (legislation) with a NIS dimension, by allowing them to share national views and experience and build upon those to make and agree recommendations.
- Focus on the NISD (in particular on OES requirements e.g. identification, security requirements, incident reporting) and on the eIDAS regulation as well as on NIS aspects of the general data-protection regulation (GDPR) (and more generally data protection) and the draft ePrivacy regulation.

Guidelines

- Establish structured dialogues, whenever possible, on a sustainable, multiannual basis, with voluntary national NIS competent-authority experts, themselves liaising with national stakeholders (e.g. OES).
- Aim to limit the number of dialogues and to increase the participation of all Member States and in a spirit of efficiency (favouring a cross-sectorial approach such as for the NIS of OES), while gradually taking sector specificities into account.
- Regularly inform national NIS competent authorities on policy via the cooperation group established by the NISD and in particular make its stocktaking.

Added value

- Support Member States in implementing EU policies by making high-quality recommendations available, building upon the experience of the EU NIS community and reducing duplication of effort across the EU.

- Foster the harmonised approach on implementation of EU policies and in particular legislation, even when mandatory harmonisation of national approaches is not enforced, such as in the NISD on 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 State capacity building

Priorities

- Advise and assist Member States in developing national cybersecurity capacities building upon national experiences and best practices.
- Focus on NISD NIS capacities, building on CSIRTs network and national CSIRT ongoing activities. ENISA is to continue to work on these with the aim of fostering the development of EU Member State CSIRTs.
- Develop NIS national capacities metrics, building upon NISD capacities, allowing for the assessment of the EU NIS capacity-development status.
- Identify and make recommendations on other national NIS capacities including their distribution across the EU NIS community to contribute to improving the NIS of the EU, e.g. national cybersecurity assessments, public-private partnerships (PPPs) such as in critical information infrastructure protection (CIIP), national information sharing schemes, etc.

Guidelines

- Carry out a regular stocktake of national NIS-capacity initiatives with a view to identifying trends to collect and analyse different approaches and practices.
- Liaise closely with national NIS competent authority experts to identify experience and best practice 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 to NIS capacities ranging from technical to organisational and policy.
- While creating a general NIS-capacity metrics, as a priority seek to identify the main trends at the EU level and advise individual Member States upon 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, on-site training).

Added value

- Continue to support the development of national NIS capacities, improving the level of preparedness and the response capacities of Member States, thus contributing to the overall cybersecurity of NIS across the EU.
- Foster sharing of best practice among Member States.
- Indirectly contribute to the capacity building of governments beyond the EU by making ENISA recommendations and training material available on the website, thus contributing to the international dimension of its mandate.
- In the context of CSIRTs, contribute to Activity 4 by supporting the development of both CSIRT maturity as well as of tools (e.g. in the context of the Connecting European Facility (CEF)) benefiting cooperation within the CSIRTs Network.

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 missions.
- In cooperation with CERT-EU, inform the European Commission and other relevant EU institutions on NIS threats via the production of regular and timely Info Notes.
- Provide (upon request and in coordination with the EU institutions) capacity-building support for training, awareness and the development of educational material.

Guidelines

- Liaison with EU agencies on the setting of 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 EU institutions with strong NIS capabilities to support ENISA actions under this objective.
- Reinforce links between EU institutions and general awareness-raising campaigns (e.g. through active engagement of EU institutions in the European cybersecurity month (ECSM)).

Added value

- Support the development of NIS capacities of EU institutions thus contributing to raising the overall level of NIS cybersecurity across the EU.
- Foster sharing of best practices among EU agencies and better drafting of NIS requirements to reduce duplication of effort and to encourage more systemic approaches to NIS.
- Complement CERT-EU work on active cybersecurity for the EU Institution through awareness raising and other proactive measures by offering advice on the NIS prevention dimension.

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

Priorities

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

Guidelines

- Build upon existing work done at national level in relation to the private sector on the basis of both regular stocktaking of national expertise (e.g. cyber hygiene) and Activity 1 work undertaken 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 (small and medium-sized enterprises (SMEs), large-sized enterprises, NIS experts or non-experts) and adopt a holistic approach of NIS capacities ranging from technical/operational to organisational and policy capacities.

- With a view to supporting EU-level information sharing on NIS developments to contribute to the functioning of ECSO as provided for in Objectives 1.3 and 2.1. 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) on an ad hoc basis and, subject 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 NIS development of businesses across the EU and support national NIS competent authorities in their efforts towards the 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

- Organise the ECSM and the European cybersecurity challenge (ECSC) with a view to making these events a sustainable EU event.
- 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 practice in awareness raising, in particular about communication activities.

Guidelines

- Establish a structured and sustainable (multiannual) dialogue with volunteer national NIS competent-authority 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 public to public authorities.
- Explore ways of using adapted communication channels under the ECSM and ECSC.

Added value

- Allow the organisation of Europe-wide events, increasing visibility on cybersecurity and on ENISA with the public, businesses, academia and the NIS community, including NIS students.
- Foster harmonisation of tailored awareness-raising messages across the EU with increased impact, building on the strengths of existing national initiatives thanks to the sharing of best practice.
- Strengthen cooperation among the Member States.
- Facilitate the development of national awareness-raising initiatives.

Activity 4 — Community. Foster the emerging European network and information security (NIS) community

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

Priorities

- Further develop and organise Cyber Europe 2020, exploring new dimensions and formats with the aim of further preparing the Member States and EU 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 according to Cyber Europe exercises, in particular the CSIRTs network provided for in the NISD.
- Contribute actively to the implementation of the blueprint by supporting MSs 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 MS crisis-management framework.
- Follow up closely the development of the CEF cybersecurity digital service infrastructure (DSI) common service platform (CSP) and ensure a smooth handover to ENISA and adoption by the CSIRT community.
- Proactively promote its expertise in cyber-crisis management and exercises to the benefit of other EU institutions and Member States wishing to develop exercises with a cyber dimension. In doing so, ensure consistency with the Cyber Europe framework.

ACTIVITY 4

Further develop and organise Cyber Europe 2020, exploring new dimensions and formats with the aim of further preparing the Member States and EU institutions to cyber crises likely to occur in the future in the EU.

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 on the CSIRTs network to ensure consistency in the development of procedures and tools for daily crisis-management information exchange.
- Explore the opportunity to participate as an observer at national or international exercises to share lessons learned, as well as to invite observers from other EU institutions and international organisations (e.g. NATO) to observe Cyber Europe on an ad hoc basis and subject to approval from the management board (MB).
- Evaluate the impact of the organisation of previous exercises and build upon these lessons learned to support the development of future exercises and in particular further develop the exercise platform.

Added value

- Allow the organisation of Europe-wide events, increasing visibility on cybersecurity and on ENISA with other EU institutions, Member States, the public, businesses, academia.
- Continue to improve cooperation among Member States and to further develop tools and procedures supporting their response to cross-border crises, thus raising the overall level of preparedness of the EU.
- Contribute to the development of the international dimension of its mandate.
- Support Objective 2.1 work by advising on policy developments related to EU-level cyber-crisis cooperation, building on its long experience of cyber-crisis exercises. Support Objective 3.1 by building on its cyber-crisis expertise to advise on national cyber-crisis capacity development.

Multiannual priorities (2019-2021) for Objective 4.2 CSIRT and other NIS community building

Priorities

- Provide the secretariat to the CSIRTs network, as provided for in the NISD.
- Actively support the CSIRT-network functioning, allow quick wins and guaranteeing the smooth functioning of the network by 2020: supporting tangible cooperation among CSIRTs.
- Take advantage of the development of the CSIRT core platform under the CEF mechanism to support the functioning of the CSIRTs network and advise, upon request, Member State CSIRTs on projects to be proposed under the future CEF call for projects.

Guidelines

- Develop a trustworthy and sustainable dialogue with MS CSIRTs and CERT-EU within the framework.
- Link its activities with those carried out under Objective 4.1, building on ENISA's expertise on cyber-crisis management, in a view to develop tools and procedures with the CSIRTs network e.g. daily information exchange on cyber-crises.

Added value

- Support increased NIS information exchange among CSIRTs and contribute to increasing cooperation among Member States in the event of incidents or of a crisis, thus contributing to increasing overall EU preparedness and response capacities.
- Build ground for increased cooperation in the future.
- Support the 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 talent with the aim of achieving priorities laid out in the WP.
- Optimise internal procedures, by using modern IT applications in several agency specialised areas.
- Develop internal management to support the development of ENISA's internal expertise as well as ensuring staff 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 on its internal processes and working methods.

Guidelines

- Propose the alignment of the multiannual staff-policy plan with the internal-expertise needs necessary to achieve the WP multiannual priorities.
- Improve recruitment effectiveness and internal process, in particular to accelerate and smooth the recruitment process, thus contributing to improving ENISA's internal expertise.
- Promote the development of sustainable teamwork among ENISA's experts.
- Continue to offer the recruitment of second national experts (SNEs).

- Continue to improve processes for monitoring financial flows (expects to maintain high commitment and payment rates to guarantee full implementation of WP).

Added value

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

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

Priorities

- Increase and improve involvement of MS NIS competent authority experts towards the implementation of the WP (stocktaking, involvement in the implementation of outputs).
- Proactively engage with other competent EU institutions (e.g. European Commission), other agencies, CERT-EU, to identify possible synergies, avoid redundancy and provide advice building on ENISA's NIS expertise.
- Seek to increase and evaluate the added value and impact of ENISA 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 EU's efforts to cooperate with non-EU countries and international organisations to promote international cooperation on NIS.

Guidelines

- When provided by the WP, establish structured (and whenever relevant and on a multiannual basis) dialogues with volunteer MS experts to deliver ENISA outputs (e.g. working groups such as that on cyber-crisis cooperation).
- Rely upon Member States when primarily responsible for national public-private cooperation, to engage with the private sector.
- Further develop tools and procedures to facilitate and make transparent the involvement of all stakeholders, in particular on the principles and procedures of the participation and consultation of national NIS competent authorities.
- Build on the network of liaison officers as the main exchange point for ENISA and MS for achieving these priorities.
- Carry out regular in-depth evaluations to assess the mid- to long-term impact of its action in certain areas of expertise.

Added value

- Build trust and mutual expertise with MS experts and other stakeholders and contribute to improve their adherence to and involvement with ENISA's work.
- Build trust and cooperation with other EU institutions and contribute to improving their own NIS.
- Increase ENISA's understanding on the needs of the European NIS community and in particular those of the Member States.
- Benefit from European NIS community expertise (in particular MS expertise) thus offering tailored, quality and up-to-date analyses and recommendations with high European added value.

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

ENISA developed key indicators to provide the metrics to measure performance, results and impact of the ENISA outcomes and output. A 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 2019-2021

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

3. WORK PROGRAMME 2019

The ENISA 2019 work programme follows the layout presented in multiannual programming Section 2. 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 of the activity and its anticipated added value, the main challenges for 2019 and a link to the multiannual objectives.

The activities presented in this section follow the structure of the ENISA strategy. After a short description of the activity the objectives are presented.

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 set out.

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 (e.g. reports, studies, papers),
  - E: event (e.g. conferences, workshops or seminars),
  - S: support activity, involving assistance to or close collaboration with e.g. EU institutions or Member States (as appropriate), for a specific activity that features established and shared objectives.
- KPIs tailored to 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.

The ENISA 2019 work programme has been amended during the first quarter of 2019 to reflect the new mandate and tasks of ENISA according to the Cybersecurity Act. The resource and budget allocations reflect the EU 2019 voted budget ([16]).

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 (NIS)

Output O.1.1.1 — Good practices for the security of the internet of things (IoT)

IoT is at the core of operations for many OES as defined in the NISD, especially considering recent initiatives towards smart infrastructures, industry 4.0 ([17]), 5G ([18]), smart grids ([19]), etc. With a great impact on the safety of the public, security and privacy, the IoT threat landscape is

[16] General budget of the EU for the financial year 2019, Section 3 Commission, pages L67/885 for Union budget contribution and L67/1963 for authorized posts allocation under the Union budget. Available here: https://eur-lex.europa.eu/budget/data/General/2019/en/SEC03.pdf

[17] https://ec.europa.eu/digital-single-market/en/fourth-industrial-revolution

[18] https://ec.europa.eu/digital-single-market/en/towards-5g

[19] https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters

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, ENISA will identify and analyse existing IoT security practices and standards (e.g. in the area of industry 4.0 and critical information infrastructures or consumer electronics), taking into consideration existing national expertise and practices. ENISA 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, ENISA will take into account and contribute to existing EU policy and regulatory initiatives (e.g. the NISD, the IoT action plan for Europe ([20]), the communication on building strong cybersecurity for the EU ([21]), the PPP on cybersecurity ([22]) and the 5G infrastructure public-private partnership (5G PPP) ([23])).

ENISA will develop targeted IoT case studies to identify risks and vulnerabilities, by setting out appropriate attack scenarios, and providing relevant recommendations and good practice. Moreover, it will consider establishing e.g. IoT security requirements, maturity levels, procurement guidelines or other means to promote awareness and to ensure security for safety. ENISA will also consider implementing online tools to visualise IoT security measures in order to further support stakeholders.

ENISA will also validate the results of the study (e.g. via joint workshops such as the two organised with Europol/EC3) with relevant national and EU initiatives (e.g. Alliance for the Internet of Things Innovation (AIOTI), Industrial Internet Consortium IIC (IIC) and interact with important digitised industries in the EU and IoT stakeholders from the public sector (e.g. DG Communications Networks, Content and Technology, the Joint Research Centre (JRC), Europol/EC3), as well as from the private sector including operators, integrators and manufacturers.

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

Output O.1.1.2 — Good practices for the security of smart cars

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 (which the emergence of 5G is expected to further promote) novel cybersecurity risks and threats arise and need to be managed. In light of the NISD, where road authorities and intelligent transport systems are among the entities identified as OES in the road-transport subsector, there is a growing call for smart-car security to be addressed.

ENISA will build on its previous smart car work ([24]) and identify and analyse existing security practices and standards in this area (e.g. UN-ECE dedicated task force (TF) on CYBER, International Organisation for Standardisation (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

[20] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2009:0278:FIN
[21] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN
[22] https://ec.europa.eu/digital-single-market/en/news/commission-decision-establish-contractual-public-private-partnership-cybersecurity-cppp
[23] https://5g-ppp.eu/
[24] https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

smart car security, safety, connectivity and autonomy, while mapping the emerging threat landscape.

Building on the previous initiative 'Europe on the Move' of May 2017, the European Commission put forward a strategy to make the EU a world leader for automated and connected mobility (17 May 2018). To assist the Commission and the Member States in achieving these objectives ENISA will consider and contribute to existing EU policy and regulatory initiatives (the NISD, the European strategy on cooperative intelligent transport systems ([25]), the DG Mobility and Transport C-ITS platform ([26]), the high-level group GEAR 2030 ([27])), as well as the 3rd mobility package ([28]) 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. The recommendation would pertain to the use of pioneer spectrum for 5G large-scale testing, cybersecurity issues and a data-governance framework that enables data sharing, in line with the initiatives of the 2018 data package. ENISA will take into account industry initiatives such as the European Automotive Telecom Alliance (EATA) and the 5G automotive alliance.

SMART CARS
ENISA will build on its previous smart car work and identify and analyse existing security practices and standards in this area analysing the emerging notions of connectivity and autonomy.

ENISA will develop targeted smart cars case studies to identify risks and vulnerabilities, by setting out 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 the Commission in the recommendation deliverable listed in the communication on CAM.

ENISA 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. Association des Constructeurs Européens d'Automobiles (ACEA).

ENISA will also validate the results of the study (e.g. via joint workshops) with relevant national and EU initiatives (such as EATA and European Road Transport Telematics Implementation Co-ordination Organisation (ERTICO) and interact with all important smart-car stakeholders from the public sector (such as the relevant European Commission service, JRC, national road authorities and from the private sector including automotive manufacturers, Original Equipment Manufacturer (OEMs)).

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

In the revised cybersecurity strategy of the EU published in September ([29]), the European Commission highlights '[…] the lack of European capacity on assessing the encryption of products and services used by the public, 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 Article 10 of its proposal for a regulation on ENISA, the 'EU cybersecurity agency', repealing Regulation (EU) 526/2013, of 13 Sept 2017,

[25] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0766
[26] https://ec.europa.eu/transport/themes/its/c-its_en
[27] https://ec.europa.eu/growth/content/high-level-group-gear-2030-report-on-automotive-competitiveness-and-sustainability_en
[28] https://ec.europa.eu/transport/modes/road/news/2018-05-17-europe-on-the-move-3_en
[29] 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

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 satisfying the criteria of security-enhancing as well as privacy-enhancing technology is encryption.

While acknowledging the importance of crypto-technologies in cybersecurity, encryption is still a key area of national security, especially for 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 practice and knowledge. In international standardisation, technical specifications for cryptographic algorithms already exist which should be considered at European level, too. Moreover, at European level the so-called SOGIS-MRA crypto catalogue ([30]) is already a major achievement as the first comprehensive collection of cryptographic means agreed on by participating MS competent authorities.

Working closely with the Member States, ENISA will act as a catalyst to raise awareness of 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.

For standardisation ENISA will 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 Quantum-Safe Cryptography (QSC) subgroup as well as TC Electronic Signatures and Infrastructures (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 European Committee for Standardisation (CEN)/European Committee for Electrotechnical Standardisation (Cenelec) groups (primarily JTC-13 as it begins its work).

3.1.0.1 Output O.1.1.4 — Good practices for the security of healthcare services

Recent cybersecurity incidents have shown that the healthcare sector is one of the most vulnerable. Based on ENISA studies, the current healthcare-sector cybersecurity situation has shown that the level of cybersecurity is low. For example, most hospitals do not 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 legacy medical devices.

Newly adopted EU legislation has indicated a shift in priorities: the NISD lists healthcare organisations as OES, the medical devices regulation ([31]) (MDR) includes obligatory safety and security provisions for medical devices and there is a Commission communication on enabling digital transformation of health and care in the digital single market ([32]).

[30] Senior Officials Group Information Systems Security, Mutual Recognition Agreement, https://www.sogis.org/uk/supporting_doc_en.html
[31] https://ec.europa.eu/growth/sectors/medical-devices/regulatory-framework_en
[32] https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering

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

To achieve these goals, ENISA will take into account existing national and EU policies and regulations, such as the requirements deriving from the NISD and will not contradict and interfere with those provisions and international standards (such as Health Insurance Portability and Accountability Act (HIPPA) and ISO 27799) as well as position papers from Commission working groups (MDR working group and the eHealth network).

ENISA will also validate the results of any studies (e.g. via joint workshops) with relevant national and EU initiatives and interact with healthcare organisations and policymakers (e.g. ASIP Sante in France, SPMS in Portugal), 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 this 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 NISD implementation (WP 2017).

Output O.1.1.5 — Good practices for maritime security (port security)

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 (by 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 ([33]). Ports are a critical information infrastructure for water transport and identified as OES in the NISD, where managing bodies of ports, including their port facilities and entities operating works and equipment contained within ports are all eligible to be classified as OES.

ENISA 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 networks and services to all relevant cyber-threat categories. The good practices will consider both the current port ICT environment and the emerging trends in 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 ENISA will take into account and contribute to existing EU policy and regulatory initiatives, such as the NISD and will not contradict and interfere with those national provisions, and interact with key stakeholders from the public sector, such as DG Mobility and Transport and the European Maritime Safety agency (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 study findings.

([33]) https://ec.europa.eu/transport/modes/maritime/ports/ports_en

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

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 (ETL) report is hence a source of generic cyberthreat 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 on threat-exposure reduction. This information will consist of available controls that are appropriate in order to reduce exposure and so mitigate the resulting risks. In addition to the ETL, 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 CTI will be in focus in 2019. Available CTI 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 a 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 the organisation of common meetings/events. In carrying out this work, collaboration with related experts (e.g. ENISA ETL stakeholder group) and vendors (through memorandums of understanding (MoUs)) will be maintained and expanded.

In 2019, ENISA will continue supporting the relevant CTI stakeholder community by organizing a CTI EU event for dissemination of CTI good practices and providing an interaction platform. This is the main instrument of mobilisation of CTI stakeholders; it will engage in the dissemination of ENISA CTI information of all kinds (e.g. Info notes).

In the realm of its involvement in the “Cybersecurity of 5G Networks” of the Commission[34], ENISA will deliver a 5G Threat Landscape mapping. This deliverable will be based on existing ENISA work in this area (SDN/5G Threat Landscape). This work will be updated – primarily to cover the radio access part – and will serve as basis for the identification of 5G related risks and their mitigation. The ENISA 5G Threat Landscape will be created with support of relevant stakeholders, while it will be supported by the Cooperation Group and the Computer Security Incident Response Teams network.

In support of the Member States, the Commission and relevant stakeholders, ENISA will consolidate national risk assessments performed by Member States into a single document. Together with the 5G Threat Landscape, this Consolidated risk assessment will flow into a joint review of the Union-wide exposure to 5G networks.

[34] Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks C(2019) 2335 final, available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58154

Output O.1.2.2 — Restricted and public Info notes on NIS

ENISA provides guidance on important NIS events and developments through Info Notes. From 2018 ENISA has produced 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 an 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 complying with its internal procedures.

General Info Notes

General info notes cover significant developments and announcements in cybersecurity. General info notes are not a response to incidents or vulnerabilities but are rather explanatory notes e.g. on 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 on such events, covering issues, points of action, mitigation measures, summaries, related practices, etc. Hence, the objective of this work is to provide a neutral overview of the state of play on an incident in a near-time manner.

Both types of Info Notes will be logically integrated with the cyber-threat information, thus building 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 stakeholders. In addition to the ENISA website, in 2019 Info Notes will be disseminated via the ENISA ETL platform.

Output O.1.2.3 — Support incident-reporting activities in the EU

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

Current and planned activities in this area include the following.

- Incident notification in the telecom sector (Article 13a telecom package). Currently ENISA facilitates the activities of the informal Article 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 (Article 19 eIDAS regulation). In 2019 ENISA will continue receiving the annual incident reports from the competent authorities. ENISA will analyse them and produce a consolidated, anonymised incident-analysis report. In addition, ENISA will build on lessons learned 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 private-sector stakeholders to better understand the needs and challenges of the sector.

- Incident notification in the context of the NISD. Further guidelines and support are needed from ENISA to facilitate the smooth implementation of the new provisions, using (where appropriate) opportunities arising under the 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 contributes to ensuring the efficient flow of voluntary information at MS request and to establish common situational awareness in the event of a large-scale cross-border incident.

ENISA has significant expertise on **incident reporting** at EU level through the work carried out with Member States and telecoms providers on the transposition of Article 13a of the 2009 telecommunications framework directive. ENISA 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

As the frequency and magnitude of cybersecurity incidents in the EU increase, the Commission recognised the need to improve shared situation awareness amongst EU and MS policymakers. In particular, the Commission 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 MS CSIRTs (on a voluntary basis) or NISD single points of contact, European cybercrime centre (EC3) at Europol and CERT-EU and where appropriate EU intelligence and situation 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 High representative of the EU (HR/VP) 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, ENISA 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 ENISA Info notes and are the intermediate reports towards the ETL report, the end year CTI 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 CTI. It is expected that such an offering will significantly enhance the capabilities of organisations with low cybersecurity maturity. And will contribute to them having a better understanding of the threat level and being in a position to better protect themselves.

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

Objective 1.3. Research, development and innovation (RDI)

Output O.1.3.1 — Supporting cPPP in establishing priorities for EU research & development

ENISA will continue providing analysis of the areas covered by the NISD, the cybersecurity package, the Commission decision on cPPP and the outcomes of relevant Horizon2020 projects e.g. the CSA projects (cyber watching, AEGIS and EU-Unity) and will aim to show where R & D activities funded in the context of H2020, CEF, Transits and GEANT would achieve the greatest impact. On cybersecurity aspects related to the GDPR, 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 and cPPP on cybersecurity in order to align the work being carried with the ENISA work programme. In addition, ENISA will continue to support NAPAC by offering a secretariat function.

ENISA will work closely with ECSO and cPPP on cybersecurity in order to align the work being carried with the ENISA work programme. In addition, ENISA will continue to support NAPAC by offering a secretariat function.

ENISA will look into adapting the current best practice 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 use 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 the Member States, to meet their goals by bringing its concrete NIS policy expertise. Relevant contributions will also be made on the proposal on the creation of the cybersecurity competence network with a European cybersecurity research and competence centre ([35]).

Type of outputs and performance indicators for each output 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 (IoT)	P: Good practices for security of IoT, Q4. E: Validation cybersecurity workshop, Q3-Q4. E: Joint ENISA-Europol conference on IoT cybersecurity, Q3-Q4. S: Support the Commission, 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	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 cybersecurity 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).

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

Output O.1.1.3 — Awareness raising on existing technical specifications for cryptographic algorithms	S: Support work in the area of cryptography and participation in SOG-IS and ETSI related groups/meetings, Q1-Q4.	Publish 2 news items or dissemination materials covering public documents and activities of the groups/meetings attended.
Output O.1.1.4 — Good practices for the security of healthcare services	P: Procurement guidelines for cybersecurity in hospitals, Q3-Q4. S: Support the Commission and the relevant MS healthcare organisations in EU policy initiatives (e.g. JASEHN WP 2018-2020), 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 maritime security (ports security)	P: Good practices for cybersecurity in the maritime sector, Q4. E: Maritime-cybersecurity workshop, Q3-Q4. S: Support the Commission, MS and maritime industry to holistically address cybersecurity 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	P: Report and online information offering; report, Q4, information offering during the year, Q1/2020 E: ENISA will organise the annual event on CTI EU, Q3-Q4. P: 5G Threat Landscape report, Q3,2019 Consolidated risk assessment report from MS input, Q3, 2019	Engage more than 10 MS in discussions and work related to the structure and content of ENISA threat landscape report. More than 5 000 downloads of the ENISA threat landscape report. Engagement of more than 80 CTI experts from industry, academia and MSs. At least 7 5G Experts participate in the review of the report At least 18 Member States participate in the Cooperation Group team supporting the activity At least 10.000 views of the delivered report At least 10 Member States provide input to be consolidated report At least 5.000 views of the delivered report
Output O.1.2.2 — Restricted and public Info notes on NIS	P: Info notes on NIS, Q1-Q2.	Coverage of all major incidents relevant to EU NIS policy priorities. Expand coverage to all key ENISA stakeholder groups.
Output O.1.2.3 — Support Incident-reporting activities in EU	P: Annual incident analysis report for the telecom sector, Q4. E: Three workshops for the Article 13a [36] working group. P: Annual incident analysis report for the trust-service providers, Q4.	More than 20 NRAs/EU MS contribute in preparation of the report (Article 13a) (P). More than 10 SBs/EU MS contribute in preparation of the report (Article 19) (P). Engage more than 10 MS in discussions and work related to

[36] Article 13a of the amended Framework Directive 2002/21/EC (2002).

	E: Two workshops for the Article 19 ([37]) meetings. S: Support MS and the Commission 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 Article 13a expert group, Q4.	implementing particularities of the NISD incident-reporting framework (S).
Output O.1.2.4 — Regular technical reports on cybersecurity situation	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 and innovation (RDI)		
Output O.1.3.1 — Supporting cPPP in establishing priorities for EU Research & Development (R & D)	S: Support for ECSO.	No paper to be produced.

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

Taking due account of recent legislative and policy developments, including the draft cybersecurity act. ENISA will continue working towards meeting preparatory requirements for the 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 the principle that, wherever possible, decisions must be taken at the level of government closest to citizens (‘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 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 MS 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 MS governments is demanding for ENISA as it is conditional to final approval of the cybersecurity act.

[37] Article 19 of the eIDAS regulation (2014).

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 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

ENISA will continue its work on supporting public and private bodies in implementing the eIDAS regulation by addressing technological aspects and building blocks for trust services. Aspects to be covered will be agreed with the Commission and MS through the eIDAS expert group. Interacting with the private sector will enhance the ability of ENISA 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. The eIDAS expert group will be consulted for approval on specific ENISA implementation guidelines and technical recommendations addressing operational aspects of trust-service providers, conformity-assessment bodies and supervisory authorities. ENISA will continue to accumulate experience of best-practice 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 Commission in assessing the relevant standards by reviewing their meeting of requirements of the eIDAS regulation. Furthermore, ENISA will continue to support the Commission 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 NISD

ENISA will leverage its expertise and good practice, among others, on critical information infrastructures, national cybersecurity 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.

ENISA can analyse specific issues identified in the second biennial cooperation group work programme (2018-2020), consult with MS competent authorities, and develop recommendations and suggestions that would allow the Commission and Member States to make informed decisions on NIS matters. It could be useful to use the work carried out on OES, DSPs and other service interdependencies 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 the national competent authorities under Objective 4 and for OES and DSP under Objective 2), under NISD objectives.

ENISA will also take stock of the lessons learned from the first year of implementation of the NISD and recommend good practices to the cooperation group and the Commission on the directive-transposition process.

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

The Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks[38] asks ENISA to support the NIS Cooperation Group and Member States with developing a so-called 5G toolbox of good practices for MS to mitigate 5G risks based on the national risk assessments and the joint risk assessment foreseen under Output 1.2.1.

In that context, ENISA will support MS and the Commission in identifying such possible good practices mitigating the risks mentioned above and in validating them against the needs and requirements of MS. The toolbox will include appropriate security measures and recommendations to mitigate the identified cybersecurity risks both at national and Union level.

OES AND DSP

ENISA will assist MSs in the implementation of OES and DSP security requirements by building on its knowledge and expertise in the area of security requirements, identification criteria, security measures and notification requirements.

Output O.2.2.3 — Assist MS in the implementation of OES and DSP security requirements

Drawing from the experience of the NIS cooperation group, ENISA will assist MSs in the implementation of OES and DSP security requirements by building on its knowledge and expertise in the area of security requirements, identification criteria, security measures and notification requirements. ENISA will work closely with Member States to identify cost effective practices and mature security frameworks.

In deriving such a set of common mechanisms, sector-specific needs are to 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 from those in the banking sector, where different risks prevail). ENISA will monitor the development of the NISD implementation (across all sectors in the MSs) and identify possible priorities and tasks for those involved.

However, ENISA 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.

ENISA will also compare and validate the results with other relevant approaches in the area of OES (e.g. Cybersecuirty Capability Maturity Model (C2M2), NICE Capability Maturity Model (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 contribute to setting the basis for sufficient convergence across the EU MSs. 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 regarding supervision and good-governance practices. In this light, ENISA will take stock of existing initiatives addressing this problem and will bring together stakeholders from different security domains to discuss the findings.

[38] Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks C(2019) 2335 final, available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58154

Output O.2.2.4 — [Output removed following the amendment of WP19.]

Output O.2.2.5 — Contribute to the EU policy in the area of privacy and data protection with policy input on security measures

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 of the technical implementation of the GDPR and of the forthcoming privacy 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 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 policymakers 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 two 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. Cooperation 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 ICT security

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 standard-developing organisations (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 NISD 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 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 as appropriate.

Output O.2.2.7 — Supporting the implementation of European Electronic Communications Code (EECC)

The proposal for the 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, NISD), the EECC, once adopted, is expected to bring more harmonisation at EU level and several improvements as regards the security part, such as the following.

- Broadening the scope to include also number-independent (Ni) interpersonal communications services (ICS) (also called over-the-top services (OTTs)).
- A comprehensive design 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. socioeconomic 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 establish 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 NISD

The key NISD obligations are currently implemented horizontally across all NISD 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 NISD 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 consistent 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. ENISA, 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 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 to customise the horizontal NISD measures. ENISA will do that by taking under consideration the sectorial specifications, standards, and existing initiatives/schemes.

ENISA will use its expertise and knowledge developed within the NISD (WP 2016, WP 2017, and WP 2018) and other CIIP-related activities. ENISA will work under the cooperation group, with MS experts.

Output O.2.2.9 — Hands on tasks in the area of certification of products and services

Having adopted the finally approved cybersecurity act and its component on certification, ENISA will support the Commission and the Member States by carrying out hands on tasks in this area for assisting them in deploying the framework.

Transitioning from policy preparation to policy implementation is a demanding action for ENISA 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 integrating existing schemes in the new EU framework in a flexible way. ENISA will continue working with stakeholders to collect, establish and understand expectations they have from the EU cybersecurity-certification framework. ENISA will implement an action plan in order to fulfil a role in the emerging EU cybersecurity certification framework for 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 ([39]). 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 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.

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	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		

[39] 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.

Output O.2.2.1 — Recommendations for technical implementations of the eIDAS regulation	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
Output O.2.2.2 — Supporting the implementation of the work programme of the cooperation group under the NISD	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. S: Support the Cooperation Group in developing a toolbox of good practices for 5G cybersecurity. (Q4 2019)	Engaging at least 12 MS in ENISA's contributions to the implementation of the NISD (S). 10 MS participate in the workshop/activity (E). Engaging at least 12 MS in ENISA's contributions to Cooperation Group efforts on 5G cybersecurity (S).
Output O.2.2.3 –Assist MS in the implementation of OES and DSPs Security requirements	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: One workshop 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 removed following the amendment of WP19.]		
Output O.2.2.5 — Contribute to EU policy in the area of privacy and data protection with policy input on security measures	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 ICT security	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 SDOs and relevant services of the European Commission and/or agencies.

Output O.2.2.7 — Supporting the implementation of EECC,	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 NISD	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
O.2.2.9 — Hands on tasks in the area of certification of products and services	P: Action plan for an EU certification framework, Q4.	Engage stakeholders from at least 15 EU MS.

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

Objective 3.1. Assist Member State capacity building

Output O.3.1.1 — Update and provide technical training for MS and EU bodies

In 2019 most of the activities in this area target at maintaining and extending the collection of good practice guidelines and training for CSIRT and other operational personnel. ENISA will support the development of MS incident-response preparedness by providing good practice guidance on key elements of NIS capacity building with a focus on CSIRT training and services in order to improve 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, ENISA will continue to provide an update of the training material, according to the findings of the stocktaking study for training in NISD sectors and provide a new set of training material based on emerging technologies in order to improve MS CSIRTs skills and capacities to efficiently manage cybersecurity events. A special emphasis is placed on supporting MS CSIRTs 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 training and advisories.

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

Output O.3.1.2 — Support EU MS in the development and assessment of NCSS

The NISD 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 national cybersecurity strategies (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 NCSs. ENISA, 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 NISD. Each year ENISA 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. ENISA 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 information 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

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, ENISA will support the development of MS 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 dialogue 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

For many years ENISA works closely with the main OES in the EU. It has set up several sectorial expert groups covering sectors such as maritime, finance and health ([40]). 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 on 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 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 ([41]).

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

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

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 Energy ISAC: ENISA plays a key role in the development and professionalisation of this ISAC. ENISA is a full member and is responsible for providing expertise through organising 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 legitimise 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 ISACs. The Commission will contribute in full to this approach with support from ENISA, with an acceleration needed in particular for sectors providing essential services as identified in the NISD'.

ENISA will support MS with the creation of national ISACs through engaging all relevant stakeholders: national competent bodies, the private sector i.e. OES 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

In December 2017, the operations of CERT-EU were formalised by way of a new Interinstitutional 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.

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 EU bodies on initiatives covering NIS dimension related to their missions

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 tabletop 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 ([42]) (including EASA, CERT-EU, EDA — including civil/defence 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 the public to gain essential cybersecurity 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 ECSM and working with the Member States delivering projects like the cybersecurity challenges as well as national initiatives, upon request from Member States.

Output O.3.3.1 — European cybersecurity challenges (ECSC)

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 cybersecurity experts in the EU MS, ENISA will continue to promote and advise EU MS on running national ‘Cybersecurity Challenge’ competitions.

ENISA will also continue to support the planning and development of the ECSC 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

Output O.3.3.2 — European cybersecurity month (ECSM) deployment

The metrics built into the ECSM- European Cybersecurity 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 the public 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

In 2019, ENISA will promote a series of new activities in the area of cybersecurity 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 programmes in the EU that aim to enhance cybersecurity skills among EU public in general, and cybersecurity experts in particular. The 2019 stocktaking exercise will cover academia, public institutions and private companies. As part of this programme, a skills-development scheme and maturity model will be established, by taking into account existing and similar frameworks and initiatives.

([42]) 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, bodies and agencies (CERT-EU), available at: https://www.eda.europa.eu/docs/default-source/documents/mou—eda-enisa-cert-eu-ec3—23-05-18.pdf

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 State capacity building		
Output O.3.1.1 — Update and provide technical training for MS and EU bodies	P: Update of existing operational training material and customisation 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-customised 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.
Output O.3.1.2 — Support EU MS in the development and assessment of NCSS	P: Good practices in innovation on cybersecurity under the NCSS, Q3-Q4. S: Developing an information 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 2 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	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	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 sectorial 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 (S).
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	S: Attending CERT-EU Steering Board 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 EU bodies on initiatives covering NIS dimension related to their missions	P: Report on the cooperation activities with relevant EU 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 — cybersecurity challenges	S: European cybersecurity challenge (ECSC) support, Q1-Q4. E: Q2-Q3: 'Award workshop' for winners of the ECSC 2019 (ENISA promotes best of the best).	At least two additional EU MS organise national cybersecurity challenges in 2019 and participate in the ECSC final.
Output O.3.3.2 — European cybersecurity month (ECSM) deployment	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	P: Q4, Stocktaking of existing services and programmes in the EU that aim to enhance cybersecurity skills for public, in general, as well as for cybersecurity experts.	Engage at least 15 organisations representing academia, public institutions and private companies from at least 10 MS.

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

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 points of contact and competent authorities set up under the NISD, 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 observer role (introduced in 2018) striving to make best use of observers.

The high-level exercise programme 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 MB after consultation with the MS Cooperation Group and the CSIRTs network set up under the NISD. 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 MB after consultation with the cooperation group and the CSIRTs network set up under the NISD 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

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 cooperation 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 cybersecurity exercising for all stakeholders. The CEP platform opens new opportunities for ENISA to enlarge the user base and thus offer to the operational cybersecurity communities opportunities to exercise and gain experience and knowledge. One way to 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 CEP.

Output O.4.1.3 — Support the implementation and further development of the cyber-crisis-collaboration blueprint

ENISA will support the implementation and further development of the cyber crisis collaboration blueprint. As specified in the blueprint: 'Cyber crisis response activities should be coordinated with other crisis management mechanisms at EU, national or sectoral levels. '

In particular, ENISA will support:

a) the Commission in further developing bilateral and multilateral Standard Operating Procedures (SOPs) for cyber-crisis cooperation with EU bodies and Institutions:

b) Member States, either through the NIS Cooperation Group activities or after individual requests by Member States for support in the development of Blueprint SOPs at a National level.

In addition, ENISA will support EU Institutions and Member States in testing their crisis management structures. Activities offered will range from remote training 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.

Output O.4.1.4 — Supporting the implementation of the information hub

Decision-supporting intelligence in the cybersecurity domain is scarce, despite today's security information overload [43]. 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 Commission communication on building strong cybersecurity for the EU [44], 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 Commission in the blueprint:

'As part of the regular cooperation at technical level to support European 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 MS CSIRTs (on a voluntary basis) or NISD single points of contact, European cybercrime centre (EC3) at Europol and CERT- EU and where appropriate the EU intelligence and situation centre at the 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 better support the fusion of Open Source information for these reports, ENISA has developed in 2018 a prototype called 'Open Cyber Situational Awareness Machine (OpenCSAM)' to perform open source information aggregation, 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 capability meant to assist in the development of EU cybersecurity situation reports, supporting a steady increase and offering guarantees in production time, quality and consistency.

CSIRTS
ENISA will continue its support to the Commission and Member States in the implementation of the NISD, in particular in the area of CSIRTs. As part of this activity, ENISA will continue its tasks as the secretariat of the CSIRTs network.

For this particular output, ENISA will leverage the experience gained from the first prototype in order to further develop OpenCSAM's functionalities and capabilities. ENISA will also foster the development of a community (Member States, Academia, Private Sector, EU Institutions) around OpenCSAM for getting contributions, feedback and evaluation during the development lifecycle. For this, a workshop is planned to take place in 2019 as well as a testing phase for the new functionalities OpenCSAM with an EU Institution related to the Aviation/Space sector.

Output O.4.1.5 — [Output removed following the amendment of WP19.]

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

ENISA will continue its support to the Commission and Member States in the implementation of the NISD, 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. ENISA 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, ENISA will be proactive in stimulating discussions within the network and will aim to provide content to support discussions

[43] 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

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

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 CSP cooperation 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.

ENISA 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

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 MS 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

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 cyber threats as well as to cross-border incidents.

In 2019, ENISA will actively support the platform handover procedure from an operational perspective (Trust Circles management). In particular, ENISA will engage in cooperation with the Commission and the Consortium for a smooth transition of the knowledge and expertise regarding the Trust Circles management task. Additionally, specific operational procedures that are mandatory to follow in order to maintain the underlying team data and references will be implemented by ENISA.

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	P: CE2020 Exercise Plan (restricted), Q4. E: Exercise planning events, Q2 & Q3. E: Cyber SOPEx 2019.	At least 80 % EU Member States/European Free Trade Association (EFTA) member 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	S: Support for the maintenance and further development of the cyber exercise platform (CEP), 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 — Supporting the implementation of the cyber-crisis-collaboration blueprint	P: Identify missing elements in the Cybersecurity Blueprint and exercise the CSIRTs network SOPs.	At least 2 exercises on the Blueprint collaboration.
Output O.4.1.4 — Supporting the implementation of the information hub	S: Enhance Blueprint stakeholders' situational awareness.	Provision of OpenCSAM tool to Blueprint stakeholders in Cyber Europe 2020.
[Output 4.1.5 removed following the amendment of WP19.]		
Objective 4.2. CSIRT and other NIS community building		
Output O.4.2.1 — EU CSIRTs network secretariat and support for EU CSIRTs network community building	S: Provide CSIRTs network Secretariat support (e.g. logistics, organisation of the meeting, agenda management, meeting minutes; conference calls infrastructure; working groups support; facilitate ad hoc operational 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).	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). 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

	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.	At least 4 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	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	S: Operational support for the MeliCERTes platform handover procedure specifically for 'Trust Circles management' task.	Engage in cooperation with the Commission and the Consortium for a smooth transition of the knowledge and expertise regarding the Trust Circles management task and related services.

ACTIVITY 5 — ENABLING. IMPROVE ENISA'S IMPACT

Objective 5.1. Management and compliance

Management

The **executive director** is responsible for the overall management of ENISA. The executive director has a personal assistant.

To support the executive director, the, MB secretariat will continue the administration of the MB 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 MB and the executive board in their functions by providing secretariat assistance.

In relation to the MB, following the applicable rules, two 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 programmes, projects and services on the overall management of ENISA, assisting the executive director in 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 ENISA. This also includes coordination with the European Commission Internal Audit Service (IAS), European Court of Auditors (ECA), European Ombudsman, European Commission, European Anti-Fraud Office (OLAF), DG Human Resources and Security, DG Budget, DG Communications Networks, Content and Technology, etc. All internal policies related to transparency, anti-fraud policy, whistle-blowers protection, declarations of interests, etc. are addressed within this activity.

RD strives to maintain and increase the efficiency and effectives of ENISA, 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 ENISA with adequate and modern procedures and tools to minimise the resources across ENISA maximising the intended delivery of the work programme and statutory commitments.

The core operations department (COD) coordinates the delivery of the core activities of ENISA. As such, the main role of the COD is to deliver activities A1-A4 of this work programme. The COD also includes the policy office and the public affairs team and the support of the ENISA Advisory Group and national liaison officers (NLO) network is also carried out within COD.

Policy office

Through the policy office, ENISA initiates and further develops strategic cooperation with relevant stakeholders active in cybersecurity community. For instance, ENISA engages in policy and strategy discussions with political and policy decision-makers (by participating or organising e.g. MEP breakfasts). Furthermore ENISA 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. The policy office also coordinates cross agency activities related to topical areas of interest. 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 a key corporate tool supporting 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 ENISA, 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 ENISA, 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

Head of Resources Department is delegated to be the Internal Control Coordinator of ENISA. It is aiming to implement the new Committee of Sponsoring Organizations of the Treadway Commission (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 MB 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 ENISA, in order to provide, to the Senior Management, executive director and the MB, independent and objective assurance.

IT

ENISA has launched a project that will run during the second half of 2019 in order to assess and improve 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 the development of a datacentre recovery site is absolutely necessary in order to enhance the IT service availability planned to be implemented in 2019.

By end of 2019 it is expected that all business applications, depending on the risk assessment, 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 in 2019 to consolidate the support technology in ENISA with modern, adequate and flexible business applications.

The Stakeholders Relationship Management application has been delivered and is available for 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.

MeliCERTes

Depending on the agreements with the European Commission, it is foreseen that as of November 2019, ENISA will take over the central component of MeliCERTes. It is envisaged that MeliCERTes will be the primary collaboration platform between participating Member States CSIRTs as well as to improve EU MS preparedness, cooperation and coordination, in order to better responding to emerging cyber threats as well as to cross-border incidents.

Negotiations are still undergoing with the European Commission to define the full scope of the components of the project to be taken over by ENISA, such as software development, helpdesk, etc.

The Corporate Services unit within the ENISA Resources Department will recruit two experts, which will be responsible for the project transition, in close collaboration with the European Commission and Consortium of providers. They will also be in charge of procuring equipment, setting up infrastructure and running/maintaining the infrastructure and other tasks as defined.

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, 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, ENISA continues its good practice to close accounts and process payments within the time frame.

ENISA 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 utilisation 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 minimize the numbers of 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 permanent ('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 HR management information system (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 ([45]). Most of the staff would be allocated to operational needs with some allocation of staff to ensure sufficient capacity for ENISA'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 %

([45]) ENISA 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.

Legal affairs, data protection and information security coordination

Legal Affairs

Legal affairs will continue supporting the legal aspects associated with the operation of ENISA. 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 ENISA 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 ([46]) the following.

- 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.
- 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; cooperate and consult with EDPS whenever needed.

Information security coordination

The information security officer 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 ENISA. The ISO is instrumental in incident handling and incident response and security event monitoring. The ISO also leads the security training for ENISA'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 committee:
  - 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.

([46]) The tasks of the DPO are explicitly mandated in Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.295.01.0039.01.ENG&toc=OJ:L:2018:295:TOC'

- 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, the public, etc. In its engagement with the stakeholders, ENISA is guided by principles as balanced representation, openness, transparency and inclusiveness.

Dissemination and Outreach

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

Several activities are planned in several Member States that will engender the cybersecurity 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 ENISA	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

In 2019, ENISA will strengthen internal communications to enhance staff engagement and to exploit opportunities for pooling and sharing. With the internal communication function being now under the HR unit, the objectives are:

- To enhance the accessibility of key HR information for staff members and managers
- To establish an internal communications strategy which is consistent and reflect the Agency’s strategic vision
- To develop internal communication processes/tools/channels/guidance document to support any organisational change
- To ensure staff is engaged (e.g.: launching of regular staff survey, dedicated staff survey, etc)
- To support the evolution/change of ENISA corporate culture

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
Staff Survey	Participation of staff in the staff survey	65 %	70 %	75 %

ENISA Advisory Group

In 2019, ENISA will continue to support the ENISA Advisory Group and will aim to reinforce the contribution of this group to the ENISA work programme.

The PSG ENISA Advisory Group is established by the new Cybersecurity Act.. It is envisaged that two meetings of the ENISA Advisory Group will take place during 2019.

National liaison officer network

ENISA in 2017 has kicked off various activities aiming at strengthening the cooperation with its NLO network. These activities were continued and were further prepared in 2018. NLOs are key actors for ENISA's daily work and they warrant the interaction with select public sector entities in the MS while they provide assurance in 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 ENISA contributes to (for example co-organiser, etc.) as well as time-critical information.
- ENISA 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 MB on missions, objectives and functioning of the NLO network will guide the development of this important tool for ENISA for community building. It is envisaged that two meetings of the NLO network will take place during 2019.

International relations

Under the executive director's guidance and initiative, ENISA will seek to strengthen contacts at an international level in line with the relevant provisions of the new Cybersecurity Act.

List of outputs: work programme 2019, after amendment

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 (NIS)
Output O.1.1.1 - Good practices for the security of the internet of things (IoT)
Output O.1.1.2 - Good practices for the security of smart cars
Output O.1.1.3 - Awareness raising on existing technical specifications for cryptographic algorithms
Output O.1.1.4 - Good practices for the security of healthcare services
Output O.1.1.5 - Good practices for maritime security (port security)
Objective 1.2. NIS threat landscape and analysis
Output O.1.2.1 - Annual ENISA threat landscape
Output O.1.2.2 - Restricted and public Info notes on NIS
Output O.1.2.3 - Support incident-reporting activities in the EU
Output O.1.2.4 - Regular technical reports on cybersecurity situation
Objective 1.3. Research, development and innovation (RDI)
Output O.1.3.1 - Supporting cPPP in establishing priorities for EU research & development
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
Objective 2.2. Supporting EU policy implementation
Output O.2.2.1 - Recommendations supporting implementation of the eIDAS regulation
Output O.2.2.2 - Supporting the implementation of the work programme of the cooperation group under the NISD
Output O.2.2.3 - Assist MS in the implementation of OES and DSP security requirements
Output O.2.2.4 - [Output removed following the amendment of WP19.]
Output O.2.2.5 - Contribute to the EU policy in the area of privacy and data protection with policy input on security measures
Output O.2.2.6 - Guidelines for the European standardisation in ICT security
Output O.2.2.7 - Supporting the implementation of European Electronic Communications Code (EECC)
Output O.2.2.8- Supporting the sectorial implementation of the NISD
Output O.2.2.9 - Hands on tasks in the area of certification of products and services
Activity 3 - Capacity. Support Europe maintaining state-of-the-art network and information-security capacities
Objective 3.1. Assist Member State capacity building
Output O.3.1.1 - Update and provide technical training for MS and EU bodies
Output O.3.1.2 - Support EU MS in the development and assessment of NCSs

Output O.3.1.3 - Support EU MS in their incident-response development
Output O.3.1.4 - Support EU MS in the development of ISACs for the NISD Sectors
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
Output O.3.2.2. Cooperation with relevant EU bodies on initiatives covering NIS dimension related to their missions
Objective 3.3. Assist in improving private sector capacity building and general awareness
Output O.3.3.1 - European cybersecurity challenges (ECSC)
Output O.3.3.2 - European cybersecurity month (ECSM) deployment
Output O.3.3.3 - Support EU MS in cybersecurity skills development
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
Output O.4.1.2 - Support activities for cyber exercises
Output O.4.1.3 - Support the implementation and further development of the cyber-crisis-collaboration blueprint
Output O.4.1.4 - Supporting the implementation of the information hub
Output O.4.1.5 - [Output removed following the amendment of WP19.]
Objective 4.2. CSIRT and other NIS community building
Output O.4.2.1 - EU CSIRTs network secretariat and support for EU CSIRTs network community building
Output O.4.2.2 - Support the fight against cybercrime and collaboration between CSIRTs and law enforcement
Output O.4.2.3 - Supporting the implementation and development of MeliCERTes platform

A ANNEXES

A.1 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 ENISA as described in the ENISA strategy. 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 optimised in order to increase the budget in operations.
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 ENISA detailed in Annex A.1.3 of this document.

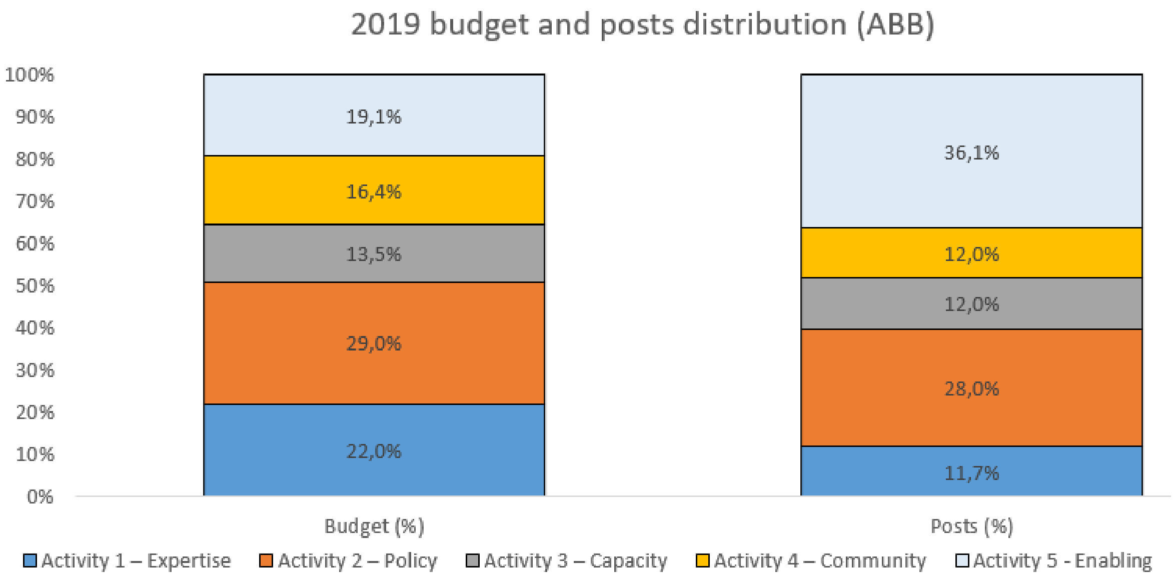
The RD already optimised all its resources. Improvements in order to gain in effectiveness and efficiency were developed. ENISA perform an internal check in relevance and optimisation of workflows, procedures and rules, to seek optimisation and efficiency. As an example the so-called paperless, (electronic workflow IT tool) which routes documents to staff involved in preparation, review and approval of all kinds of work-related documents and transactions represents a huge improvement and cost savings in all processes of ENISA.

Moreover, the RD 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 ENISA having in mind that the benchmarking of the EU Commission accept level up to 25 % of this group.

Job type[47]	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 %

For years 2019-2021, ENISA 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 are in line with the additional resources and budget in the voted general budget of the European Union for the financial year 2019 ([48]).



Overview of activities budget and resources

The budget and posts distribution is based on the ABB methodology of ENISA, which is line with the activity-based management (ABM) principle. ABB focuses on integrated budgeting and financial management, based on activities linked to ENISA'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 goods and services procured.
- **Indirect** budget is the cost estimate of salaries, mission costs and overhead costs, attributable to each **operational or compliance** activity. The indirect budget is redistributed against direct budget in all activities.

[47] 2018 values are part of the final Single Programming Document 2020-2022.
[48] General budget of the EU for the financial year 2019, Section 3 Commission, pages L67/885 for Union budget contribution and L67/1963 for authorized posts allocation under the Union budget. Available here: https://eur-lex.europa.eu/budget/data/General/2019/en/SEC03.pdf

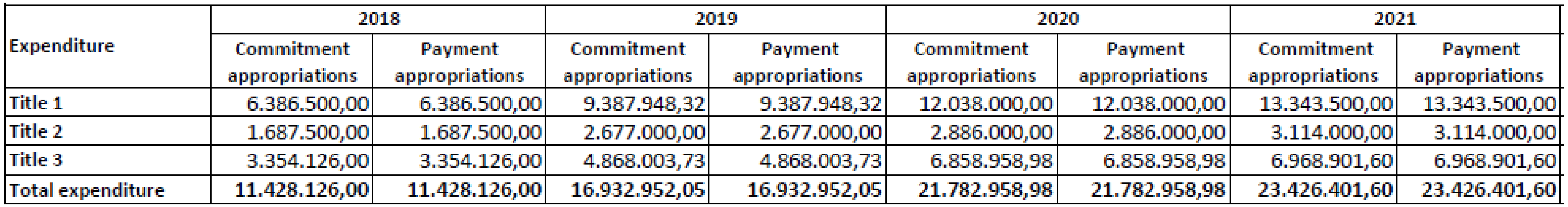
- **Compliance** posts from Activity A5 Enabling are redistributed to Core activities — A1 to A4, and **operational** posts of the Activity A5.
- Total ABB posts (FTEs) are the sum of all the posts from all activities (A1 to A5) after the re-distribution.

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

2019	Total ABB budget (€)	Total ABB posts (FTEs)
Activity 1 - Expertise. Anticipate and support Europe in facing emerging network and information security challenges	3.732.004,50	11,51
Activity 2 - Policy. Promote network and information security an EU policy priority	4.904.920,21	27,45
Activity 3 - Capacity. Support Europe in maintaining state-of-the-art network and information security capacities	2.281.854,18	11,81
Activity 4 - Community. Foster the emerging European Network and Information Security Community	2.772.346,20	11,81
Activity 5 - Enabling. Reinforce ENISA's impact	3.241.826,95	35,42
Total	16.932.952,05	98,00

A.2 HUMAN AND FINANCIAL RESOURCES 2019-2021

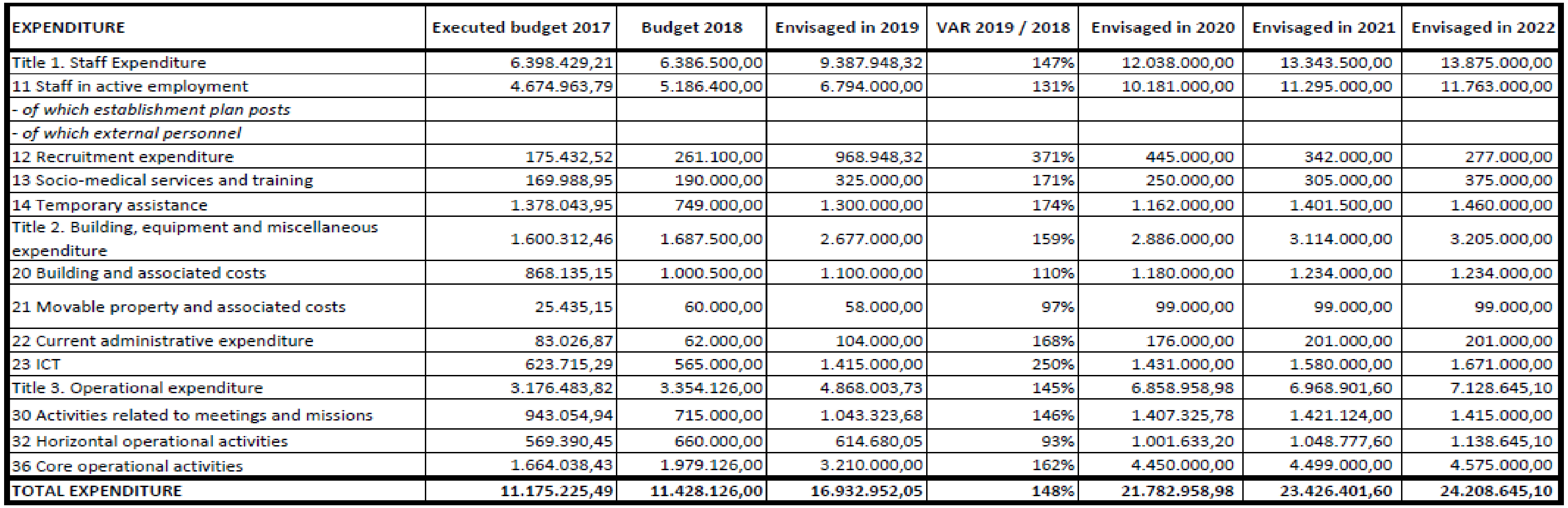
Table 1. Expenditure overview



Expenditure	2018		2019		2020		2021	
	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	9.387.948,32	9.387.948,32	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	2.677.000,00	2.677.000,00	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	4.868.003,73	4.868.003,73	6.858.958,98	6.858.958,98	6.968.901,60	6.968.901,60
Total expenditure	11.428.126,00	11.428.126,00	16.932.952,05	16.932.952,05	21.782.958,98	21.782.958,98	23.426.401,60	23.426.401,60

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

Commitment appropriations



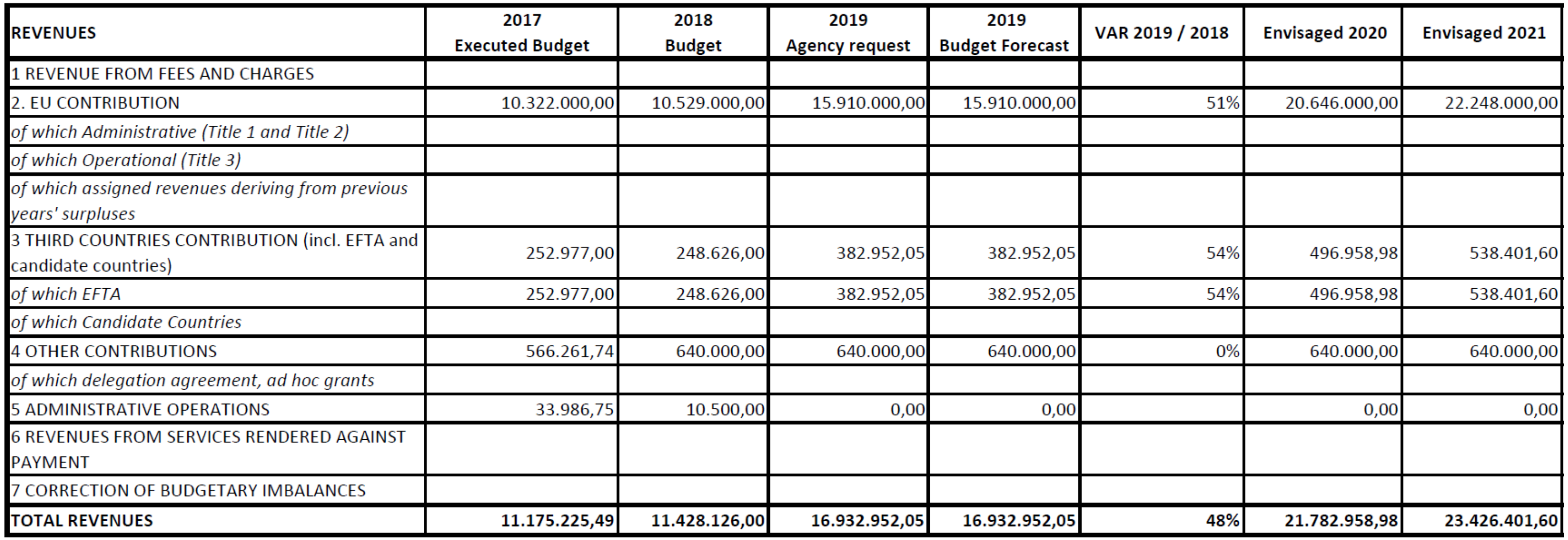
EXPENDITURE	Executed budget 2017	Budget 2018	Envisaged in 2019	VAR 2019 / 2018	Envisaged in 2020	Envisaged in 2021	Envisaged in 2022
Title 1. Staff Expenditure	6.398.429,21	6.386.500,00	9.387.948,32	147%	12.038.000,00	13.343.500,00	13.875.000,00
11 Staff in active employment	4.674.963,79	5.186.400,00	6.794.000,00	131%	10.181.000,00	11.295.000,00	11.763.000,00
- of which establishment plan posts							
- of which external personnel							
12 Recruitment expenditure	175.432,52	261.100,00	968.948,32	371%	445.000,00	342.000,00	277.000,00
13 Socio-medical services and training	169.988,95	190.000,00	325.000,00	171%	250.000,00	305.000,00	375.000,00
14 Temporary assistance	1.378.043,95	749.000,00	1.300.000,00	174%	1.162.000,00	1.401.500,00	1.460.000,00
Title 2. Building, equipment and miscellaneous expenditure	1.600.312,46	1.687.500,00	2.677.000,00	159%	2.886.000,00	3.114.000,00	3.205.000,00
20 Building and associated costs	868.135,15	1.000.500,00	1.100.000,00	110%	1.180.000,00	1.234.000,00	1.234.000,00
21 Movable property and associated costs	25.435,15	60.000,00	58.000,00	97%	99.000,00	99.000,00	99.000,00
22 Current administrative expenditure	83.026,87	62.000,00	104.000,00	168%	176.000,00	201.000,00	201.000,00
23 ICT	623.715,29	565.000,00	1.415.000,00	250%	1.431.000,00	1.580.000,00	1.671.000,00
Title 3. Operational expenditure	3.176.483,82	3.354.126,00	4.868.003,73	145%	6.858.958,98	6.968.901,60	7.128.645,10
30 Activities related to meetings and missions	943.054,94	715.000,00	1.043.323,68	146%	1.407.325,78	1.421.124,00	1.415.000,00
32 Horizontal operational activities	569.390,45	660.000,00	614.680,05	93%	1.001.633,20	1.048.777,60	1.138.645,10
36 Core operational activities	1.664.038,43	1.979.126,00	3.210.000,00	162%	4.450.000,00	4.499.000,00	4.575.000,00
TOTAL EXPENDITURE	**11.175.225,49**	**11.428.126,00**	**16.932.952,05**	**148%**	**21.782.958,98**	**23.426.401,60**	**24.208.645,10**

Payments appropriations

EXPENDITURE	Executed budget 2017	Budget 2018	Envisaged in 2019	VAR 2019 / 2018	Envisaged in 2020	Envisaged in 2021	Envisaged in 2022
Title 1. Staff Expenditure	6.398.429,21	6.386.500,00	9.387.948,32	147%	12.038.000,00	13.343.500,00	13.875.000,00
11 Staff in active employment	4.674.963,79	5.186.400,00	6.794.000,00	131%	10.181.000,00	11.295.000,00	11.763.000,00
- of which establishment plan posts							
- of which external personnel							
12 Recruitment expenditure	175.432,52	261.100,00	968.948,32	371%	445.000,00	342.000,00	277.000,00
13 Socio-medical services and training	169.988,95	190.000,00	325.000,00	171%	250.000,00	305.000,00	375.000,00
14 Temporary assistance	1.378.043,95	749.000,00	1.300.000,00	174%	1.162.000,00	1.401.500,00	1.460.000,00
Title 2. Building, equipment and miscellaneous expenditure	1.600.312,46	1.687.500,00	2.677.000,00	159%	2.886.000,00	3.114.000,00	3.205.000,00
20 Building and associated costs	868.135,15	1.000.500,00	1.100.000,00	110%	1.180.000,00	1.234.000,00	1.234.000,00
21 Movable property and associated costs	25.435,15	60.000,00	58.000,00	97%	99.000,00	99.000,00	99.000,00
22 Current administrative expenditure	83.026,87	62.000,00	104.000,00	168%	176.000,00	201.000,00	201.000,00
23 ICT	623.715,29	565.000,00	1.415.000,00	250%	1.431.000,00	1.580.000,00	1.671.000,00
Title 3. Operational expenditure	3.176.483,82	3.354.126,00	4.868.003,73	145%	6.858.958,98	6.968.901,60	7.128.645,10
30 Activities related to meetings and missions	943.054,94	715.000,00	1.043.323,68	146%	1.407.325,78	1.421.124,00	1.415.000,00
32 Horizontal operational activities	569.390,45	660.000,00	614.680,05	93%	1.001.633,20	1.048.777,60	1.138.645,10
36 Core operational activities	1.664.038,43	1.979.126,00	3.210.000,00	162%	4.450.000,00	4.499.000,00	4.575.000,00
TOTAL EXPENDITURE	11.175.225,49	11.428.126,00	16.932.952,05	148%	21.782.958,98	23.426.401,60	24.208.645,10

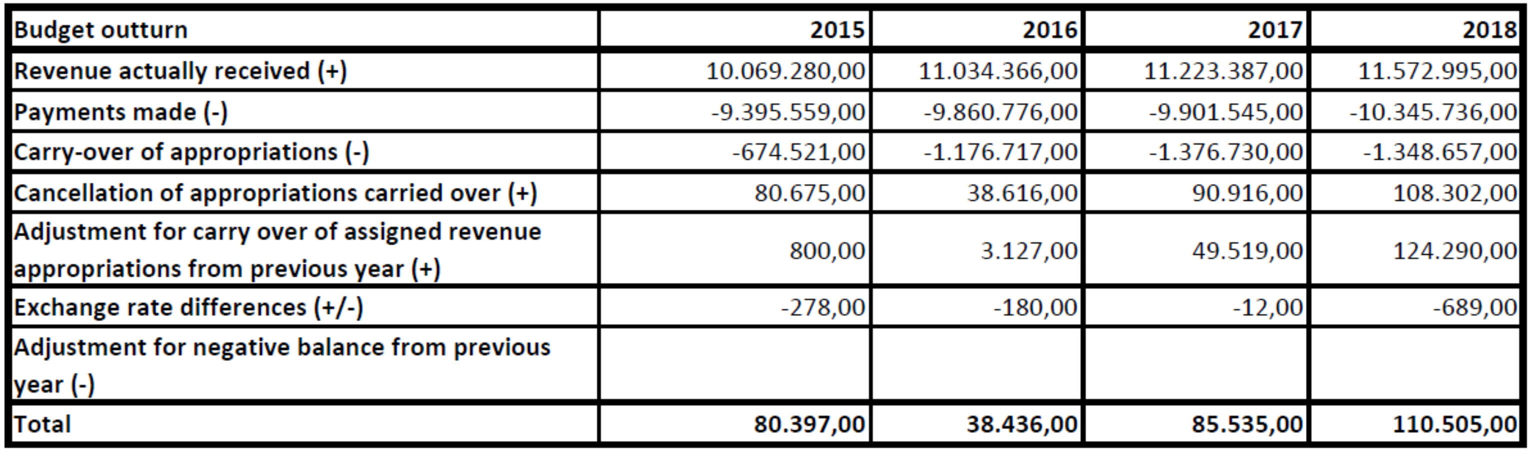
Table 2— Revenue overview

Revenues	**2017**	**2018**	**2019**	**2020**	**2021**
	Revenues estimated by the agency	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	15.910.000,00	20.646.000,00	22.248.000,00
Other revenue	853.225	899.126	1.022.952,05	1.136.958,98	1.178.401,60
Total revenues	**11.175.225**	**11.428.126**	**16.932.952,05**	**21.782.958,98**	**23.426.401,60**



REVENUES	2017 Executed Budget	2018 Budget	2019 Agency request	2019 Budget Forecast	VAR 2019 / 2018	Envisaged 2020	Envisaged 2021
1 REVENUE FROM FEES AND CHARGES							
2. EU CONTRIBUTION	10.322.000,00	10.529.000,00	15.910.000,00	15.910.000,00	51%	20.646.000,00	22.248.000,00
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)	252.977,00	248.626,00	382.952,05	382.952,05	54%	496.958,98	538.401,60
of which EFTA	252.977,00	248.626,00	382.952,05	382.952,05	54%	496.958,98	538.401,60
of which Candidate Countries							
4 OTHER CONTRIBUTIONS	566.261,74	640.000,00	640.000,00	640.000,00	0%	640.000,00	640.000,00
of which delegation agreement, ad hoc grants							
5 ADMINISTRATIVE OPERATIONS	33.986,75	10.500,00	0,00	0,00		0,00	0,00
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT							
7 CORRECTION OF BUDGETARY IMBALANCES							
TOTAL REVENUES	**11.175.225,49**	**11.428.126,00**	**16.932.952,05**	**16.932.952,05**	**48%**	**21.782.958,98**	**23.426.401,60**

Table 3 — Budget out-turn and cancellation of appropriations. Calculation of budget out-turn



Budget outturn	2015	2016	2017	2018
Revenue actually received (+)	10.069.280,00	11.034.366,00	11.223.387,00	11.572.995,00
Payments made (-)	-9.395.559,00	-9.860.776,00	-9.901.545,00	-10.345.736,00
Carry-over of appropriations (-)	-674.521,00	-1.176.717,00	-1.376.730,00	-1.348.657,00
Cancellation of appropriations carried over (+)	80.675,00	38.616,00	90.916,00	108.302,00
Adjustment for carry over of assigned revenue appropriations from previous year (+)	800,00	3.127,00	49.519,00	124.290,00
Exchange rate differences (+/-)	-278,00	-180,00	-12,00	-689,00
Adjustment for negative balance from previous year (-)				
Total	**80.397,00**	**38.436,00**	**85.535,00**	**110.505,00**

Cancellation of appropriations

- Cancellation of Commitment Appropriations

No commitment appropriations were cancelled.

In 2017, ENISA demonstrated 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 ENISA 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 EUR 1 411 440.51, 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 EUR 968 198.32 carried forward, 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 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	Envisaged in 2020	Envisaged in 2021
Officials	AD								
	AST								
	AST/SC								
TA	AD	34	28	34	29	34	43	51	57
	AST	14	15	14	13	13	16	18	19
	AST/SC								
Total		**48**	**43**	**48**	**42**	**47**	**59**	**69**	**76**
CA GFIV		16	12	28	17	28	28	28	28
CA GF III		15	12	2	11	5	2	2	2
CA GF II		1	0	0	0	0	0	0	0
CA GFI		1	1	0	1	0	0	0	0
Total CA		**33**	**25**	**30**	**29**	**33**	**30**	**33**	**33**
SNE		**3**	**1**	**6**	**3**	**3**	**9**	**12**	**12**
Structural service providers									
TOTAL		**84**	**69**	**84**	**74**	**83**	**98**	**114**	**121**
External staff for occasional replacement						5	5	5	5

NB: For 2017 Extra 7 seconded national expert (SNE) positions were granted to ENISA, without the corresponding budget so selections could not take place as budget was not available.

Table 2 — Multiannual staff policy plan 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	Establishment plan 2020		Establishment plan 2021	
	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
AD 14															
AD 13															
AD 12		3		3				3			6		6		6
AD 11															
AD 10		5		2				5			5		5		5
AD 9		10		3				10			12		12		12
AD 8		15		8				15			19		21		21
AD 7				1									3		6
AD 6				10									3		6
AD 5				1											
Total AD	**0**	**34**		**29**				**34**			**43**		**51**		**57**
AST 11															
AST 10															
AST 9															
AST 8															
AST 7		2		1				2			3		4		5
AST 6		5		1				5			7		8		8
AST 5		5		2				5			5		5		5
AST 4		2		5				1			1		1		1
AST 3				4											
AST 2															
AST 1															
Total AST	**0**	**14**		**13**				**13**			**16**		**18**		**19**
AST/SC 1															
AST/SC 2															
AST/SC 3															
AST/SC 4															
AST/SC 5															
AST/SC 6															
Total AST/SC															
TOTAL		**48**		**42**				**47**			**59**		**69**		**76**

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

A.4 HUMAN RESOURCES - QUALITATIVE

A.4.1 Recruitment policy

Statutory staff

ENISA 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/Articles 11 and 81 of Conditions of Employment of Other Servants of the European Union (CEOS)) and streamlining processes. The acquisition of a modern e-recruitment tool from another EU agency would definitively help.

ENISA 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 SC 1-SC 2, AST 1-AST 3, FG I, FG II.
- 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 AST 4-AST 7, FG III.
- Senior assistant job category (staff carrying out administrative, technical activities requiring high degree of autonomy and carrying out significant responsibilities in staff management, budget implementation or coordination): typically, these posts are filled by grades AST 7-AST 11 and only for the two Assistants to Head of departments by FG IV.

ENISA continues to enhance the management of selection procedure with a focus on improving time to hire, developing good practices in recruitment and streamlining processes.

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 AD 5, FG IV 13.
- Officer/administrator job category (staff providing officer expertise in a specific field of knowledge): typically, these posts are filled by grades AD 6-AD 7, 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 AD 8-AD 9.
- Team leader job category (staff providing operational excellence with some managerial responsibilities): typically, these posts are filed by grades AD 7-AD 10, FG IV 14-18.
- Lead expert/Advisor job category (staff providing strategical operational excellence with some managerial responsibilities if needed): typically these posts are filled by grades AD9 – AD12.

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 AD 9-AD 12.

- 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 AD 11-AD 13).
- Executive director (filled by grades AD 14-15).

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.

On the duration of employment, temporary agents (TAs) and contract agents (CAs) are offered typically long-term contract of three years, renewable for another limited period of five years[49]. 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 on employment contract renewal. In addition, ENISA is activating short-term contract agents (2 years, renewable once for a maximum one year) to be allocated depending on business needs or any other human resources constraints (i.e. long-term sick leave or part-time, etc.) This engagement of staff allows ENISA to keep an adequate degree of flexibility and adapt the workforce based in the business needs.

Non-statutory staff
ENISA welcomes SNEs as an opportunity to foster the exchange of experience and knowledge of ENISA 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 ENISA’s work and in the European system in general. The traineeship may last from a minimum of six months to a maximum of 12 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. ENISA holds a framework contract that has been awarded to a temping agency.

A.4.2 Appraisal of performance and reclassification/promotions

ENISA has adopted the implementing rules: MB 2016/10 on Reclassification of CAs, 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.

[49] With the view to the draft CSA and with the aim to attract and retain the most qualified and motivated staff, the contract length for TA has been changed into 5 years initial contract with the possibility to be renewed for an indefinite period (ED Decision 16/2019 of 20 February 2019).

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/SC 1					
AST/SC 2					
AST/SC 3					
AST/SC 4					
AST/SC 5					
AST/SC 6					
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**		

A.4.3 Mobility policy

All internal moves are processed via Article 7 of the Staff Regulations and for transparency purposes are published internally on INTRAENISA. In order to create a motivated and versatile workforce, ENISA has adopted an ED policy 01/2017 of 22 February 2017 on internal mobility policy. ENISA also joined the inter-agency job market (IAJM) with the view, as for all other agencies, to offer possibilities of mobility to staff in agencies by assuring a continuation of careers and grades. In 2016 and 2018, 2 staff members moved via the IAJM.

A.4.4 Learning and development

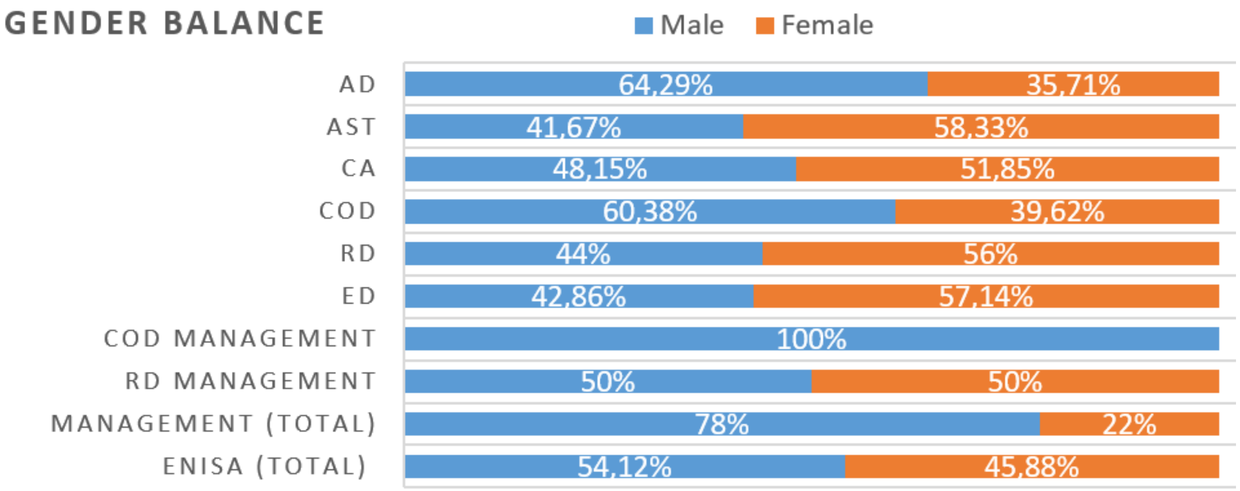
ENISA is striving for excellence in the approach to developing staff. In order to make the most out of its internal expertise and to develop mechanisms to retain staff, the organisation is focusing on offering a wide range of Learning and Development Opportunities including mandatory training (e.g. Ethics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

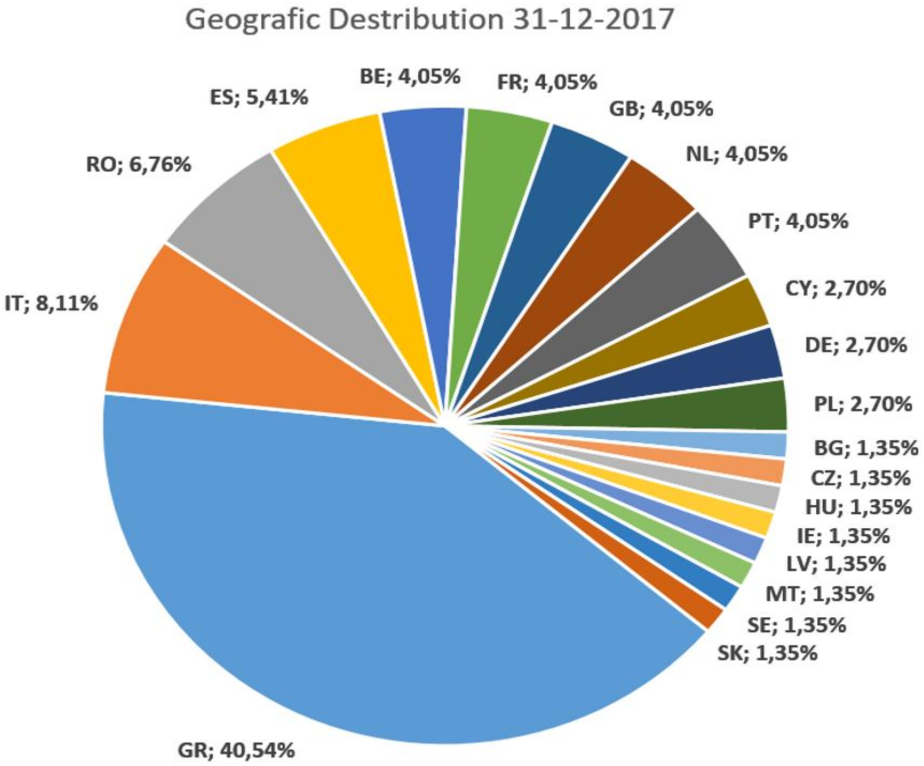
A.4.5 Gender and geographical balance

As of 31/12/2017 ENISA counts with 74 staff members (42 TAs from which 29 ADs and 13 ASTs), 29 CAs and 3 SNEs.

The overall gender balance among ENISA staff shows a male prevalence that is understandable given the scope of ENISA’s work. As a measure to promote equal opportunities, the terms of published vacancy notices prevent any kind of discrimination and the selection board 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, ENISA nominated in 2016 and 2017 a French woman as head of HR and a Swedish woman as head of finances and procurement.

For 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:





A.4.6 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 three 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 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 PRIVILEGES AND IMMUNITIES

Agency privileges	Privileges granted to staff	
	Protocol of privileges and immunities/diplomatic status	Education/day care
Under 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 Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU) applies to ENISA and its staff.	Under 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 ENISA 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 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 focuses on ENISA's core operational activities, with an estimated expenditure above EUR 30 000. The overall objective of the annual evaluations is to evaluate the effectiveness, efficiency, added value, utility, coordination and consistency.

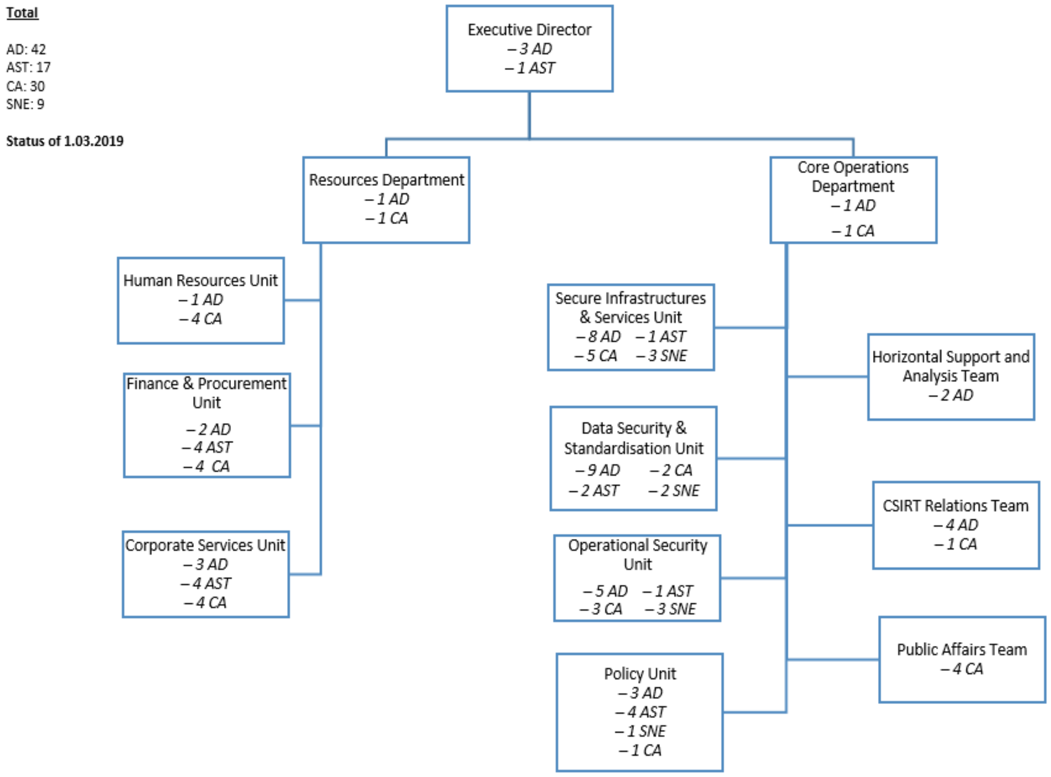
A.8 RISKS 2019

The risk assessment was performed by the IAS in 2016. Three areas were proposed for the next 3 years: Stakeholders' Involvement in the Production of Deliverables in ENISA (done in 2017), Human Resources (2018), Information and Communication Technology (2019).

A.9 PROCUREMENT PLAN 2019

2019 WP Procurement Planning	Direct budget (in EUR)	Procurement (tender) procedure required	Launch Dates	All other expenditure
Activity 1 - Expertise. Anticipate and support Europe in facing emerging network and information security challenges	875.000,00	765.000,00	Q1-Q4	110.000,00
Activity 2 - Policy. Promote network and information security an EU policy priority	1.150.000,00	1.130.000,00	Q1-Q4	20.000,00
Activity 3 - Capacity. Support Europe in maintaining state-of-the-art network and information security capacities	535.000,00	505.000,00	Q1-Q4	30.000,00
Activity 4 - Community. Foster the emerging European Network and Information Security Community	650.000,00	580.000,00	Q1-Q4	70.000,00
Activity 5 - Enabling. Reinforce ENISA's impact	760.073,73	712.767,00	Q1-Q4	47.306,73
Total A1-A5	3.970.073,73	3.692.767,00	Q1-Q4	277.306,73

A.10 ENISA ORGANISATION

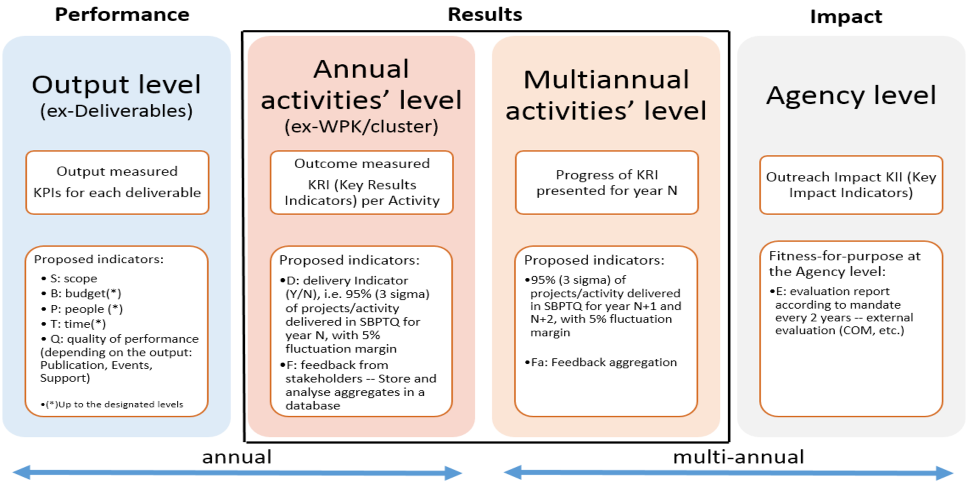


B ANNEX: SUMMARISING THE KEY INDICATORS FOR THE MULTIANNUAL ACTIVITIES

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

The purpose of key indicators for ENISA is to provide the metrics to measure against performance, results and impact of ENISA's outcome, output and impact. Key indicators seek to better support policy dynamics on NIS, 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 ENISA to report, and the need to avoid any unnecessary burden on ENISA. ENISA 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 ENISA remains the focal point for the key indicators introduced. The key notions and main vectors of annual and multiannual measurements are presented below.


Performance
Results
Impact
Output level
(ex-Deliverables)
Output measured
KPIs for each deliverable
Proposed indicators:
• S: scope
• B: budget(*)
• P: people (*)
• T: time(*)
• Q: quality of performance (depending on the output: Publication, Events, Support)
•(*)Up to the designated levels
Annual activities' level
(ex-WPK/cluster)
Outcome measured
KRI (Key Results Indicators) per Activity
Proposed indicators:
•D: delivery Indicator (Y/N), i.e. 95% (3 sigma) of projects/activity delivered in SBPTQ for year N, with 5% fluctuation margin
•F: feedback from stakeholders -- Store and analyse aggregates in a database
Multiannual activities' level
Progress of KRI presented for year N
Proposed indicators:
•95% (3 sigma) of projects/activity delivered in SBPTQ for year N+1 and N+2, with 5% fluctuation margin
•Fa: Feedback aggregation
Agency level
Outreach Impact KII (Key Impact Indicators)
Fitness-for-purpose at the Agency level:
•E: evaluation report according to mandate every 2 years -- external evaluation (COM, etc.)
annual
multi-annual

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 the following.
  i) Adherence to the scope of the deliverable or project.
  ii) Budget (or financial resources) available to the output or project, remaining within prescribed levels with a ± 5 % margin.

iii) People (or human resources) available to the output or project, remaining within prescribed levels with a ± 5 % margin.

iv) Time available to carry out the output or project remaining within prescribed levels with a ± 5 % margin.

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

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

  i) Delivery indicator aiming at delivery of at least 95 % against work programme planning. This is equivalent to a 3σ (3 Sigma) organisation (reaching between 93.3 % and 99.3 %); clearly ENISA 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 abovementioned deviation rate of ±5 % ( ). The criteria used, being scope, budget, people, time and quality, they all refer to the proper execution of the project leading up to the production of output. This evaluation is done at the end of the project within ENISA.

  ii) Following the production process that leads up to an output, feedback from stakeholders is collected on each output. Results are further aggregated on a multiannual basis by ENISA.

- Impact is measured at ENISA level only; it is based on feedback received from the evaluation of ENISA's performance (own initiatives and commissioned consulting at ENISA'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 ENISA level, are presented below.

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 completed 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 multiannual performance (**)	Fa	Numerical: quantitative target			
Time (e.g. duration of project plus or minus 5 %)	T	Variable: TLR	(*) *Feedback via e.g. survey associated with deliverables on website*					
Quality (e.g. citations, downloads, MS participation etc.)	Q	Integer: quantitative target	(**) *Aggregations of deliverables or categories thereof*					

All rating indicators follow a variable traffic-light rating (TLR) system that is laid out as follows:

- Green, that reflects 5 % deviation meaning that the planning/performance are appropriate and within prescribed levels.

- Yellow, that reflects 20 % deviation meaning that the planning/performance need to be revisited.
- Red, which reflects deviation above 20 % meaning that the planning/performance need thorough review.

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

Below follows an example of output related indicators to be collected on 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 the established requirements	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. workshop on privacy and security (***) Support e.g. NIS portal					

Below follows an example of outcome related indicators to be collected on the key types of agency activities, at the annual and at the multiannual level.

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

	45 % positive 45 % neutral 10 % negative	50 % positive 40 % neutral 10 % negative	55 % positive 40 % neutral 5 % negative	50 % positive 41 % neutral 9 % negative

C ANNEX: LIST OF ABBREVIATIONS

ABB: activity-based budgeting
ABM: activity-based management
APF: annual privacy forum
BEREC: Body of European Regulators of Electronic Communications
CAM: connected and automated mobility
CE2016: Cyber Europe 2016
CEF: Connecting Europe Facility
CEN: European Committee for Standardisation
Cenelec: European Committee for Electrotechnical Standardisation
CEP: cyber exercise platform
CERT: computer emergency response team
CERT-EU: Computer Emergency Response Team for the EU institutions, bodies and agencies
CIIP: critical information-infrastructure protection
CNW: CSIRTs network
COD: Core Operations Department
COM: European Commission
cPPP: cybersecurity Security public-private partnership
CSCG: ETSI CEN-CenelecENELEC cybersecurity Security coordination group
CSIRT: computer-security and incident-response team
CSP: common service platform
CSS: cybersecurity security strategy
CSSU: corporate stakeholders and services unit
CTI: cyber-threat intelligence
DG: directorate-general
DPA: data protection authorities
DPO: data protection officer
DSM: digital single market
DSP: digital service provider
E: Event, type of output (e.g. conferences, workshops or seminars)
EATA: European Automotive Telecom Alliance
EB: ENISA executive board
EBA: European Banking Authority
EC3: European cybercrime centre, Europol
ECA: European Court of Auditors
ECB: European Central Bank
ECSC: European cybersecurity challenge
ECSM: European cybersecurity month
ECSO: European cybersecurity organisation
ED: executive director
EDA: European Defence Agency
EDPS: European Data Protection Supervisor
EEAS: European External Action Service
EECC: EU electronic communications code
EFTA: European Free Trade Association (Stockholm Convention) (Iceland, Liechtenstein, Norway and Switzerland)
eID: electronic Identity
eIDAS: regulation on electronic identification and trusted services for electronic transactions in the internal market
ERA: European Railway Agency
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 equivalent
GDPR: general data protection regulation
H2020: Horizon 2020
HoD: head of department
HR: human resources
IAC: internal audit capability
IAJM: Inter-agency job market
IAS: Internal Audit Service
ICC: internal control coordination
ICS: industrial control systems
ICT: information and communication technology
INTCEN: EU intelligence and situation centre
IoT: internet of things
IS: information systems

ISAC: information-sharing and analysis centre
ISO: information-security officer
ISP: internet service providers
IT: information technology
IXP: internet exchange point
KGI: key goal indicator
KII: key impact indicator
KPI: key performance indicator
LEA: law-enforcement agency
M2M: machine to machine
MB: management board
MEP: Member of the European Parliament
MFF: multiannual financial framework
MS: Member State
NAPAC: National public authority representatives committee
NCSS: national cybersecurity strategies
NIS: network and information security
NISD: NIS directive
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
PAT: public affairs team
PDCA: plan-do-check-act
PETs: privacy-enhancing technologies
PNR: passenger name record
PPP: public-private partnership
PSD: payment services directive
PSG: permanent stakeholders group
Q: Quarter
QMS: quality management system
R & D: Research and Development
RD: resources department
S: Support activity, type of output
SB: supervisory body
SCADA: supervisory control and data acquisition
SDO: standard-developing organisations
SIAC: single intelligence analysis capacity
SME: small and medium-sized enterprise
SNE: seconded national experts
SO: strategic objectives
SOGIS: Senior Officials Group Information Systems Security
SOP: standard operating procedure
SRAD: stakeholder relations and administration department
TA: temporary agent
TC: technical committee
TF: task force
TF-CSIRT: task force of computer-security and incident-response teams
TLR: traffic light rating
Transits: Computer-security and incident-response team (CSIRT) personnel training
TSP: trust service provider
US: United States
WP: Work programme

D ANNEX: LIST OF POLICY REFERENCES

ENISA situates its work in the wider context of a legal and policy environment as pointed out below. Its activities and tasks are fulfilled as set out in 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: 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

	Passenger name record (PNR) directive	Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132–149, available at: ELI: http://data.europa.eu/eli/dir/2016/681/oj
2015		
	Digital Single Market Strategy for Europe (DSM)	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe, COM/2015/0192 final, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX:52015DC0192
	Payment Services Directive	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), OJ L 337, 23.12.2015, p. 35–127, available at: http://data.europa.eu/eli/dir/2015/2366/oj
	The European Agenda on Security	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, The European Agenda on Security, COM/2015/0185 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2015:0185:FIN
2014		
	eIDAS Regulation	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73–114, available at: http://data.europa.eu/eli/reg/2014/910/oj
	Communication on Thriving Data-Driven Economy	Towards a thriving data-driven economy, COM(2014) 442 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the regions, July, 2014, available at: https://ec.europa.eu/digital-agenda/en/news/communication-data-driven-economy
2013		
	Council Conclusions on the Cybersecurity Strategy	Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security policy Joint Communication on the cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace, agreed by the General Affairs Council on 25 June 2013, http://register.consilium.europa.eu/pdf/en/13/st12/st12109.en13.pdf
	Cybersecurity Strategy of the EU	Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An open, safe and secure cyberspace, JOIN(2013) 1 final, available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667
	ENISA regulation	Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, OJ L 165, 18.6.2013, p. 41–58, available at: http://data.europa.eu/eli/reg/2013/526/oj
	Directive on attacks against information systems	Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14.8.2013, p. 8–14, available at: http://data.europa.eu/eli/dir/2013/40/oj
	Framework financial regulation	Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council, OJ L 328, 7.12.2013, p. 42–68, http://data.europa.eu/eli/reg_del/2013/1271/oj
	COM Regulation 611/2013 on the measures applicable to the notification of personal data breaches	Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, OJ L 173, 26.6.2013, p. 2–8, available at: http://data.europa.eu/eli/reg/2013/611/oj
2012		

	Action Plan for an innovative and competitive Security Industry	Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee regarding an action plan for an innovative and competitive Security Industry, COM(2012) 417 final
	European cloud computing strategy	The Communication COM(2012)529 ‘Unleashing the potential of cloud computing in Europe’, adopted on 27 September 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF
	EP resolution on CIIP	European Parliament resolution of 12 June 2012 on critical information infrastructure protection — achievements and next steps: towards global cybersecurity (2011/2284(INI)), available at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167
2011		
	Council conclusions on CIIP	Council conclusions on Critical Information Infrastructure Protection ‘Achievements and next steps: towards global cybersecurity’ (CIIP), 2011, Adoption of Council conclusions, available at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST %2010299 %202011 %20INIT
	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 cybersecurity’, 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

TP-AH-19-101-EN-N

ABOUT ENISA

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

ENISA
European Union Agency for Network
and Information Security
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion Office
Nikolaou Plastira 95
Vassilika Vouton, 700 13, Heraklion, Greece

enisa.europa.eu

978-92-9204-301-8
doi: 10.2824/98700