ENISA Programming Document 2020-2022

Including Multiannual planning, Work programme 2020 and Multiannual staff planning

STATUS: DRAFT, V2

VERSION: JANUARY 2019

Document History

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

DATE	VERSION	MODIFICATION	AUTHOR
December 2018	V1	First draft sent on 12/12/2019 to MB for consultation. Feedback deadline 08/01/2019.	ENISA
January	V2	Draft V2 send for MB written approval	ENISA

About ENISA

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

Table of Contents

Foreword by the Executive Director

[To be added in a later version].

Mission Statement

The mission of ENISA has been to contribute to securing Europe’s information society by raising “awareness of network and information security and to develop and promote a culture, of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organizations in the Union”.

ENISA 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.

In 2019 the mandate[1] of the Agency is planned to be extended and the role of ENISA will be reinforced in the EU cybersecurity landscape. ENISA supports the European institutions, the Member States and the business community in addressing, responding to and especially in preventing network and information security problems. It does so through a series of activities across six areas:

- Expertise: anticipate and support Europe's knowledge in facing emerging cybersecurity challenges
- Policy: support to cybersecurity policy making and implementation in the Union.
- Capacity: support for capacity building across the Union (e.g. through trainings, recommendations, awareness raising activities).
- Cooperation: foster the EU cybersecurity community cooperation (e.g. support to the CSIRTs activities and network, coordination of pan-European cyber exercises).
- Certification: preparing candidate cybersecurity certification schemes or reviewing for digital products, services and processes.
- Enabling: reinforcing ENISA’s impact and efficiency (e.g. engagement with the stakeholders and international relations).

The area ‘Certification’ represents a new activity for ENISA and comes about as a result of the Cybersecurity Act.

In doing so, ENISA will act “*without prejudice to the competences of the Member States*” regarding their national security[2] and in compliance with the right of initiative of the European Commission. In order to achieve its mission, several objectives and tasks[3] have been attributed to ENISA, “*without prejudice to the competences of the Member States regarding network and information security and in any case to activities concerning public security, defence, national security*”[4].

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

[1] 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
[2] Article 1(2) of ENISA Regulation (EU) No 526/2013
[3] Article 2 and 3 of ENISA Regulation (EU) No 526/2013
[4] Article 1(2) of ENISA Regulation (EU) No 526/2013

ENISA’s approach is strongly impact driven, based on the involvement of all relevant stakeholder communities, with a strong emphasis on pragmatic solutions that offer a sensible mix of short-term and long-term improvements. The Agency will try to continue to provide the Union institutions, bodies and agencies (hereinafter: “Union institutions”) and the Member States services on request, based on the new mandate, to support their NIS capability development, allowing this way a more agile and flexible approach to achieving its mission.

Priorities

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

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

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

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

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

• **Operational cooperation and crisis management**: strengthening the existing preventive operational capabilities, in particular upgrading the pan-European cybersecurity exercises (Cyber Europe); supporting the operational cooperation as secretariat of the CSIRTs Network (as per NIS Directive provisions) by ensuring, among others, the well-functioning of the CSIRTs Network IT infrastructure and communication channels and by ensuring a structured cooperation with CERT-EU, European Cybercrime Centre (EC3), EDA and other relevant EU bodies in line with the Commission proposal for the Cybersecurity Act[5].

• **Support the Commission and assist Member States regarding the EU cybersecurity Blueprint** as presented in the Commission's recommendation for a coordinated response to large-scale cybersecurity incidents and crises at the EU level[6].

• **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 the field of cybersecurity certification. The draft Regulation foresees a role for ENISA in terms of preparing candidate European cybersecurity certification schemes or reviewing existing ones, with the assistance, expert advice and close cooperation of the European Cybersecurity Certification Group. Upon receiving a requests from the European Cybersecurity Certification Group or the EU Commission to prepare a candidate 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 as well as appropriate stakeholders. ENISA also supports the EU Commission in its role as Chair of the European Cybersecurity Certification Group.

[5] 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

[6] COMMISSION RECOMMENDATION (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises

Section I. General context

Threat Landscape

2018 was a year that brought significant changes in the cyberthreat landscape. 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 15 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 interest of stakeholders in such trainings is a clear indicator for their appetite in building capabilities and skills.

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 currently 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 the 2018's 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 of cyber-criminals.
- State-sponsored agents increasingly target banks by using attack-vectors utilised by cyber-crime.
- Skill and capability building are in the focus of defenders. Public organisations struggle with staff retention due to strong competition with industry in attracting cybersecurity talents.
- Technical orientation of cyberthreat intelligence is 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 assessed and analysed by means of the content of the ENISA Threat Landscape 2018 (ETL 2018). Identified open issues leverage on these trends and propose actions to be taken in the areas of policy, business and research/education. They serve as recommendations and will be taken into account in the future activities of ENISA and its stakeholders.

In the realm of all these developments, ENISA has identified numerous activities to cope with the trends of the cyberthreat landscape and increase knowledge and capability levels for various stakeholder groups. The content of the present programming document is oriented towards activities that will lead to a reduction of exposure to the assessed cyberthreats.

Policy Initiatives

Since its set up in 2004, ENISA, has actively contributed to: raising awareness of NIS challenges in Europe, the development of MS NIS capacities and the reinforcement of the cooperation of MS and other NIS stakeholders.

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

The adoption of the NIS Directive (2016) meant extending areas of action in order to accompany the evolution of NIS in Europe. In particular, ENISA plays a key role in:

- contributing to the NIS technical and operational cooperation by actively supporting Member States' CSIRTs' cooperation within the European CSIRTs Network and the NIS Cooperation Group;
- providing input and expertise into policy level collaboration between national competent authorities in the framework of the Cooperation Group,
- supporting the reinforcement of the NIS of Union institutions in strong cooperation with CERT-EU and with the institutions themselves.

In parallel, ENISA will continue to contribute to the reinforcement of NIS as a driver of the DSM and more generally of economic growth in Europe, including the development of NIS and related ICT industries in Europe.

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

The publication of the new EU cybersecurity package on 13th of September 2017, with its set of legislative and non-legislative measures, has identified ENISA as a key pillar of the EU's ambition towards the reinforcement of cybersecurity across Europe. The Communication[7] and in particular the proposed Cybersecurity Act[8].foresees the strengthening and reinforcing of ENISA.

According the press release of the European Commission announcing the agreement on the Cybersecurity Act[9], "*the Cybersecurity Act includes:*

- *A permanent mandate for the EU Cybersecurity Agency, ENISA, to replace its limited mandate that would have expired in 2020, as well as more resources allocated to the agency to enable it to fulfil its goals, and*
- *a stronger basis for ENISA in the new cybersecurity certification framework to assist Member States in effectively responding to cyber-attacks with a greater role in cooperation and coordination at Union level.*

In addition, ENISA will help increase cybersecurity capabilities at EU level and support capacity building and preparedness. Finally, ENISA will be an independent centre of expertise that will help promote high level of awareness of citizens and businesses but also assist EU Institutions and Member States in policy development and implementation.

The Cybersecurity Act also creates a framework for European Cybersecurity Certificates for products, processes and services that will be valid throughout the EU. This is a ground breaking development as it is the first internal market law that takes up the challenge of enhancing the security of connected products, Internet of Things devices as well as critical infrastructure through such certificates. The creation of such a cybersecurity certification framework incorporates security features in the early stages of their technical design and development (security by design). It also enables their users to ascertain the level of security assurance, and ensures that these security features are independently verified. […]

The new rules will help people trust the devices they use every day because they can choose between products, like Internet of Things devices, which are cyber secure.

The certification framework will be a one-stop shop for cybersecurity certification, resulting in significant cost saving for enterprises, especially SMEs that would have otherwise had to apply for several certificates in several countries. A single certification will also remove potential market-entry barriers. Moreover, companies are incentivized to invest in the cybersecurity of their products and turn this into a competitive advantage."

[7] 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

[8] 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

[9] European Commission - Press release, EU negotiators agree on strengthening Europe's cybersecurity, 10/12/2018 available at: http://europa.eu/rapid/press-release_IP-18-6759_en.htm

Section II. Multi-annual programming 2020 – 2022

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

Priorities are completed with indications on

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

Annual outputs will derive from these priorities.

Activity 1 – Expertise. Anticipate and support Europe's knowledge in facing emerging cybersecurity challenges

Multiannual priorities (2020-2022) for Objective 1.1. Improving knowledge on the security of digital developments

Priorities

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

Guidelines

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

Added-value

- provide European-wide visibility to existing NIS expertise, in particular developed at national level;
- foster convergent understanding of NIS challenges across the EU NIS community as well as best practices to address them, by offering tailored, high quality and up-to-date analysis and recommendations;
- raise awareness of operators, European institutions and national public authorities on rising security challenges that should be taken into account at technical and policy levels;
- support its work under Activity 2 (Policy), 3 (Capacity), 4 (Cooperation) and 5 (Certification) 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 (2020-2022) for Objective 1.2. Cybersecurity threat landscape and analysis

Priorities

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

Guidelines

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

Added-value

- offer an EU-wide independent synthesis on technical threats of general interest for the EU, in particular in the context of the implementation of the NIS Directive (operators of essential services, digital service providers);
- improve general awareness on threats of national and European public and private entities and bodies and foster mutual understanding by National Competent Authorities on current and future threats;
- establish a dialogue among relevant threat intelligence stakeholders in 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 analysis tailored to their needs;
- support other Activities by advising on threats that may influence EU cybersecurity;

Multiannual priorities (2020-2022) for Objective 1.3. Research & Development, Innovation

Priorities

- support Member States and the European Commission in defining EU priorities in the field of R&D and deployment.
- Participate in relevant activities promoted by with the established body set up by the proposed regulation[10] establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

[10] https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-establishing-european-cybersecurity-industrial-technology-and-research

- Capitalise on ENISA's support to Member States and economic operators for cybersecurity preparedness and resilience as well as on certification and standardisation; provide input to research and deployment priorities and formulate technical requirements.

Guidelines

- provide the secretariat of the National Public Authorities committee of ECSO (NAPAC);
- support cooperation among National Public Authorities on issues related to the definition of R&D and when relevant liaise with other stakeholders' represented within ECSO;
- participate in the activities of the European Cybersecurity Industrial, Technology and Research Competence Centre;

Added-value

- contribute to reduce the gap between research and implementation;
- provide input on cybersecurity developments in the context of the soon to be established European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

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

Multiannual priorities (2020-2022) for Objective 2.1. Supporting EU Policy Development

Priorities

- carry out a regularly updated stocktaking of ongoing and future EU policy initiatives with NIS implications and make it available to the European Commission and national NIS competent authorities;
- focus in particular on policies related to the sectoral dimension of NIS and on policies dedicated to cybersecurity in view of ensuring coherence with the framework and principles agreed upon in the NIS Directive;
- seek to identify when possible NIS challenges that may require policy developments at EU level;
- build upon this stocktaking and taking into accounts NIS challenges previously identified, offering NIS expert advice the European Commission and other relevant Union institutions on these policy developments.

Guidelines

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

Added-value

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

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

Multiannual priorities (2020-2022) for Objective 2.2. Supporting EU Policy Implementation

Priorities

- support national NIS competent authorities to work together towards the implementation of already agreed EU policies (legislations) with a NIS dimension, by allowing them to share national views and experiences and build upon those to draw consensual recommendations;
- focus on the NIS Directive in particular regarding requirements related to Operators of Essential Services (OES) (e.g. identification, security requirements, incident reporting) and on eIDAS Regulation and take account of the on NIS aspects of, GDPR (and more generally data protection) and the draft ePrivacy Regulation insofar as this reflects the ENISA regulation;
- support cybersecurity activities in the context of the implementation of the European Electronic Communications Code;
- assisting the Cooperation Group, supporting consistent NIS implementation across borders, regular reporting on the state of implementation of the EU legal framework; advising and coordinating sectorial cybersecurity initiatives in NIS sectors;

Guidelines

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

Added-value

- support Member States in implementing EU policies by making available high quality recommendations building upon the experience of the EU NIS community and reduce duplication of efforts across the EU;
- support the activities of the Cooperation Group and of the MS in relation to NIS directive implementation on a European perspective; foster the harmonized approach on implementation of EU policies and in particular legislations.

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

Multiannual priorities (2020-2022) for Objective 3.1 Assist Member States' capacity building

Priorities

- advise and assist Member States in developing national cybersecurity capacities building upon national experiences and best practices;

- focus on NIS capacities foreseen in the NIS Directive, building on ongoing activities in the CSIRTs Network and national CSIRTs which ENISA should continue to work on with the aim of fostering the strengthening of EU Member States' CSIRTs;
- develop a NIS national capacities metrics, building upon capacities foreseen in the NIS Directive, allowing an assessment of the state of NIS capacity development within the EU;
- identify and draw recommendations on other national NIS capacities which the spread across the EU NIS community would contribute to reinforcing the NIS of the EU, e.g. national cybersecurity assessments, PPPs such as in the field of CIIP, national information sharing schemes, etc.
- Providing support to the establishment of national and European Information Sharing and Analysis Centres (ISACs) in various sectors;

Guidelines

- carry out a regular stocktaking of national NIS capacity initiatives with a view to identify trending developments in view of collecting and analysing different approaches and practices;
- liaise closely with national NIS competent authorities' experts to identify experience and best practices on national NIS capacity developments;
- take into account developments and recommendations that may arise from the CSIRTs network as well as the Cooperation Group;
- adopt a holistic approach of NIS capacities ranging from technical to organizational and policy level;
- while creating general NIS capacity metrics, seek in priority to identify main trends at the EU level and advise individual Member States upon their request;
- explore the development of tools and initiatives with a view to making ENISA's recommendations more visible and to increase their impact (e.g. summer school, onsite trainings);
- offer advice on how to improve private-private exchanges of information (e.g. via ISACs) and on an ad hoc basis and, without prejudice to achieving its priorities under this objective, continue to support specific European ISACs;

Added-value

- continue to support the development of national NIS capacities reinforcing the level of preparedness and response capacities of Member States thus contributing to the overall cybersecurity of NIS across the EU;
- foster sharing of best practices among Member States;
- structured cooperation with CERT-EU to provide technical assistance to Member States in case of significant incidents and to support incident analysis; providing assistance upon request to Member States to handle incidents and analyse of vulnerabilities, artefacts and incidents;
- facilitate cooperation between individual Member States in dealing with emergency response by aggregating national situational reports based on information made available to the Agency by Member States;
- indirectly contribute to capacity building of governments beyond the EU by making its recommendations and training material available on its website, thus contributing to the international dimension of its mandate;
- in the context of CSIRTs, contribute to its work under Activity 4 by supporting the development of CSIRTs maturity as well as tools (e.g. in the context of CEF) benefiting to the cooperation within the CSIRTs network and the development.

Multiannual priorities (2020-2022) for Objective 3.2 Assist in the EU institutions' capacity building

Priorities

- representation by ENISA on the Steering Board of CERT-EU of the EU Agencies
- Cooperation with relevant EU agencies on initiatives covering NIS dimension related to their mission;
- provide (upon request and in coordination with the institutions) capacity building support for trainings, awareness, and development of education material.

Guidelines

- Liaison with EU agencies on defining NIS requirements;
- capacity building through regular interactions (e.g. annual workshop)in cooperation with the ICT Advisory Committee of the EU Agencies ;
- partner with CERT-EU and other EU institutions and agencies (e.g. EC3, EDA, EEAS, EASA) and other bodies with strong NIS capabilities in view of supporting its actions under this objective;
- reinforce links between Union institutions and agencies and other bodies and cooperate in dissemination activities linked to cybersecurity capacity building and general cybersecurity awareness;

Added-value

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

Multiannual priorities (2020-2022) for Objective 3.3 Awareness raising

Priorities

- Work together with the relevant national authorities to advise private sector on how to improve their own NIS through the elaboration of key recommendations for the cybersecurity of the private sector;
- support information sharing among public and private sectors on NIS developments at European level;
- organize the European Cybersecurity Month (ECSM) and the European Cybersecurity Challenge (ECSC) with a view to making these events a venue for EU cybersecurity awareness raising; pooling, organising and making available to the public, through a dedicated portal, information on security of network and information systems, in particular cybersecurity, provided by the EU institutions, agencies and bodies;
- carry out regular stocktaking of national awareness raising initiatives;
- build upon this stocktaking and in liaison with the ECSM and ECSC, analyse and provide recommendations and advice on best practices in the field of awareness raising, in particular with regard to communication activities;

Guidelines

- build upon existing work done at national level in relation with the private sector on the basis on regular stocktaking of national expertise on this issue (e.g. cyber hygiene) as well as upon its work under Activity 1 to offer high-quality, up-to-date and high value recommendations to the benefit of the EU NIS community;

- adapt its recommendations to specific target audiences (SMEs, large size enterprises, NIS experts or non-experts) and adopt a holistic approach of NIS capacities ranging from technical/operational to organizational and policy capacities;
- establish a structured and sustainable (multiannual) dialogue with volunteer national NIS competent authorities' experts on awareness raising and communication, responsible for the national dimension of the ECSM and ECSC; explore ways of using adapted communication channels within the framework of the ECSM and ECSC;
- adopt a holistic approach to awareness raising and adapt its recommendations to specific target audiences, from the citizens to public authorities;

Added-value

- raise awareness within the private sector on the need to reinforce their NIS;
- support the development of the NIS of businesses across the EU and support national NIS competent authorities in their similar efforts towards private sector, thus contributing to raising the level of the overall cybersecurity of NIS across the EU;
- allow the organization of EU-wide events, increasing visibility on cybersecurity and on ENISA with the EU citizens, businesses, academia and the NIS community, including NIS students;
- foster harmonization of tailored awareness raising messages across the EU with increased impacts, building upon the strengths of existing national initiatives thanks to the sharing of best practices among them;
- strengthen cooperation among the Member States;
- facilitate the development of national awareness raising initiatives on a national level.

Activity 4 – Cooperation. Foster the operational cooperation within the European cybersecurity community

Multiannual priorities (2020-2022) for Objective 4.1 Cyber crisis cooperation

Priorities

- further develop and organize Cyber Europe 2020, exploring new dimensions and formats with the aim of further preparing the Member States and Union institutions to cyber crises likely to occur in the future in the EU;
- integrate existing and future EU-wide crisis management orientations, mechanisms, procedures and tools within the framework of Cyber Europe exercises, in particular the CSIRTs network foreseen in the NIS Directive and the Cooperation Group;
- contribute actively to the implementation of the blueprint by supporting MS in integrating into national crisis management frameworks EU-level orientations, mechanisms, procedures and tools; the Agency will contribute to develop a cooperative response, at Union and Member States level, to large-scale cross-border incidents or crises related to the cybersecurity through a series of tasks from contributing to establish a wide situational awareness across the Union to testing the cooperation plans for incidents;
- integrate existing and future EU-wide crisis management orientations, mechanisms, procedures and tools within the already existing crisis management framework of the MS;
- follow up closely the development of the CEF Cybersecurity DSI CSP and ensure the smooth handover to ENISA and adoption by the CSIRT community;
- proactively develop its expertise in the field of cyber crisis management and exercises in cooperation with other Union institutions and Member States wishing to develop exercises with a cyber dimension. In doing so, ensure consistency with the Cyber Europe framework;

Guidelines

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

Added-value

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

Multiannual priorities (2020-2022) for Objective 4.2 Community building and operational cooperation

Priorities

- provide the secretariat to the CSIRTs network foreseen in the NIS directive;
- ensure, among other things, the well-functioning of the CSIRTs Network IT infrastructure and communication channels. Ensure structured cooperation with CERT-EU, EC3 and other relevant EU bodies;
- take advantage of the development of the CSIRT core platform within the framework of the “Connecting European Facility” (CEF) mechanism to support the functioning of the CSIRTs network and advice, upon request, Member States’ CSIRTs on projects to be proposed within the framework of future CEF call for projects;
- reinforce the role of the Single Point of Contact (NISD), having into account that is used to exercise a liaison function to ensure cross-border cooperation of MS;

Guidelines

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

Added-value

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

Activity 5 – Certification. Develop cybersecurity certification schemes for digital products, services and processes

Multiannual priorities (2020-2022) for Objective 5.1 Support activities related to cybersecurity certification

Priorities

- support the work undertaken within the EU Cybersecurity Certification Framework;
- making available to designated stakeholders and the general public, information on cybersecurity certification schemes through a dedicated portal;
- Support the EU Commission in its role as Chair of the EU Cybersecurity Certification Group;
- Support the Stakeholder Cybersecurity Certification Group;

Guidelines

- providing analysis of the main trends in the cybersecurity market; market observatory;
- maintaining content on a dedicated website;
- development and maintenance of information on the EU cybersecurity certification framework, through a dedicated portal; portal and associated IT system maintenance;
- Organise stakeholder consultations and/or contributions regarding candidate schemes.

Added-value

- support Member States in implementing EU policies by making available high quality recommendations building upon the experience of the EU NIS community and reduce duplication of efforts across the EU; making available to the public up to date information on the certification schemes;
- support the deployment of the EU Cybersecurity Certification framework;
- support cooperation between all stakeholders connected to the EU Cybersecurity Framework, including industry, governmental bodies, standardisation bodies, etc.

Multiannual priorities (2020-2022) for Objective 5.2 Developing candidate cybersecurity certification schemes

Priorities

- support the work undertaken within the EU Cybersecurity Certification Framework, including providing technical expertise to prepare candidate European cybersecurity certification schemes in functional application areas e.g. Cloud, IoT, etc.;
- support to Union policy development and implementation regarding standardisation, certification and Market Observatory;
- facilitating the take-up of risk-management standards of electronic products, networks and services and advise the relevant cybersecurity certification framework stakeholders on technical security requirements;

- focus on policies dedicated cybersecurity security certification, in view of ensuring coherence with the framework and principles agreed upon in the draft Cybersecurity Act.

Guidelines

- foster dialog in the context of the work undertaken within the Certification Framework, including providing technical expertise to prepare candidate European cybersecurity certification schemes;

Added-value

- Support to Union policy development and implementation on standardisation (European and international, as appropriate) and certification.
- Contribute to the implementation of the draft Cybersecurity Act, according to the tasks assign to the Agency

Activity 6 – Enabling. Reinforce ENISA's impact

Multiannual priorities (2020-2022) for Objective 6.1 Management and compliance

Priorities

- Optimize talents acquisition and retention with the aim of achieving ENISA mandate;
- mature management skills in ENISA and assure adequate working environment and staff wellbeing;
- lean, secure and compliant administration using best practices and tools;
- Staff skills development, embracing the future Agency needs, in line with EU needs in the area of cybersecurity;
- 100% compliance in our financial and legal framework;
- Assessment and deliver the Agency's business needs and internal strategy;

Guidelines

- propose the alignment of the multiannual staff policy plan with the internal expertise's needs necessary to achieve ENISAs mandate objectives;
- improve recruitment effectiveness and internal process, in particular in view of accelerating and smoothing the recruitment process, thus contributing to improving ENISA's internal expertise;
- promote the development of sustainable team-work among ENISA's staff members;
- enhance the recruitment of Second National Experts;
- continue to improve processes for monitoring financial flows and expects to maintain high commitment and payment rates to guaranty full implementation of WP and compliance;
- adopt sophisticated finance management tool;
- enhance IT security for ENISA systems and be the state of art in cybersecurity for ENISA internal systems;
- upgrade ENISA management maturity level;
- enhance the Quality Management System in ENISA

Added-value

- improve the general quality and efficiency of ENISA's activities by strengthening the Quality Management System of the Agency;
- Reduce risks in the Agency in several activities and management and optimize the use of financial and human resources. .

Multiannual priorities (2020-2022) for Objective 6.2 Engagement with stakeholders and international relations

Priorities

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

Guidelines

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

Added-value

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

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

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

Human and financial resource outlook for the years 2020-2022

Annex A1 provides the outlook of resources and budget allocation for 2020. Also, it contains a brief description on trend regarding allocation of resources and budget for the new tasks.

Section III. Work Programme Year 2020

The ENISA Work Programme for the year 2020 follows the lay out presented in the multi-annual programming Section II. In this section objectives, results and indicators are identified in relation to each activity. After a short description of the activity the objectives are presented. A short narrative is included, consisting of a description and added value of the activity, the main challenges for 2020 and link to the multi-annual objectives.

The main outputs/ actions in the specific year, for this case for 2020, are listed within each objective. For each objective there are several outputs defined. For each output, the following are included in this document:

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

In the preparation of Work Programme 2020, ENISA assumes that the new ENISA regulation will be in place by latest mid-2019, and covers new tasks and activities using resources as proposed in the draft Cybersecurity Act COM (2017)477.

Activity 1 – Expertise. Anticipate and support Europe’s knowledge in facing emerging cybersecurity challenges

Objective 1.1. Improving knowledge on the security of digital developments

Output O.1.1.1 – Building knowledge on the security of Internet of Things

The Agency has been working on IoT security for a number of years, producing among else work on baseline IoT security recommendations[11] (WP2017), as well as sectorial work in Industry 4.0/smart manufacturing[12] (WP2018), and secure development guidelines (WP2019), etc. With a great impact on citizens’ safety, security and privacy, the IoT threat landscape is extremely complex and wide. 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.

[11] See https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[12] See https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

Building on its previous work on IoT security, the Agency will identify and analyse existing IoT security practices, national expertise, regulatory initiatives and standards that aim at protecting the IoT ecosystem as a whole. The Agency will map the evolving threat landscape and compare these practices and standards and develop guidelines for the security of the Internet of Things focusing on its impact on the consumers as well as the overall supply chain (for example 3rd party dependencies, integration of components, etc.) – particularly in the context of Industry 4.0 and smart infrastructures.

To satisfy these goals, the Agency will take into account and contribute to existing EU policy and regulatory initiatives (the NIS Directive, the Internet of Things - An action plan for Europe[13], the Communication on Building strong cybersecurity for the EU[14], the Public Private Partnership (PPP) on cybersecurity[15], etc.). ENISA will liaise with relevant stakeholders (public and private sector, as well as EU funded IoT research projects) and EU initiatives (e.g. AIOTI).

The Agency will consider developing targeted IoT case studies to identify risks and attack scenarios, as well as providing relevant recommendations and good practices. Accordingly, it will consider defining e.g. IoT secure procurement guidelines to support consumers, IoT supply chain security guidelines, or other means to promote awareness and to ensure “security for safety”.

ENISA will also validate the results of the study (e.g. via joint workshops) with relevant IoT stakeholders.

Output O.1.1.2 – Building knowledge on the security of Connected and Automated Mobility (CAM)

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

The Agency will build on its previous work on smart cars[16] (WP2016, WP2019) and will monitor security practices and standards in the area of smart cars (e.g. UN-ECE dedicated TF on CYBER, ISO/SAE standardisation work) considering the emerging notions of connectivity and autonomy. ENISA will examine the security challenges arising from the deployment of connected and autonomous vehicles, as well as issues such as V2V and V2X communications. ENISA will review these practices and standards and highlight or suggest good practices and potential legislative action required for security of smart cars focused on safety and the issues of connectivity and autonomy.

To assist the Commission and the Member States in achieving these objectives the Agency will consider and contribute to existing EU policy and regulatory initiatives (the NIS Directive, the European strategy on Cooperative Intelligent Transport Systems[17], the C-ITS Platform of DG MOVE[18], the High Level Group GEAR

[13] See See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2009:0278:FIN
[14] See http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN
[15] See https://ec.europa.eu/digital-single-market/en/news/commission-decision-establish-contractual-public-private-partnership-cybersecurity-cppp
[16] See https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars
[17] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0766
[18] See https://ec.europa.eu/transport/themes/its/c-its_en

2030[19]), as well as the planned Commission Recommendation on CAM, the 3rd Mobility package[20] and the Communication on Connected and Automated Mobility (CAM) and the relevant work of Euro NCAP.

To ensure an aligned approach across Member States, the Agency will support their work under the NIS Cooperation framework for the identification of the operators of essential services in the transport sector and the establishment of common follow-up processes regarding cyberattacks against road infrastructures.

The Agency will also validate the results of the study (e.g. via joint workshops) with relevant smart cars stakeholders from public sector such as the relevant European Commission service, JRC, national road authorities, and from the private sector including automotive manufacturers, OEMs, together with other key stakeholders from the CAM ecosystem.

Output O.1.1.3 – Building knowledge on Artificial Intelligence security

Artificial Intelligence (AI) technologies facilitate intelligent and automated decision-making and are thus a prerequisite to the deployment of IoT and Industry 4.0 scenarios, as well as other application areas. Interesting showcase examples of AI include smart manufacturing (robotics), autonomous driving, smart cities, etc. Whereas undoubtedly beneficial, one should not sidestep the fact that AI and its application on automated decision making –especially in safety critical deployments such as in autonomous vehicles-might open new avenues in manipulation and attack methods.

When considering security in the context of AI, one needs to consider that AI can be exploited to manipulate the expected outcomes, but also that AI techniques can be utilised to support security operations. Accordingly, adversarial techniques to manipulate AI algorithms are emerging and therefore relevant risks need to be managed. Conversely, AI is emerging as being a highly significant tool in the area of cyber-security, since it can be used to identify attack patterns and thus facilitate security management/policy implementation supervision.

The Agency will conduct a preliminary study on the challenges related to AI security considering relevant issues, risks and solutions. In doing so, the Agency will map relevant stakeholders and engage the wider community and will validate the results of the study (e.g. via joint workshops) with relevant national and EU initiatives and interact with AI stakeholders from the public sector such as the relevant European Commission services, etc.

Output O.1.1.4 – Building knowledge on the security of Healthcare services

Recent cybersecurity incidents have shown that healthcare is one of the most vulnerable sectors. Previous ENISA studies have highlighted that the healthcare sector has a relatively low level of maturity concerning cyber security. Newly adopted EU legislations have indicated that there has been a shift in priorities: the NIS Directive defines healthcare organisations as operators of essential services, the Medical Devices Regulation[21] (MDR) includes obligatory safety and security provisions for medical devices and the EC

[19] See https://ec.europa.eu/growth/content/high-level-group-gear-2030-report-on-automotive-competitiveness-and-sustainability_en
[20] See https://ec.europa.eu/transport/modes/road/news/2018-05-17-europe-on-the-move-3_en
[21] https://ec.europa.eu/growth/sectors/medical-devices/regulatory-framework_en

Communication on enabling digital transformation of health care in the Digital Single Market[22] as described in 2018 communication of the European Commission on Data Package[23].

The Agency, based on previous experience, will support Healthcare organisations in enhancing their cyber security level by helping them assessing risk in the healthcare information systems. This work will enable Healthcare organisations to identify vulnerabilities and evaluate risks for all assets in the healthcare ecosystem. The agency will consider assessing implementation scenarios , e.g. ePrescription systems, remote patient healthcare, proactive/predictive approaches to healthcare, mHealth, Cloud and big data for healthcare services (list is indicative). The goal is to provide a collection of common practices for ensuring cybersecurity in interoperable hospital systems and related care environments.

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

This work builds on previous work of ENISA in the areas of Healthcare security (WP 2015, WP 2019), Smart Hospitals (WP 2016) and NIS Directive implementation (WP 2017, WP 2019).

Output O.1.1.5 – Building knowledge on maritime security

The maritime sector plays a key role in the EU economy and society, accounting for a large segment of Europe’s overall freight and passenger transport. However, as the sector has been steadily undergoing a digital transformation with the introduction of innovative solutions based on ICT, the cyber risk profile has also changed. Combined with a significant increase in cyber-attacks against key maritime actors such as ports and shipping companies, this change highlights the need for maritime cybersecurity to be addressed in more detail.

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

ENISA will interact with relevant key stakeholders from the public sector, such as DG MOVE and EMSA and from the private sector, such as managing bodies of ports, port facilities, water transport companies, operators of vessel traffic services and ICT product and service vendors to collect information and validate the study findings.

This work builds on previous work of ENISA in the areas of maritime (WP2011, WP2019), intelligent transportation systems (WP 2015) and smart critical infrastructures (WP 2016).

[22] https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering
[23] http://europa.eu/rapid/press-release_IP-18-3364_en.htm

Output O.1.1.6 – Building knowledge on cryptographic algorithms

In the revised Cybersecurity strategy of the EU published in September[24], the European Commission highlights "[…] the lack of European capacity on assessing the encryption of products and services used by citizens, businesses and governments within the Digital Single Market. Strong encryption is the basis for secure digital identification systems that play a key role in effective cybersecurity […]". Furthermore, in Article 10 of its proposal for a Regulation of the European parliament and of the Council on ENISA, the "EU Cybersecurity Agency", repealing Regulation (EU) 526/2013, of 13 September 2017 the European Commission is calling ENISA to *"[…] advise the Union and the Member States on research needs and priorities in the area of cybersecurity, with a view to enabling effective responses to current and emerging risks and threats, including with respect to new and emerging information and communications technologies, and to using risk-prevention technologies effective"*". One of the most important technologies that is satisfying the criteria of a security enhancing technology as well as privacy enhancing technology is encryption.

While acknowledging the importance of crypto technologies with regard to cyber security, particularly encryption is still a key area of national security, especially when it comes to the protection of sensitive governmental systems as well as critical information infrastructures. To harmonise both - market needs and Member States responsibilities - it is essential to work together on sharing existing approaches, best practices and knowledge. In international standardisation, technical specifications for cryptographic algorithms already exist which should be considered at European level, too. Moreover, at the European level the so called SOGIS-MRA Crypto catalogue[25] is already a major achievement as a first comprehensive collection of cryptographic means agreed on by participating Member States' competent authorities.

Working closely with the Member States, ENISA will act as a catalyst to raise awareness on already existing cryptographic means based on a wider promotion of the SOGIS catalogue. Especially in light of the new EU certification framework where ENISA plays a significant role, ENISA will continue in 2020 the discussion with the existing SOGIS crypto working group on possibilities of a long-term relationship and exchange. ENISA will continue to participate in respective meetings of the group.

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

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

[24] 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

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

Objective 1.2. Cybersecurity Threat Landscape and Analysis

Output O.1.2.1 – Annual ENISA Threat Landscape

The annual ETL report

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

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

The dissemination, concise presentation and online availability of cyberthreat intelligence will be in the focus in 2020. Available cyberthreat intelligence will be interlinked with other related ENISA results (see also chapter Multiannual priorities (2020-2022) for Objective 1.2. NIS threat landscape and analysis).

In this manner, ETL stakeholders will be in the position to access and interact with ENISA cyberthreat information on a permanent basis. In 2020, ENISA will continue the cooperation with CERT-EU in the area of Threat Landscaping. This effort will be carried out in conjunction with the relevant working group in the CSIRTs Network by means of information exchanges, use of CERT-EU services and organisation of common meetings/events. In carrying out this work, synergies with related experts (i.e. ENISA ETL Stakeholder Group) and vendors (through MoUs) will be maintained and expanded.

CTI EU Event

In 2020, ENISA will continue supporting the relevant Cyberthreat Intelligence stakeholder community by supporting CTI good practices and by providing an interaction platform. This is the main instrument of mobilization of CTI stakeholders; it will be engaged in the dissemination of ENISA CTI information of all kinds (e.g. Info Note).

Maturing the European Cyber-threat Intelligence Practice

Building on its previous work analysing current and emerging threats, ENISA shall promote good practices in the area of Cyber-threat Intelligence (CTI) by means of defining a capability framework and a maturity model, in collaboration with the Stakeholder’s Community.

ENISA will prepare a CTI capability framework providing hands-on guidelines on how organizations can revise their cyber resilience strategies by introducing technical and non-technical context into their defence capabilities. The proposed framework consists in a practical tool that helps organizations of any size and sector establishing a well-defined CTI Program, with concrete requirements, a clear process, outputs and metrics to evaluate the impact. The aim of this tool is to promote a shift from reactive to a proactive cybersecurity posture by including cybersecurity into organization’s business and risk strategies.

In addition to the above, ENISA will prepare a CTI Maturity Model with practical guidelines on how to evaluate the state of play of the CTI Program within an organization of any size and sector. The purpose of this tool is to help organizations to self-assess and evaluate their CTI Program maturity and ultimately define a roadmap for continuous improvement.

ENISA shall promote knowledge and experience sharing activities among members of the Cyber-threat Intelligence Community. As a key initiative, ENISA will organize an annual meeting/event (CTI-EU), mobilizing experts, academics and the industry, to debate and envision the future of Cyber Threat Intelligence (CTI) as a key practice.

Reporting on Emerging Cybersecurity Threats

ENISA will identify good practices in the area of technological foresight and horizon scanning to support the research of emerging cybersecurity challenges and threats relevant to organizations of any size and sector. From the outcome of this research, ENISA will present a methodology and practical guidelines streamlining a process to construct informed representations of possible futures trends and scenarios. ENISA expects that with the adoption of such methodology, organizations will promote internal awareness on emerging cybersecurity challenges and threats and define early mitigation strategies.

Using the abovementioned methodology, ENISA will analyse and report on emerging cybersecurity challenges and threats through an annual research program. The consideration of future technological trends and challenges is part of the ENISA planning and knowledge management process. The outcome of this research aims at facilitating the decision making process in setting priorities for future ENISA work programs and defining thematic areas aligned with social and economic needs of citizens and organizations. The ENISA report on Future Cybersecurity Challenges and Threats is essentially a source of information about emerging technologies trends that may potentially lead to security challenges and constrains from its adoption and adaptation. The report presents possible mitigation strategies and existing emerging security solutions attempting to anticipate threats and minimize its impact. To produce this report, ENISA will apply a year-long research process involving the input from a variety of sources and contributions from members of Expert and Stakeholders groups that includes researchers, academia, representatives from the civil society and industry. ENISA expects that this report will promote extensive discussion and sufficient awareness around the topics, within the cyber security community and the society as whole.

Output O.1.2.2 – Restricted and public Info notes on cybersecurity

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

CSIRT Info Notes

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

General Info Notes

General info notes cover significant developments and announcements in the field of cyber security with the sole purpose of promoting general awareness and presenting actionable mitigation strategies. General info notes are not a response to incidents or vulnerabilities but rather explanatory reviews, neutral and independent analysis of major 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 unbiased information regarding such events, covering issues, points of action, mitigation measures, summaries, related practices, etc. Hence, the objectives of this work are to provide a neutral overview of the state-of-play and promote awareness to the essence of the threat in analysis at a near-time manner.

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

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

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

Output O.1.2.3 – Support incident reporting activities in the EU

As EU level incident reporting obligations have been introduced under multiple type of legislative instruments, developing efficient reporting schemes across sectors and across geographical borders, is one of the objectives of the activities developed by ENISA in this sector. Such reporting schemes should remain simple, pragmatic and relevant for both public and private sector without increasing the cost of operation.

Current and foreseen activities in this area include:

- Incident notification in the telecom sector (Article 13a of the Telecoms framework directive, to be replaced by Article 40 of the EECC); currently ENISA facilitates the activities of the Article 13a Expert Group, which discusses general supervision of security in the telecom sector and maintains annual summary reporting about telecom incidents. ENISA in this context works closely with several industry groups and supports the Article 13a expert group with analysing cross-cutting security issues. The new EU Electronic Communications Code (EECC) due to be adopted will require major work and support, because the scope of supervision and the scope of security breach reporting is extended.
- Incident notification for the trust services sector (Article 19 of the eIDAS regulation): Electronic trust services is a growing sector and increasingly important with many cross-border dependencies. ENISA plays a key role by collecting and analysing security incidents from across the EU. In 2020 ENISA will analyse security incidents and produce a consolidated, anonymised annual report. In addition, ENISA will develop lessons learnt from past incidents and recommend good practices, in collaboration with the Member States. In this context ENISA engages also with the private sector and with relevant fora like FESA and the eID expert group.
- Incident notification under the NIS Directive: In 2018 ENISA provided templates. ENISA will work with the Commission and MS to exploit synergies in the different notification schemes. ENISA will also develop sectorial approaches to incident notification to best suit the individual sectors. In this context ENISA shall support the efficient flow of information about mandatory incident notifications and voluntary incident notifications to establish a common picture across sectors and across the EU.

ENISA has significant expertise on ***incident reporting*** at the EU level through the work carried out with Member States and telecoms providers on the transposition of Article 13a of the Telecommunications Framework Directive of 2009, and Article 19 of the eIDAS regulation.

Output O.1.2.4 – Supporting the operational sectoral implementation of the NIS Directive

For this particular output, ENISA will produce good practice for sectoral CSIRTs and product CSIRTs (PSIRTs) to support operational capabilities development according to the Annex I of the NIS Directive.

In addition to the above, the Agency will also organise a validation workshop with EU, Member States and sectorial stakeholders to present the results and gather feedback on current experience with multi-stakeholders approach on incidents, threats and vulnerabilities.

ENISA will also support the dissemination of operational sectoral good practices. This will enable stakeholders to better adopt NISD CSIRT requirements in their business, reinforce cooperation with product CSIRTs (PSIRT). All this will enable more efficient incident management practices and will thus contribute to a more proper, more agile adaptation to the multi-stakeholders collaboration on incidents, threats and vulnerabilities in EU.

Objective 1.3. Research & Development, Innovation

Output O.1.3.1 – Supporting EU research & development programmes

ENISA will continue providing analysis of the areas covered by the NIS Directive, the Cybersecurity Package, the COM decision on cPPP and the outcomes of relevant Horizon2020 projects e.g. the CSA projects (cyberwatching, AEGIS and EU-Unity) and will aim to show where R&D activities funded in the context of H2020, , TRANSITS and GEANT would achieve the greatest impact. On cybersecurity aspects related to the General Data Protection Regulation, ENISA will work in close cooperation 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 look into adapting the current best practices and guidelines for protecting EU systems and networks, services, IoT and cloud ecosystems and supply-chains according to the evolving threats. As well as building specific used cases that can be adopted by the IT Security community.

Additionally, ENISA will continue supporting and advising the Commission and organisations in this area, other agencies (e.g. EDA, ESA), industrial communities as well as in the Member States to meet their goals by bringing in its concrete NIS policy expertise. Such relevant contributions will also be made regarding the proposal on the creation of the Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre[26]. In this context ENISA will collaborate closely with the European Cybersecurity Research and Competence Centre to be set-up in the context of this work.

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

Summary of outputs and performance indicators in Activity 1 Expertise

Summary of Outputs in Activity 1 – Expertise. Anticipate and support Europe's knowledge in facing emerging cybersecurity challenges		
Outputs	**Type of output (P=publication, E=Event, S=Support)**	**Performance indicator**
Objective 1.1. Improving knowledge on the security of digital developments		
Output O.1.1.1 –Building knowledge on the security of Internet of Things	P: Guidelines for securing the Internet of Things, Q4 E: Validation cyber security workshop, Q3-Q4 E: Joint ENISA – Europol Conference on IoT Cyber Security, Q3-Q4 S: Support the EC, MS and IoT stakeholders in major EU initiatives, Q1-Q4	Engage 10 IoT stakeholders from 5 EU MS in the preparation of the study (P) and/or validation workshop (E)
Output O.1.1.2 –Building knowledge on the security of Connected Automated Mobility (CAM)	P: Recommendations for the security of CAM, Q4 E: CAM security workshop, Q3-Q4 S: Support the Commission, MS and automotive industry to holistically address cyber security of CAM in relevant policy initiatives, Q1-Q4	Engage 5 automotive manufacturers and 5 CAM stakeholders from 5 EU MS in the preparation of the study, i.e. publication (P) and workshop (E)
Output O.1.1.3 – Building knowledge on Artificial Intelligence security	P: Artificial intelligence: Cybersecurity challenges, Q4 E: Artificial intelligence security workshop, Q3-Q4	Engage 10 stakeholders in the preparation of the publication (P) At least 20 stakeholders participating in the workshop (E)
Output O.1.1.4 - Building knowledge on the security of Healthcare services	P: Good practices for assessing cybersecurity risks in healthcare organisations, Q4 S: Support EU healthcare organisations in identifying risks in their systems, Q1-Q4 E: Annual eHealth workshop, 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 – Building knowledge on maritime security	P: Guidelines for cyber security in the maritime sector, Q4 E: Maritime cyber security workshop, Q3-Q4 S: Support the Commission, MS and maritime industry to holistically address cyber security of the maritime sector, Q1-Q4	Engage 10 maritime sector stakeholders from 5 EU MS in the preparation of the study (P) and/or the workshop (E)
Output O.1.1.6 – Building knowledge on cryptographic algorithms	S: Support work in the area of cryptography and participation in SOG-IS and ETSI related groups/meetings, Q1-Q4.	2 news items or dissemination materials published covering public documents and activities of the groups/meetings attended.
Objective 1.2. Cybersecurity 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. E: ENISA will organise the annual event on Cyberthreat Intelligence EU (CTI EU), Q3-Q4	Engage more than 10 MS in discussions and work related to the structure and content of ENISA Threat Landscape. More than 5.000 downloads of the ENISA Threat Landscape report. Engagement of more than 80 CTI experts from industry, academia and Member States.
Output O.1.2.2 – Restricted and public Info notes on NIS	P: Info notes on NIS, Q1-Q4	Coverage of all major incidents relevant to EU NIS policy priorities. Expand coverage to all key ENISA stakeholder groups.

Output O.1.2.3 – Support Incident reporting activities in the EU	P: Annual Incident Analysis Report for the Telecom Sector, Q4 E: Three workshops for the Art. 13a[27] working group P: Short Position Paper - Analysis of a technical topic requested by the Art. 13a EG, Q1-Q4 P: Annual Incident Analysis Report for the Trust Service Providers, Q4 E: Two workshops for the Art. 19[28] meetings S: Support MS and the EC in implementing NISD incident reporting requirements. P: Good practices for further development of the NISD incident notification frameworks across EU, Q4	More than 20 NRAs/EU MS contribute in preparation of the report (Art. 13a) (P) More than 10 SBs/EU MS contribute in preparation of the report (Art. 19) (P) Engage more than 10 MS in discussions and work related to implementing particularities of the NISD incident reporting framework (S).
Output O.1.2.4 - Supporting the operational sectoral implementation of the NIS Directive	P: good practice on sectoral CSIRT capabilities (per critical sectors and PSIRTs) E: validating workshop with EU MS and sectoral CSIRTs/PSIRTs, Q4	Engage sectoral CSIRTs and PSIRTs in MS
Objective 1.3. Research & Development, Innovation		
Output O.1.3.1 – Supporting EU research & development programmes	S: Support for EU Cybersecurity Competency Centres. Tbd.	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 – Supporting policy developments in NIS Directive sectors

While the NIS Directive addresses elements of cybersecurity in different sectors (OESs and DSPs), there are several initiatives at EU and MS level that involve cybersecurity and are orthogonal to the work conducted in the context of the NIS Directive. An indicative yet not exhaustive list of examples includes the work from DG MOVE on the Cooperative Intelligent Transport Systems (C-ITS), the work from EASA on the introduction of requirements for the management of information security risks by organisations involved in civil aviation activity, the work from DG FISMA and ECB on finance-related regulations, DG GROW on the Medical Devices Regulation (MDR), the work of DG SANTE in the eHealth Network (eHN) and the Joint Action Plan, as well as forthcoming work from DG ENER on cybersecurity for the energy sector to name a few.

Taking due account of recent legislative and policy developments in sectors that are defined in the NIS Directive (OESs and DSPs), ENISA will work with the European Commission, Member State and EU Agencies to promote harmonised and coordinated efforts towards sectoral cybersecurity in the EU. Any planned activity in the area of cybersecurity in sectors of the NIS Directive that is foreseen in the WP will respect existing EU and national efforts and interests, while taking into consideration the ongoing legislative process.

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

The Agency will provide support to the Commission and the Member States in the policy area related to sectors of the NIS Directive, by conducting a stock taking of the different initiatives taking place in the different sectors. In doing so the Agency will map policies affecting the NISD sectors and the role and responsibilities of involved actors. The results of this mapping of the policy landscape will be validated with all related stakeholders. Moreover, the Agency will upon request support the development of relevant policy initiatives with the aim to ensure coordinated efforts across the EU.

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 risk, assurance and technology aspects as building blocks for the delivery of dependable trust and electronic identification services. Aspects to be covered will be agreed with the EU Commission and Member States through the eIDAS experts group. Interacting with private sector actors will enhance the ability of the Agency to make further meaningful contributions to this area. In implementing the Cybersecurity Act, ENISA will support in terms of analysis the efforts of the Member States and the Commission in the area of electronic identity. To produce specific implementation guidelines and technical recommendations a number of stakeholders and collaboration areas will be consulted in order to address operational aspects of trust service providers, conformity assessment bodies and supervisory authorities while leveraging on past experience to emphasise implementation and interoperability. Towards an effort to exchange information and share best practices, ENISA will collaborate closely with the eIDAS Expert Group (Trust Services) and the Cooperation Network (established by the Commission Implementing Decision 2015/296). These recommendations will complement the existing knowledge base that ENISA created for the trust service providers.

ENISA will take account of recommendations and standards being developed by CEN/CENELEC, ETSI and the ISO and IEC and seek to avoid both duplication of work and potentially conflicting approaches. In this regard, ENISA will support the European Commission to assess applicable standards by reviewing to what extent they meet the requirements of the eIDAS Regulation. Furthermore, ENISA will continue to support the European Commission in the implementation of specific areas of interest such as qualified time stamps, qualified website authentication certificates, mobile applications etc., as appropriate. Lastly, ENISA will support the European Commission on implementation aspects and tasks related to Article 49 of eIDAS.

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

ENISA will support the European Commission and the Member States in delivering the NIS Cooperation Group's 2018-2020 work programme. In this context ENISA will also analyse specific issues and draft working papers, consult with Member States' competent authorities, collect and develop good practices recommendations supporting the NIS Cooperation group.

ENISA will leverage its expertise in Critical Information Infrastructure Protections, National Cyber Security Strategies, CSIRTs, security assessment frameworks, baseline security requirements and incident notification in different critical sectors (such as energy, transport, finance etc.), standardisation, ICT certification and others to contribute to the different work streams of the Cooperation group. Contribution refers to both the existing and ongoing work streams on e.g. security measures, incident reporting, energy sector security, large scale incident taxonomy, etc., as well as forthcoming ones that will be specified and aligned to the work programme of the Cooperation group upon its finalization.

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

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

Output O.2.2.3 – Contribute to the EU policy in the area of privacy and data protection with input on cybersecurity related measures

Within the scope of its cybersecurity mandate, ENISA will support trust and promote trust and security in digital services in relation to privacy and data protection. ENISA in close cooperation with institutional (EU Commission, EDPS) stakeholders and the MS, including the EDPB, will work within its mandate to support the technical analysis of cybersecurity measures.

Currently in its 8th edition, the Annual Privacy Forum (APF) will remain the instrument of choice to bring together key communities, namely policy, academia and industry, in the broader area of privacy and data protection while focusing on privacy related application areas. Co-operation activities with European Data Protection Supervisor, the European Data Protection Board and national Data Protection Authorities will be further pursued.

Output O.2.2.4 – Guidelines for the European standardisation in the field of 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 SDOs (CEN/CENELEC and ETSI) by contributing to standardisation work at the strategic and tactical levels (e.g. by joining appropriate working and management groups, observing relevant Technical and Conference programme Committees and co-organising conferences etc.). New requirements associated primarily with the implementation and secondly transposition of the EU legal instruments in place in the Member States will be taken into account, including aspects of the NIS Directive, the Cybersecurity Act, the GDPR, as well as preparing for the upcoming ePrivacy Regulation, etc. This output will seek to analyse the gaps and provide guidelines for, in particular, the development or repositioning of standards, facilitating the promulgation and adoption of NIS standards. ENISA brings in this relationship its technical and organisation NIS know-how which can be further leveraged into standards in terms of extending or assessing them to render them more appropriate to stakeholders. By bringing in its concrete NIS policy expertise, ENISA will produce “how to” and “what else” guides in an effort to contribute to European standardisation.

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

Output O.2.2.5 – Supporting the implementation of European Electronic Communications Code

The European Electronic Communications Code (EECC), replacing the current Telecom framework directive that was in place since 2009, brings important changes to the electronic communications landscape and to the work of the telecom regulators across the EU. The new code, the EECC, was adopted in 2018, is expected to bring more harmonisation at EU level and several improvements as regards the security part, such as:

- broadens the scope of application to include also number-independent (Ni) interpersonal communications services (commonly known as Over-The-Top(OTT) services),
- a broader definition of security incidents, which is aligned with the definitions in the NIS Directive and in eIDAS, which will result in more types of incidents being reported,

ENISA will support competent authorities in the Member States with the transition, the new supervision tasks, and liaise with relevant industry players to support an effective, efficient and harmonized implementation of the security requirements in (Article 40) of the EECC. ENISA will build on the Article 13a Expert Group and its contacts with the private sector in order to define guidelines and good practices

Because the competent authorities for the EECC are in many Member States the same authorities that supervise the Digital Service Providers and the Digital Infrastructure under the NIS Directive, ENISA will ensure that this output remains closely aligned with the ongoing NISD work in the relevant NIS Cooperation Group work-streams.

Summary of outputs and performance indicators in 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 – Supporting policy developments in NIS Directive sectors	P: EU map of policy sectorial initiatives related to NIS Directive, Q4 S: Supporting Commission, EU Agencies, MS in policy developments related to NISD sectors, Q1-Q4 E: Three workshops with stakeholders from sectors, Q2-Q4 S: Supporting Commission, EU Agencies, MS and/or private sector in the sectorial implementation of NISD sectors, Q1-Q4	Engage stakeholders from at least 10 relevant stakeholders (P and S) At least 20 stakeholders participating in workshops (E)
Objective 2.2. Supporting EU policy implementation		
Output O.2.2.1 – Recommendations supporting implementation of the eIDAS Regulation	P: Recommendations to support the technical implementation of the eIDAS Regulation in Trust Services and/or eID, Q4. P: Any additional area in support of the implementation of eIDAS in line with Article 49 of eIDAS, Q4. E: Trust Services Forum, Q2 P: The future of digital identity and prospects of digital identity ecosystem, Q4.	Engaging at least 5 representatives from different bodies/Member States in the validation of the recommendations. Review and acceptance by at least 10 stakeholders (trust service providers, conformity assessment bodies, and supervisory authorities) from at least 5 Member States. 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 NIS Directive	S: Support the Cooperation Group in assessing the implementation of the NISD and other NISD related activities, Q1-Q4 S: Update existing “living documents” already developed in the context of the CG, Q1-Q4	Engaging at least 12 MS in ENISA’s contributions to the implementation of the NIS Directive (S)

	S: Support the work of the 2018-2020 Cooperation Group Work Programme as well as its Work Streams, Q1-Q4	10 MS participate in the workshop/activity (E)
Output O.2.2.3 – Contribute to EU policy in the area of privacy and data protection with technical input on cybersecurity related measures	P: Technical analysis of cybersecurity measures in data protection and privacy in close cooperation with competent EU Institutions i.e. the Commission, and further authorities such as the EDPS, and MS including the EDPB), Q4 E: APF 2020, Q2/Q3	At least 5 representatives from different bodies/MS participate in the preparation of the recommendations. More than 60 participants from relevant communities to attend the APF
Output O.2.2.4 – Guidelines for the European standardisation in the field of ICT security	P: Guidance and gaps analysis for European standardisation in NIS, with reference to the legal framework, Q4. E Joint CEN/ETSI/ENISA standardisation conference	Participation in drafting and review of the guidelines of at least 5 representatives of European Standard Developing Organizations (SDOs) and relevant services of the European Commission and/or Agencies
Output O.2.2.5 - Supporting the implementation of European Electronic Communications Code (EECC)	E: 2 workshops with public and private sector stakeholders S: Support the Commission, the competent authorities in the implementation of European Electronic Communications Code , Q1-Q4	At least 10 MS and 5 providers participate in the activities/workshops related to the new EECC

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

Objective 3.1. Assist Member States' capacity building

Output O.3.1.1 – Technical trainings for MS and EU bodies

In 2020 most of the activities in this area target at maintaining and extending the collection of good practice guidelines and trainings for CSIRT and other operational personnel such as product CSIRT (PSIRT) or operators of essential services (OES). The Agency will support the development of Member States' national incident response preparedness by providing good practice guidance on key elements of NIS capacity building with a focus on CSIRT/PSIRT/OES trainings and services in order to improve skills of operational teams and their personnel. ENISA will further build upon successful work in the area of 'training methodologies'.

In detail, the Agency will continue to provide an update of the training material, according to the findings of the stocktaking study for trainings in NISD sectors and provide a new set of a training material based on emerging technologies in order to reinforce MS operational skills and CSIRT/PSIRT capacities to efficiently manage cyber security events. A special emphasis is placed on supporting MS and EU bodies with concrete advice (like good practice material) and concrete action (like training). ENISA will as well offer, upon their request, direct support to single Member States to provide technical trainings and advisories. Last but not least, ENISA will continue supporting TRANSITS trainings.

In 2020, ENISA will further enhance its methodology, seminars and trainings on: a) core CSIRT services such as incident handling, digital forensics and vulnerability management b) cyber crisis management and c) the organisation and management of exercises. This activity will build on the current developed material and infrastructure for onsite and online trainings on these subjects. In addition, this activity will cover the delivery of these trainings upon request.

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

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

ENISA will continue assisting EU MS to develop their capabilities in the area of National Cyber Security Strategies (NCSS). The Agency, building on previous years' work in this area, will assist MS to deploy existing good practices in the related areas and offer targeted and focused assistance on specific NCSS objectives (e.g. CIIP, creation of PPPs etc.). A priority in this area will be to support MS so that their NCSS adequately reflect the priorities and requirements of the NIS Directive. Each year the Agency focuses on one of the objectives of the strategy (e.g. collaboration, CIIP, governance). ENISA will investigate the activities of MS and examine best practices and new potential incentives.

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

Finally, ENISA will enhance the NCSS map with additional valuable information related to the NISD creating an Info Hub. As for the past 6 years, ENISA will organise the annual NCSS workshop focusing on validating the findings of the study.

Output O.3.1.3 – Support EU MS in their incident response development

In 2020 ENISA will concentrate its efforts on supporting MS to enhance their incident response capabilities by assisting them with their CSIRT maturity assessments and enhancements. In addition, the Agency will continue to monitor CSIRT landscape development in Europe and provide an updated view on the CSIRT landscape and incident response practice development in Europe. In close cooperation with the NISD CSIRTs Network and the Connecting Europe Facility's MeliCERTes initiative, the agency will support the development of Member States' national incident response capabilities by providing recommendations and advisory on key dimensions of NIS capability building with a focus on the development and efficient functioning of national and sectorial CSIRTs and PSIRTs. ENISA will as well offer, upon their request, direct support to single Member States to assess and improve their incident response capabilities.

The main objectives of this output in 2020 is to help MS's and other ENISA incident response stakeholders, such as the EU institutions, bodies and agencies, to develop, deploy and enhance 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, maturity assessments and corresponding tools. As a continuous effort, ENISA will continue supporting cross-border CSIRT community projects, tools development as well as the global dialog about common issues and challenges in the incident response domain.

Output O.3.1.4 – ISACs for the NISD Sectors in the EU and MS

For many years ENISA has been working closely with the main operators of essential services in the EU. It has set up several sectoral expert groups covering sectors such as maritime, finance and health.[29] Through this effort and based on this experience with sectors or sector-specific topics like ICS/SCADA, ENISA holds a unique position in the EU to fulfil a key role concerning EU focused ISACs. It is a natural role for ENISA and continuation of its activities in the last 10 years to coordinate, in conjunction with CEF funding, the further 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[30].

ENISA has been working on the topic of CIIP since 2010, so it is uniquely prepared to assume a special role in Pan European sectorial ISAC. Some indicative (but not exhaustive) examples include:

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

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

ENISA will support MS the entire lifecycle of national/ European ISACs through engaging all relevant stakeholders: national competent bodies, the private sector i.e. operators of essential services or manufacturers and other relevant bodies. ENISA will also explore the possibility of synergies across national ISACs (national ISAC to national ISAC) as well as across EU sectorial ones. The Agency will also consider utilising its sectoral expertise that it has acquired through past and ongoing efforts to provide support (upon request) to ISACs in the form of knowledge sharing, e.g. webinars and other means of communicating knowledge. This will help the private companies operating in numerous MS to have increased benefits from such a collaboration.

[29] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services
[30] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2018-cef-telecom-calls-proposals

Objective 3.2. Support EU institutions' capacity building.

Output O.3.2.1 – Liaison with the EU agencies on operational issues related to CERT-EU's activities

Since December 2017 ENISA participates as Members of the Steering Board of CERT-EU, as the representative of EU agencies that use the services of CERT-EU. In this context ENISA will 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. In this context 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 institutions, agencies and other bodies on cybersecurity initiatives

ENISA has increased its cooperation efforts with a number of EU institutions and agencies and contributed to the preparation of activities linked to cybersecurity of to the Presidencies. In 2020 ENISA will intensify its cooperation efforts on cybersecurity with EU institutions and agencies and other relevant bodies in the context of the cybersecurity dimension of their mandate. This encompasses building on the Memorandum of Understanding and associated implementation activities on collaboration with EC3, EDA and CERT-EU. As such, ENISA will liaise with the relevant EU agencies ([31]) (including EASA, EC3, CERT-EU, EDA — including civil/defence cooperation, EEAS, etc.). ENISA will also participate in organising cybersecurity related events in cooperation with EU institutions and agencies and other relevant bodies.

Objective 3.3. Awareness raising

Output O.3.3.1 – European Cyber Security Challenges

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.

It is ENISA's aim to turn the ECSC in to one of the largest EU cybersecurity events, where all EU and EFTA countries will take part. The ECSC brand will be associated with the top cybersecurity talents of Europe and, by adding spinoffs, such as hackathons and start-ups camps, we expect ECSC to become one of the key incubators of cybersecurity entrepreneurship in Europe.

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

The Agency will also continue to support the planning and development of the European Cyber Security Challenge 2020. The goal for 2020 will be to further increase the interest in this type of events by promoting excellence in the form of cyber competitions, in the future the ECSC final competition can be followed by the creation of 'Team Europe' that will represent Europe in a future International competition. To this

[31] 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

extend, ENISA has already established some contacts with representatives of similar competitions in other regions outside Europe.

Output O.3.3.2 – European Cyber Security Month deployment

In 2020, ENISA will continue to support the EU MS in promoting the cybersecurity awareness raising activities like European Cyber Security Month (ECSM). European Cyber Security Month is to address disparity of cybersecurity practices across Member States in two stages. The first stage is to support the Member States so that the awareness and behaviour of citizens in each Member State is raised to a mature baseline. The second stage is to further lower the cybersecurity risks by raising the maturity of citizen's behaviour in unison; at the European level.

ENISA and the European Commission can achieve the objectives of the European Cyber Security Month by driving the pan-European campaign so as to ensure all Member States are actively committed to the European Cyber Security Month and that industry is also involved and 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

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

Summary of outputs and performance indicators in Activity 3 Capacity

Summary of Outputs in Activity 3 – Capacity. Support Europe maintaining state-of-the-art network and information security capacities		
Outputs	**Type of output (P=publication, E=Event, S=Support)**	**Performance indicator**
Objective 3.1. Assist Member States' capacity building		
Output O.3.1.1 - Technical trainings for MS and EU bodies	P: operational training material development and customization to the needs of a NISD Sector (details on operational category can be found on ENISA training website), Q4 S: dedicated training room and technical lab development, Q4 P: Delivery of a training session of the NISD Sector customized training material mentioned above, Q4 S: TRANSITs (European CSIRT training event) support, Q4	At least one training material developed to support operational practices of CSIRTs in Europe. At least 5 CSIRTs contribute to and validate the training material. 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	S: Support MS in NCSS development and assessment, Q1-Q4 E: 1 workshop with EU MS on NCSS development, Q2-Q4	At least 3 MS supported in the implementation of NCSS lifecycle (S). Engage stakeholders (national competent authorities or private sector) from at least 12 EU MS (E).

Output O.3.1.3 – Support EU MS in their incident response development	S: Supporting enhancement of CSIRTs capabilities and maturity in Europe, Q4 P: CSIRT and IR landscape in Europe; updated status report, Q4 P: CSIRT online Inventory update – European interactive map of CSIRTs, Q2 & Q4 S: CSIRT online Inventory tool development, Q4 P: ENISA CSIRT maturity assessment online tool development, Q4 S: Continue activities and involvement in CSIRT structures (e.g. FIRST, TF-CSIRT-TI, NATO NCIRC, GFCE including CEF MeliCERTes project), Q1-Q4	Identify and report on number of MS supported and type of support provided Two CSIRT inventory updates Provide updated report on CSIRT and IR landscape in Europe Support or advisory provided at least to two CSIRTs to enhance their team's maturity. ENISA supports at least 2 international CSIRT or taskforce initiatives in community fora like FIRST, TF-CSIRT-TI or GFCE.
Output O.3.1.4 –ISACs for the NISD Sectors in the EU and MS	P: EU map of national and EU ISACs, Q4 S: Support relevant public and private stakeholders in establishing EU and national ISACs, Q1-Q4. S: Support EU and MS ISAC activities, Q1-Q4	At least 3 ISACs supported (S). Engage at least 12 organisations representing at least 3 sectors from at least 8 MS in this activity (P)
Objective 3.2. Support EU institutions' capacity building		
Output O.3.2.1 – Liaison with the EU agencies on operational issues related to CERT-EU's activities	S: Attending CERT-EU SB meetings S: Liaison with EU agencies using CERT-EU services notably through ICTAC	Consultation with EU Agencies and representing their views at CERT-EU SB level.
Output O.3.2.2 - Cooperation with relevant EU institutions, agencies and relevant bodies on cybersecurity initiatives	P: Report on the cooperation activities with relevant union bodies, Q4 S: Cooperation in organising events, conferences, workshops co-organized with EU institutions, agencies and relevant bodies on cybersecurity initiatives	Engage the relevant EU stakeholders (including EASA, EC3, CERT-EU, EDA, EEAS, etc.)
Objective 3.3. Awareness raising		
Output O.3.3.1 – Cyber Security Challenges	S: European Cyber Security Challenge support, Q1-Q4 E: Q2-Q3: 'Award workshop' for winners of the European Cyber Security Challenge 2020 (ENISA promotes best of the best)	At least two additional EU MS organise national cyber security challenges in 2020 and participate in the European Cyber Security Challenge Final. At least one contact from Non EU country to promote the international engagement
Output O.3.3.2 – European Cyber Security Month 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 programs in the EU that aim to enhance cyber security skills among EU citizens, in general, and cyber security experts	Engage at least 15 organisations representing academia, public institutions and private companies from at least 10 MS

Activity 4 – Cooperation. Foster the operational cooperation within the European cybersecurity community

Objective 4.1. Cyber crisis cooperation

Output O.4.1.1 – Planning of Cyber Europe 2020

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

CE2020 will focus on testing capabilities and procedures, namely large-scale incident management cooperation procedures at EU and national-levels. The crisis escalation scenario will be realistic and focused in order to capture better how incidents are managed and cooperation happens in real-life. The exercise will include explicit scenarios for the CSIRTs Network, Single Point of Contacts and Competent Authorities set up under the NIS Directive, including focusing on one or more of the essential sectors. Also there will be designs to exercise the various aspects of the Cyber Crisis Collaboration Blueprint, in collaboration with the Commission, also considering the recommendations in this regard provided by the NIS Cooperation Group, such as the 'cybersecurity Incident Taxonomy' or those on 'Cooperation procedures amongst Member States and functions and capabilities of the National Single Point of Contact'. Depending on the availability of resources in 2020 ENISA will also enhance the observers role (introduced in 2018) striving to make best use of observers.

The high-level exercise program brief will include the strategic dimensions of the exercise will be prepared based on the lessons learned from CE2018, to drive the whole planning process ENISA will assemble group of planners from the participating countries to work closely towards developing a detailed exercise plan (ExPlan) in 2019. ENISA will involve the group of planners in the relevant planning steps and take into account their input towards a consented plan. The exercise planning will avoid overlaps with other major related activities.

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

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

Output O.4.1.3 – Support activities for Cybersecurity collaboration with other EU institutions and bodies

ENISA will work with other EU Institutions and bodies in the development of Cybersecurity collaboration tasks based on an agreed roadmap.

In particular, ENISA will work in further developing bilateral and multilateral cooperation with:

- DG Connect
- the European Cybercrime Centre at Europol (Europol/EC3)
- the EU Intelligence Analysis Centre (INTCEN)
- the EU Military Staff Intelligence Directorate (EUMS INT) and Situation Room (SITROOM), working together as SIAC (the Single Intelligence Analysis Capacity)
- the European Defence Agency (EDA)
- the Computer Emergency Response Team for the EU Institutions (CERT-EU)
- the Emergency Response Coordination Centre in the European Commission

ENISA will also work with the aforementioned organisations in order to build capacities and synergies in exercising, training and cyber skills.

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[32]. ENISA is at the crossroads of most if not all public-private, cross-sector cybersecurity communities in Europe, from the technical to the strategic level. As indicated in the EC Communication on Building strong cybersecurity for the EU[33], ENISA serves as "the focal point for information and knowledge in the cybersecurity community". As a result, ENISA is in a unique position to leverage its network to gather information, process it and foster timely, tailored and highly relevant situational awareness to support decision-making in both the public and the private European sectors, as recommended by the EC in the blueprint:

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

In order to support the drafting of these reports and process meaningfully the massive amounts of inputs they require, ENISA has initiated the development, in 2018, of a tool that acts as a cybersecurity news sources aggregator, provides awareness and assists threat analysts in drafting cybersecurity reports. An initial prototype is already in place which has been reviewed by experts from ENISA, various EU institutions and the private sector to validate its added value in their work. In 2019 the next phase of development will

[32] 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

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

commence towards a ready to use product by the end of 2019 or beginning 2020. The tools is using the latest technologies in Artificial Intelligence and Natural Language Processing in order to facilitate the creation of EU cybersecurity reports by providing a specialized cybersecurity search engine, 24/7 monitoring of trending news regarding cybersecurity as well as an immediate access on ENISA's own work on relative subjects. Additional functionalities and improvements will be periodically added according to the latest technological evolutions and the needs of the users of this tool.

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

Output O.4.1.5 – Supporting the EU Cybersecurity blueprint

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

Based on the Commission's guidance and lessons learned by the EU PACE exercise, ENISA will drive initiatives in the mitigation of identified gaps in cooperation between

- EU cyber security stakeholders main actors like DG Connect, the European Cybercrime Centre at Europol (Europol/EC3), the EU Intelligence Analysis Centre (INTCEN), the EU Military Staff Intelligence Directorate (EUMS INT) and Situation Room (SITROOM) working together as SIAC (the Single Intelligence Analysis Capacity), the EU Hybrid Fusion Cell (based in INTCEN), the Computer Emergency Response Team for the EU Institutions (CERT-EU), the Emergency Response Coordination Centre in the European Commission and possibly the Cybersecurity Emergency Response Fund.
- The rest of EU bodies, agencies and Institutions that should be under the EU cybersecurity blueprint umbrella for the handling and mitigation of cyber oriented crises.

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

ENISA will assist Member States to engage in the EU Cybersecurity Crisis Response Framework with National Cybersecurity Crisis Response Frameworks. Furthermore, upon request or emerging needs, ENISA will organise workshops and/or table-top exercises to validate that these procedures allow for the exchange of information without undue delay, prior to their use either in real life or in larger exercises such as Cyber Europe.

Objective 4.2. Community building and operational cooperation

Output O.4.2.1 – EU CSIRTs Network support

ENISA will continue its support to the Commission and Member States in the implementation of the NIS Directive, in particular in the area of CSIRTs. As part of this activity, ENISA will continue its tasks as the secretariat of the CSIRTs Network and actively support its functioning by suggesting ways to improve cooperation and trust building among CSIRTs. The agency will also support this cooperation by developing and providing guidance and good practices in the area of operational community efforts, such as on information exchange and secure communication, on request by the members of the CSIRTs Network. In particular, the Agency will be proactive in stimulating discussions within the network and will aim to provide content to support discussions on policy and technical initiatives according to the CSIRTs Network's own work program.

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

The Agency will further provide, improve, develop and secure the CSIRTs Network infrastructure for its members' smooth collaboration and administration use.

Output O.4.2.2 – Support the fight against cybercrime and collaboration across CSIRTs, LEA and other operational communities

In 2020, ENISA will continue collaborating directly or indirectly with key stakeholders such as EUROPOL/EC3, and possibly other Agencies concerned (e.g. CEPOL, Eurojust) in an effort to support the cooperation between the CSIRT and the law enforcement communities and the extensions that this collaboration may have to other communities of stakeholders concerned. ENISA is likely to continue its analysis and the production of training material on the basis of such analysis in an effort to lower the barriers in cooperation across these communities.

In addition, the Agency will continue collaboration with other operational EU bodies to ensure a structured cooperation with CERT-EU, European Cybercrime Centre (EC3), EDA and other relevant EU bodies in line with the Commission proposal for the Cybersecurity Act.

Output O.4.2.3 – Supporting the operations of MeliCERTes platform

ENISA is committed to further support MeliCERTes platform, which is envisaged as the primary collaboration platform between participating Member States CSIRTs and which is helping to enlarge EU MS preparedness, cooperation and coordination to effectively respond to emerging cyber threats as well as to cross-border incidents.

Any particular CSIRT need to maintain its data within the MeliCERTes framework. Some of this data must be vetted by the centralized workflow – such as the mandate or memberships in CSIRT communities – in order to correctly reflect any changes in the related Central Trust Circles CTCs.

In 2020, ENISA will fully support the platform from an operational perspective. In particular, ENISA will deploy specific operational procedures that are mandatory to follow in order to maintain the underlying team data and references. In this regard also centralized workflows to maintain the Central Trust Circles (CTCs) of the MeliCERTes platform.

Summary of outputs and performance indicators in 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	P: CE2020 After Action Report (restricted), Q4 E: Exercise events, Q1 - Q4	At least 80% EU/ EFTA Member States and countries confirm their support for Cyber Europe 2020
Output O.4.1.2 – Support activities for Cyber Exercises	S: Support for the maintenance and further development of the Cyber Exercise Platform, Q4	At least one exercise with two different entities is organised in 2020.
Output O.4.1.3 – Support activities for Cybersecurity collaboration with other EU institutions and bodies	S: Supporting the implementation of the Cybersecurity collaboration roadmap with EU institutions	At least 3major collaboration tasks from the roadmap are achieved.
Output O.4.1.4 – Supporting the implementation of the information hub	S: Support for other EU Agencies having a role in cybersecurity.	Established communication Evaluation of the tool by at least 3 EU bodies/agencies
Output O.4.1.5 – Supporting the EU Cybersecurity blueprint	S: Emergency directories and processes for cooperation activities during crises	At least 3 stakeholders of the Blueprint are consulted.
Objective 4.2. CSIRT and other NIS community building		
Output O.4.2.1 – EU CSIRTs Network support	S: Provide CSIRTs Network Secretariat E: provide meeting organisation and support (minimum 1 event) E: provide team building activity for the CNW, Q4 P: Q1-Q4: Facilitate preparation of the next evaluation report for the cooperation group P: 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. S: Q1-Q4, Provide CSIRTs Network communication infrastructure development, maintenance, security (Portal, mailing lists, chat), Q4 P: provide regular pentest of the CNW infrastructure, Q4 E: Trust building exercise (co-located with the regular CSIRTs Network meeting) P: Q4 Further support for CNW specific information exchange and secure communication issues (according to the CSIRTs Network Action plan) S: Active Secretariat support and engagement during annual Cyber SOPEx 2019 exercise of the CSIRTs Network according to the CNW SOPs. S: CSIRT maturity assessment and peer review support for members of the CSIRTs Network.	Organize at least 1 CNW meeting 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 conference call facility backup for the need of the CSIRTs Network operations. At least two penetration tests and necessary security and functionality improvements made to the Cooperation Portal. At least one team building event organised during regular CSIRTs Network Meeting At least four communication checks done to test CNW communication channels readiness. Provide active Secretariat support to the facilitator of the SOP exercise during execution according to the CNW procedures.

Output O.4.2.2 – Support fight against cybercrime and collaboration across CSIRTs, LEA and other operational communities	P: A report on a topic emenating from the 2019 A report on cooperation P: Training material based on such report E: Q3, annual ENISA/EC3 workshop for national and governmental CSIRTs and their LEA counterparts S: Structured cooperation with CERT-EU	At least 5 MS CSIRT representatives, 5 MS law enforcement representatives, and EC3 participate in the preparation of the roadmap At least 15 MS participate in ENISA/EC3 annual workshop Engage with CERT-EU on structured cooperation
Output O.4.2.3 - Supporting the operations of MeliCERTes platform	S: Operational support for the MeliCERTes platform	Provide support to CSIRTs using MeliCERTes according to agreed operational procedures.

Activity 5 – Cybersecurity certification. Developing security certification schemes for digital products, services and processes

Objective 5.1. Support activities related to cybersecurity certification

Taking due account of legislative and policy developments in the area of EU Cybersecurity Certification and acting within the boundaries of its competence, ENISA will continue working towards meeting 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 subsidiarity as it applies in the area of certification.

Building on the work which will be undertaken in 2019, ENISA will provide support to the Commission and the Member States in the policy area of EU cybersecurity certification framework within the scope of the approved Cybersecurity Act. ENISA will seek to stimulate the interaction and involvement of Member States' as well as public policy and industry stakeholders in the emerging EU certification framework.

In view of its new role as per the cybersecurity Act, ENISA will seek to join the process of drawing up a rolling work programme for certification, in support of the Commission. In interacting with the Commission and following an annual plan, ENISA could assist in aggregating requirements from the private sector and institutional stakeholders to facilitate Commission efforts.

ENISA will provide support for the organisation of the EU cybersecurity certification framework (organisational and IT systems and support) and analysis of functional equivalence of existing certification schemes across the EU (at the MS as well as the EU level) with the emerging EU certification framework for the purpose of facilitating the transition to the new EU framework. ENISA will continue to interact with key stakeholders associated with the EU cybersecurity certification framework.

Output 5.1.1 – Support for the EU Cybersecurity Certification Group and potential subgroups

ENISA supporting the European Commission in its role as chair of the European Cybersecurity Certification Group, will provide support for the organisation of the EU cybersecurity certification Group and potential subgroups, with services to be discussed with the EU Commission e.g. support for the Secretariat, organisational aspects etc.

Output 5.1.2 – Research and analysis of the market as an enabler for certification

By means of analysis and drafting reports, ENISA will seek to maintain a high level of understanding of the main drivers for cybersecurity certification in the EU. Areas of interest will gradually include consumer and industrial IoT, Cloud Computing, IoT and consumer electronics etc., with a view to analyse the added value of and opportunities for the EU cybersecurity certification framework to protect citizen rights (e.g. consumer rights, personal data, privacy etc.) and public interest (e.g. public purchasing in the MS, by means of public procurement). An additional area of interest include market analysis in relation to manufacturers and service providers impacted by the EU cybersecurity certification framework.

Output 5.1.3 – Set-up and maintain a Certification portal

There are technical and organisational tasks associated with the setting up of and the maintenance of a portal. Clearly an IT system in support of the EU cybersecurity certification framework goes beyond the scope of a portal as it must accommodate the needs of stakeholders involved (document management, consultations) and allow for the presentation of dependable information on certification schemes.

Objective 5.2. Developing candidate cybersecurity certification schemes

Output 5.2.1 – Hands on tasks in the area of cybersecurity certification of products, services and processes

Based on the PDCA (plan-do check-act, and repeat) approach, ENISA will strive to provide a full life-cycle set of services that spawn across, (a) planning (b) data collection (c) consultations (d) drafting and reviewing. ENISA will have drawn up a general methodology to prepare candidate cybersecurity certification schemes. ENISA will use its capability to provide a planning, prioritisation thereof, lists of associated stakeholders to be involved in input giving and consultations. ENISA will develop a feedback mechanism toward stakeholders concerned e.g. standardisation organisations. ENISA will continue delivering its EU Cybersecurity Certification Conference in 1 or 2 editions per year.

Output 5.2.2 – Tasks related to specific candidate scheme

Importantly, ENISA will draw up candidate cybersecurity certification schemes on the basis of the work undertaken in 2019 and input received from stakeholders involved as well as through its own means and capabilities according to the Rolling Work Programme or on requests according to the Cybersecurity Act. ENISA will also follow up with its candidate schemes all the way till submitted to and accepted by the EU Commission for formal consideration and eventual approval.

Summary of outputs and performance indicators in Activity 5 Certification

Summary of Outputs in Activity 5 – Cybersecurity certification. Developing cybersecurity certification schemes for digital products, services and processes		
Outputs	**Type of output (P=publication, E=Event, S=Support)**	**Performance indicator**
Objective 5.1. Support activities related to cybersecurity certification		
Output O.5.1.1 – Support for the EU Cybersecurity Certification Group and potential subgroups	S: Support the EU Commission in the ECCG E : 1-4 ECCG meetings p.a. E: 8 subgroup meetings	Planning and execution of tasks related to meetings; Commission feedback
Output O.5.1.2 – Research and analysis of the market as an enabler for certification	P: A report on market situation in relation to cybersecurity certification	Eight MS and ten industry representatives providing input
Output O.5.1.3 – Set-up and maintain a Certification portal	S: Tasks include review of requirements; implementation updates; content updates	Meeting milestones, in terms of implementation and usability of the

		resources provided; available portal for the existing European certification schemes
Objective 5.2. Developing candidate cybersecurity certification schemes		
Output O.5.2.1 – Hands on tasks in the area of cybersecurity certification of products, services and processes	P: Use the methodology for the preparation of candidate cybersecurity certification schemes S: Interaction with stakeholders / data collection E: EU Cybersecurity certification framework Conference	Number of stakeholders identified and actively participating in the scheme drafting preparation and consultation (at least 10 private and or public organisations) At least 60 participants from relevant stakeholders
Output O.5.2.2 – Tasks related to specific candidate scheme	P: Various schemes produced throughout the year	Draft at least 1 scheme per year or 50% of the ones requested and prioritised for 2020, by ECCG and the EU Commission

Activity 6 – Enabling. Reinforce ENISA's impact

Objective 6.1. Management and compliance

Management

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

In 2020, the **Management Board Secretariat** will continue to support the Management Board and the Executive Board in their functions by providing secretariat assistance. It includes, but is not limited to the support for meetings and correspondence that takes place between meetings, the management of annual declarations of interest and of commitment and other requirements.

In relation to the MB, two ordinary meetings will be organised during 2020 and informal meetings will be held as necessary. The MB Portal will be supported for the MB. In relation to the Executive Board, one formal meeting will be organised per quarter and informal meetings, when necessary.

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

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

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

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

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

Policy Office

The Policy Office reports into the Head of Core Operations. Through the Policy office, the Agency initiates and further develops strategic cooperation with relevant stakeholders active in the cybersecurity community. For instance, the Agency engages in policy and strategy discussions with political and policy decision makers (by participating or organizing e.g. MEP Breakfasts). Furthermore the Agency engages and further develops strategic relationships with e.g. specific industry sectors at decision making level, and identifies the strategic issues on cybersecurity. The Policy office will also be in a position to support various legislative bodies in respect of legislative initiatives. Some of the results of these activities of the Policy Office are published as opinion papers on ENISA webpage. Besides these activities, more details of the activities delivered by the Policy Office and Public Affairs team are detailed in Objective 5.2 Engagement with stakeholders and international activities.

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

Public Affairs Team

The Public Affairs Team (PAT) reports into the Head of Core Operations and is responsible for coordinating all activities with the media and press, including press releases, news items and interviews to enhance the reputation and image of the Agency.

It supports the entire Agency with regards to publications, social media promotion, website management, public affairs activities and awareness campaigns. The PAT team is also responsible for establishing ENISA's corporate visual identity.

The PAT team also plays a major role in supporting events attended by the Agency, ensuring that ENISA is well represented from a public affairs perspective, that appropriate publicity material is available and, where appropriate, that booths are arranged and supported.

Internal control

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

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

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

IT activities

During 2020 it is expected that the Agency has a new fully operating datacentre. In combination with the already existing datacentre recovery site ENISA this will enhance IT service availability and the Agency will be prepared for any challenges that may arise.

Following up the assessment of information security risks and IT operational procedures, ENISA will be putting in place and updating all policies and procedures to mitigate any risks identified.

For 2020 it is expected that all business applications will be securely available on the most widely used mobile devices. By this timeframe the platform consolidation should be complete and mature, with adequate, flexible and advance reporting and monitoring tools.

IT support all internal electronic infrastructure in the Agency, this includes but is not limited to core applications for business use and operation systems.

Task	Objective	Level of completion 2020	Level of completion 2021	Level of completion 2022
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	98%	98%	98%
Availability of internal applications	Availability	95%	95%	95%
Help desk, reply with success to all service requests	Efficiency	99%	99%	99%

Finance, Accounting and Procurement

The Agency plans to upgrade its internally developed electronic tools used for Procurement in order to simplify and further automate its tasks related to tendering and contracting. This is deemed necessary due to the expected increase in the volume of work based on a significantly increased operational budget. It is anticipated that further development of the in-house systems should be outsourced to professional web developers as the current in-house applications are at a low level of complexity due to the limitations of the SharePoint platform. The aim is to improve the utilization of resources, to have a better overview of all financial and procurement processes, to provide better reporting and subsequently a high level of transparency. Internal policies will also need to 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 to optimise the available resources.
Budget planning and implementation will be resourced with a new electronic tool.

Task	Objective	Level of completion 2020	Level of completion 2021	Level of completion 2022
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	90%	90%	90%
Payments against appropriations carried over from year N-1 (C8 funds)	Efficiency and Sound Financial Management	95%	95%	95%
Payments made within Financial Regulation timeframe	Efficiency and Sound Financial Management	98%	98%	98%
Planned Procurement Activities versus actual implementation of the year	Efficiency and Sound Financial Management	70%	80%	90%

Human Resources

The ultimate goal of HR is to attract, select, develop and retain highly qualified staff, to put in place optimal organisational structures, to promote a safe working environment, to create a culture that reflects ENISA's vision and values in which staff can give their best in achieving the organisation's objectives. By offering a broad array of services (Recruitment, Performance management, L&D, Career management, Working conditions, Social rights, etc.) HR's objective is to deliver a successful day-to-day management of ENISA statutory staff and external staff (e.g. trainees) in compliance with the Staff Regulations/CEOS. Additionally, investment and efforts are focusing on several projects such as the acquisition of an E-Recruitment tool, the development in closed collaboration with the European Commission's services of SYSPER.

Task	Objective	Level of completion 2020	Level of completion 2021	Level of completion 2022
Efficient management of selection procedures	Reduction of time to hire (*in line with EU HR standard definition it is the time between the closure date for applications and the signature of the reserve list by the ED)*	5 months	5 months	5 months
Turnover of staff	Reduce the turnover ratio of statutory staff (TA and CA)	<15%	<15%	<15%
Staff's Performance Management	Implementation and monitoring of the appraisal and reclassification exercises (launching and closing the exercises)	100%	100%	100%
Staff Survey	Participation of staff in the staff survey	70%	75%	75%

Legal affairs, data protection and information security coordination

Legal Affairs

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

Data Protection Compliance tasks and Data protection Office

The main tasks of the Data Protection Officer (DPO) include[34]:

- 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; co-operate and consult with EPDS whenever needed.

[34] 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, 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

Information Security coordination

The Chief Information Security Officer (CISO) coordinates the Information Security Management System on behalf of the Authorising Officer. In particular, the CISO advises the ICT Unit to develop and implement information security policies, standards, guidelines and baselines that seek to secure the confidentiality, integrity and availability of the information systems of the Agency. The CISO is instrumental in incident handling and incident response and security event monitoring. The CISO also leads the security training for the Agency's staff and he provides security guidance on all IT projects, including the evaluation and recommendation of technical controls. In 2020 the CISO 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 IT security training for ENISA staff
- Implementing new systems and tools that can support improvements on Information Security.

Objective 6.2. Engagement with stakeholders and international activities

Stakeholders communication and dissemination activities

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

Dissemination and Outreach

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

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

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

Area	Metric	Increase Relative to Previous Year		
		2020	2021	2022
Volume of media material published by the agency	Number of press communications published	30%	30%	20%
Number of social media items	Number of social media items published	40%	40%	30%
Number of social media followers	Number of social media followers	25%	25%	20%
Number of corporate events	Number of corporate events	40%	10%	10%
Website traffic	Number of page views/visits/unique visitors/returning visitors	30%	30%	20%

Internal communications

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

Task	Objective	Level of completion		
		2020	2021	2022
Maintain staff informed on ENISA Activities (internal communications)	20 staff meetings per year	100%	100%	100%
Team building activities	Events with participation of all staff	2	2	2

Permanent Stakeholders Group

In 2020, ENISA will continue to support the Permanent Stakeholders Group (PSG) and will aim to reinforce the contribution of the PSG to the ENISA Work Programme.

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

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

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

National Liaison Officer Network

ENISA in 2017 has kicked off various activities aiming at strengthening the cooperation with its National Liaison Officers’ (NLO) Network. These activities were continued and were further elaborated in 2018 and 2019. NLOs are key actors for the Agency’s daily work and they warrant the interaction with select public sector entities in the MS while they provide assurance in terms of outreach, effective liaison with the MS and dissemination of ENISA deliverables.

ENISA will build upon these activities with the NLO Network, as a further the first point of contact for ENISA in the MS beyond the Management Board, with emphasis on:

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

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

International relations

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

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

- Acting within its mandate, ENISA will develop contacts with important cybersecurity bodies outside the EU where synergies are beneficial to the EU cybersecurity programme. An example is NIST, which plays an important role in the implementation cybersecurity in the US.
- ENISA will follow the development of relevant subjects at the international level in order to align EU activities with other global players. An example here is provided by the work that ITU is doing with CSIRTs, which needs to be aligned and will create added value and harmonization to all.
- ENISA staff will attend international conferences on an 'as needed' basis. For instance, the Meridian Conference is the main CIIP conference of the year and the FIRST conference plays the same role for CERTs.
- The ED may attend international conferences in order to enhance the Agency visibility and may also request other staff members to attend such conferences when it is in the interest of the Agency.

List of Outputs in work programme 2020

Activity 1 – Expertise. Anticipate and support Europe's knowledge in facing emerging cybersecurity challenges
Objective 1.1. Improving knowledge on the security of digital developments
Output O.1.1.1 – Building knowledge on the security of Internet of Things
Output O.1.1.2 – Building knowledge on the security of Connected and Automated Mobility (CAM)
Output O.1.1.3 – Building knowledge on Artificial Intelligence security
Output O.1.1.4 – Building knowledge on the security of Healthcare services
Output O.1.1.5 – Building knowledge on maritime security
Output O.1.1.6 – Building knowledge on cryptographic algorithms
Objective 1.2. Cybersecurity Threat Landscape and Analysis
Output O.1.2.1 – Annual ENISA Threat Landscape
Output O.1.2.2 – Restricted and public Info notes on cybersecurity
Output O.1.2.3 – Support incident reporting activities in the EU
Output O.1.2.4 – Supporting the operational sectoral implementation of the NIS Directive
Objective 1.3. Research & Development, Innovation
Output O.1.3.1 – Supporting EU research & development programmes
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 – Supporting policy developments in NIS Directive sectors
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 NIS Directive
Output O.2.2.3 – Contribute to the EU policy in the area of privacy and data protection with input on cybersecurity related measures
Output O.2.2.4 – Guidelines for the European standardisation in the field of ICT security
Output O.2.2.5 – Supporting the implementation of European Electronic Communications Code
Activity 3 – Capacity. Support Europe maintaining state-of-the-art network and information security capacities
Objective 3.1. Assist Member States' capacity building
Output O.3.1.1 – Technical trainings 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 – ISACs for the NISD Sectors in the EU and MS
Objective 3.2. Support EU institutions' capacity building.
Output O.3.2.1 – Liaison with the EU agencies on operational issues related to CERT-EU's activities
Output O.3.2.2. – Cooperation with relevant EU institutions, agencies and other bodies on cybersecurity initiatives
Objective 3.3. Awareness raising
Output O.3.3.1 – European Cyber Security Challenges
Output O.3.3.2 – European Cyber Security Month deployment
Output O.3.3.3 – Support EU MS in cybersecurity skills development
Activity 4 – Cooperation. Foster the operational cooperation within the European cybersecurity community
Objective 4.1. Cyber crisis cooperation
Output O.4.1.1 – Planning of Cyber Europe 2020
Output O.4.1.2 – Support activities for Cyber Exercises
Output O.4.1.3 – Support activities for Cybersecurity collaboration with other EU institutions and bodies
Output O.4.1.4 – Supporting the implementation of the information hub
Output O.4.1.5 – Supporting the EU Cybersecurity blueprint
Objective 4.2. Community building and operational cooperation
Output O.4.2.1 – EU CSIRTs Network support
Output O.4.2.2 – Support the fight against cybercrime and collaboration across CSIRTs, LEA and other operational communities
Output O.4.2.3 – Supporting the operations of MeliCERTes platform

Activity 5 – Cybersecurity certification. Developing security certification schemes for digital products, services and processes
Objective 5.1. Support activities related to cybersecurity certification
Output 5.1.1 – Support for the EU Cybersecurity Certification Group and potential subgroups
Output 5.1.2 – Research and analysis of the market as an enabler for certification
Output 5.1.3 – Set-up and maintain a Certification portal
Objective 5.2. Developing candidate cybersecurity certification schemes
Output 5.2.1 – Hands on tasks in the area of cybersecurity certification of products, services and processes
Output 5.2.2 – Tasks related to specific candidate scheme

Annexes A

A.1 Annex I: Resource allocation per Activity 2020 – 2022

Next sections of this Annex presents the evolution of past and current situation, as well as the distribution of resources and budget for the 6 activities of the WP2020.

Overview of the past and current situation.

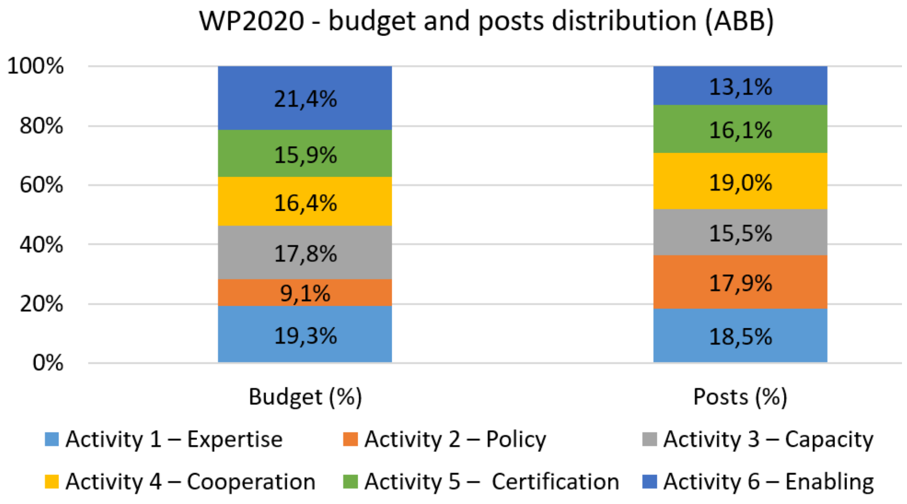
WP 2020 is following the COM guidelines and MB decisions. The Work Programme is structured following the objectives and the priorities of the Agency, using a structure build on the previous years, where a new activity was added to address the work to be carried on in the area of cybersecurity certification.

Regarding ENISA's budget, the variations between the years 2017 and 2018 is neutral. In 2018, a slight increase in the title II was adopted. When preparing this document, for 2019, the final budget of the Agency is still to be approved. The Annexes provide data in 2 Scenarios for the Work programme 2019.

As already presented, in the preparation of Work Programme 2020, ENISA is using the resources proposed in the Annexes of the European Commission's proposal for ENISA's new mandate COM(2017) 477 Final (Cybersecurity Act). The human and financial resources of past and current situation are presented in the Annexes of this document.

Resource programming for the years 2020-2022

The distribution of budget and resources for 2020 for the activities A1 to A6 is presented in the chart.



Following the publication of the NIS Directive (NISD), the Agency is re-allocating budget and resources to the new tasks/activities provisioned for the Agency in the Directive. Another area which will probably require more budget / resources is the Cybersecurity Public Private partnership (cPPP). Furthermore a significant part of the new resources and budget are foreseen, according to Draft Cybersecurity Act, to be allocated to the new Activity 5 on cybersecurity certification.

For the interval 2020-2022 it is foreseen an increase of budget and resources allocated to the new activity on Cybersecurity certification and well as to operational activities described in the draft Cybersecurity Act.

The budget and resources allocations for 2020 to 2022 within the summary tables and Annexes are in line with the European Commission's proposal for ENISA's new mandate COM(2017) 477 Final.

Overview of activities budget and resources

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

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

- **Direct** Budget is the cost estimate of each **Operational** activity (listed in Activities A1 to A6) in terms of goods and services procured.
- **Indirect** Budget is the cost estimate of salaries, mission costs and overhead costs, attributable to each **Operational or Compliance** activity. The indirect budget is re-distributed against direct budget in all Activities.
- **Compliance** posts from Activity A6 Enabling are redistributed to Core Activities - A1 to A5, and **operational** posts of the Activity A6.
- Total ABB posts (FTEs) are the sum of all the posts from all activities (A1 to A6) after the re-distribution.

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

WP2020	**Total ABB budget (€)**	**Total ABB posts (FTEs)**
Activity 1 - Expertise. Anticipate and support Europe's knowledge in facing emerging cybersecurity challenges	4.213.495,91	21,04
Activity 2 - Policy. Promote network and information security as an EU policy priority	1.981.689,86	20,36
Activity 3 - Capacity. Support Europe in maintaining state-of-the-art network and information security capacities	3.886.420,89	17,64
Activity 4 - Cooperation. Foster the operational cooperation within the European cybersecurity community	3.578.585,57	21,71
Activity 5 - Cybersecurity certification. Developing security certification schemes for digital products, services and processes	3.463.147,33	18,32
Activity 6 - Enabling. Reinforce ENISA's impact	4.662.293,64	14,93
Total	**21.785.633,20**	**114,00**

A.2 Annex II: Human and Financial Resources 2020-2022

Table 1. Expenditure overview

Expenditure	2018		2019 Scenario 1		2019 Scenario 2 (voted budget)		2020		2021		2022	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1	6.386.500,00	6.386.500,00	7.133.782,80	7.133.782,80	9.477.948,32	9.477.948,32	12.038.000,00	12.038.000,00	13.343.500,00	13.343.500,00	13.875.000,00	13.875.000,00
Title 2	1.687.500,00	1.687.500,00	1.604.101,00	1.604.101,00	2.497.000,00	2.497.000,00	2.886.000,00	2.886.000,00	3.114.000,00	3.114.000,00	3.205.000,00	3.205.000,00
Title 3	3.354.126,00	3.354.126,00	2.901.000,00	2.901.000,00	4.958.003,73	4.958.003,73	6.861.633,20	6.861.633,20	6.968.901,60	6.968.901,60	7.140.156,60	7.140.156,60
Total expenditure	**11.428.126,00**	**11.428.126,00**	**11.638.883,80**	**11.638.883,80**	**16.932.952,05**	**16.932.952,05**	**21.785.633,20**	**21.785.633,20**	**23.426.401,60**	**23.426.401,60**	**24.220.156,60**	**24.220.156,60**

Next tables show the commitments and payment appropriations based on the same structure for the next years, where *WP2019 information of Scenario 2 is provided*[35].

[35] Voted budget for 2019 is now known and is increased with approx. 400k compared with Scenario 2 budget. The following tables provide allocation of the voted budget 2019 where Scenario 2 is referred.

Commitment appropriations

EXPENDITURE	Commitment appropriations						
	Executed Budget 2017 (31/12/17)	Budget 2018	Envisaged in 2019 (Scenario 2)	Envisaged in 2020	VAR 2020 / 2019 (Scenario 2)	Envisaged in 2021	Envisaged in 2022
Title 1 : Staff Expenditure	6.398.429	6.386.500	9.477.948,32	12.038.000	27%	13.343.500	13.875.000,00
11 Staff in active employment	4.674.964	5.186.400	6.794.000,00	10.181.000	50%	11.295.000	11.763.000,00
- of which establishment plan posts							
- of which external personnel							
12 Recruitment expenditure	175.432	261.100	971.948,32	445.000	-54%	342.000	277.000,00
13 Socio-medical services and training	169.989	190.000	325.000,00	250.000	-23%	305.000	375.000,00
14 Temporary assistance	1.378.044	749.000	1.387.000,00	1.162.000	-16%	1.401.500	1.460.000,00
Title 2: Building, equipment and miscellaneous expenditure	1.600.312	1.687.500	2.497.000,00	2.886.000	16%	3.114.000	3.205.000,00
20 Building and associated costs	868.135	1.000.500	1.100.000,00	1.180.000	7%	1.234.000	1.234.000,00
21 Movable property and associated costs	25.435	60.000	58.000,00	99.000	71%	99.000	99.000,00
22 Current administrative expenditure	83.027	62.000	104.000,00	176.000	69%	201.000	201.000,00
23 ICT	623.715	565.000	1.235.000,00	1.431.000	16%	1.580.000	1.671.000,00
Title 3: Operational expenditure	3.176.484	3.375.000	4.958.003,73	6.851.310	38%	6.968.901,60	7.140.156,60
30 Activities related to meetings and missions	943.055	715.000	1.043.323,68	1.410.000	35%	1.410.000	1.415.000,00
32 Horizontal operational activities	569.390	660.000	614.680,05	1.001.633,20	63%	1.059.901,60	1.150.156,60
36 Core operational activities	1.664.038	1.979.126	3.300.000,00	4.450.000,00	35%	4.499.000	4.575.000,00
TOTAL EXPENDITURE	11.175.225	11.428.126	16.932.952,05	21.785.633,20	29%	23.426.401,60	24.220.156,60

Payments appropriations

EXPENDITURE	Payment appropriations						
	Executed Budget 2017 (31/12/17)	Budget 2018	Envisaged in 2019 (Scenario 2)	Envisaged in 2020	VAR 2020 / 2019 (Scenario 2)	Envisaged in 2021	Envisaged in 2022
Title 1 : Staff Expenditure	6.398.429	6.386.500	9.477.948,32	12.038.000	27%	13.343.500	13.875.000,00
11 Staff in active employment	4.674.964	5.186.400	6.794.000,00	10.181.000	50%	11.295.000	11.763.000,00
- of which establishment plan posts							
- of which external personnel							
12 Recruitment expenditure	175.432	261.100	971.948,32	445.000	-54%	342.000	277.000,00
13 Socio-medical services and training	169.989	190.000	325.000,00	250.000	-23%	305.000	375.000,00
14 Temporary assistance	1.378.044	749.000	1.387.000,00	1.162.000	-16%	1.401.500	1.460.000,00
Title 2: Building, equipment and miscellaneous expenditure	1.600.312	1.687.500	2.497.000,00	2.886.000	16%	3.114.000	3.205.000,00
20 Building and associated costs	868.135	1.000.500	1.100.000,00	1.180.000	7%	1.234.000	1.234.000,00
21 Movable property and associated costs	25.435	60.000	58.000,00	99.000	71%	99.000	99.000,00
22 Current administrative expenditure	83.027	62.000	104.000,00	176.000	69%	201.000	201.000,00
23 ICT	623.715	565.000	1.235.000,00	1.431.000	16%	1.580.000	1.671.000,00
Title 3: Operational expenditure	3.176.484	3.375.000	4.958.003,73	6.861.633,20	38%	6.968.901,60	7.140.156,60
30 Activities related to meetings and missions	943.055	715.000	1.043.323,68	1.410.000,00	35%	1.410.000	1.415.000,00
32 Horizontal operational activities	569.390	660.000	614.680,05	1.001.633,20	63%	1.059.901,60	1.150.156,60
36 Core operational activities	1.664.038	1.979.126	3.300.000,00	4.450.000,00	35%	4.499.000	4.575.000,00
TOTAL EXPENDITURE	11.175.225	11.428.126	16.932.952,05	21.785.633,20	29%	23.426.401,60	24.220.156,60

Table 2 – Revenue Overview

Revenues	2017	2018	2019 (Scenario 2, allocated budget)	2020	2021	2022
	Revenues estimated by the agency including Amending Budget	Revenues estimated by the agency	Revenues estimated by the agency	Revenues estimated by the agency	Revenues estimated by the agency	Revenues estimated by the agency
EU contribution	10.322.000	10.529.000	15.910.000,00	20.646.000	22.480.000	23.023.000,00
Other revenue	853.225	899.126	1.022.952,05	1.139.633,20	1.178.401,60	1.197.156,60
Total revenues	**11.175.225**	**11.428.126**	**16.932.952,05**	21.785.633,20	23.426.401,60	24.220.156,60

REVENUES	2017	2018	2019 (Scenario 2)	Envisaged 2020	VAR 2020 / 2019	Envisaged 2021	Envisaged 2022
	Executed Budget	Revenues estimated by the agency	As requested by the agency		(Scenario 2)		
1 REVENUE FROM FEES AND CHARGES							
2. EU CONTRIBUTION	**10.322.000**	**10.529.000**	**15.910.000,00**	**20.646.000**	**30%**	**22.248.000**	**23.023.000,00**
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**	**248.626**	382.952,05	499.633,20	**30%**	538.401,60	557.156,60
of which EFTA	**252.977**	**248.626**	382.952,05	499.633	**30%**	538.401,60	557.156,60
of which Candidate Countries							
4 OTHER CONTRIBUTIONS	**566.261**	**640.000**	**640.000,00**	**640.000**	**0%**	**640.000**	**640.000,00**
of which delegation agreement, ad hoc grants							
5 ADMINISTRATIVE OPERATIONS	**33.986**	**10.500**	-	**0**		**0**	-
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT							
7 CORRECTION OF BUDGETARY IMBALANCES							
TOTAL REVENUES	**11.175.225**	**11.428.126,00**	**16.932.952,05**	**21.785.633,20**	29%	23.426.401,60	24.220.156,60

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

Budget Outturn	2015	2016	2017	2018
Revenue actually received (+)	10.069.280	11.034.366	11.223.387	11.572.995,00
Payments made C1 (-)	9.395.559	9.860.775	9.901.545	-10.345.736,00
Carry-over of appropriation (-)	674.521	1.176.717	1.376.731	-1.348.657,00
Cancellation of appropriations carried over (+)	80.675	38.616	90.916	108.302,00
Adjustment for carry over of assigned revenue appropriations from previous year (+)	800	3.127	49.519	124.290,00
Exchange rate differences (+/-)	278	-180	-12	-689,00
Adjustment for negative balance from previous year (-)				
TOTAL	**80.397**	**38.436**	**85.535**	**110.505,00**

Cancellation of appropriations[36]

- Cancellation of Commitment Appropriations

  No commitment appropriations were cancelled.

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

  No payment appropriations were cancelled.
- Cancellation of Payment Appropriations carried over

  (Fund source "C8" – appropriations carried over automatically from 2016 to 2017.)

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

A.3 Annex III: Human Resources – Quantitative

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

Staff population		**Authorised under EU budget 2017**	**Actually filled as of 31 12.2017**	**Authorised under EU budget for year 2018**	**Actually filled as of 31.12.2018**	**In draft budget for year 2019 Scenario 1**	**In draft budget for year 2019 Scenario 2**	**Envisaged in 2020**	**Envisaged in 2021**	**Envisaged in 2022**
Officials	AD									
	AST									
	AST/SC									
TA	AD	34	29	34	32	34	43	51	57	60
	AST	14	13	13	12	13	16	18	19	19
	AST/SC									
Total		**48**	**42**	**47**	**44**	**47**	**59**	**69**	**76**	**79**
CA GFIV		28	17	28	16	28	28	28	28	28
CA GF III		2	11	5	10	2	2	5	5	5
CA GF II			0	0	0	0	0	0	0	0
CA GFI			1	0	1	0	0	0	0	0
Total CA		**30**	**29**	**33**	**27**	**30**	**30**	**33**	**33**	**33**
SNE		**6**	**3**	**3**	**3**	**6**	**9**	**12**	**12**	**12**
Structural service providers										
TOTAL		**84**	**74**	**83**	**74**	**83**	**98**	**114**	**121**	**124**
External staff for occasional replacement						5	5	5	5	5

[36] Information to be updated in later version.

Table 2 – Multi-annual staff policy plan year 2020 – 2022

Category and grade	Establishment plan in EU Budget 2018		Filled as of 31/12/2018		Modifications in year 2018 in application of flexibility rule		Establishment plan in voted EU Budget 2019		Modifications in year 2019 in application of flexibility rule		Establishment plan 2020	Establishment plan 2021		Establishment plan 2022	
	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				6			6		6		6
AD 11															
AD 10		5		3				5			5		5		5
AD 9		10		4				12			12		12		12
AD 8		15		9				19			21		21		22
AD 7				3							3		6		8
AD 6				8							3		6		6
AD 5				1											
Total AD		**34**		**32**				**43**			**51**		**57**		**60**
AST 11															
AST 10															
AST 9															
AST 8															
AST 7		2		1				3			4		5		5
AST 6		5		2				7			8		8		8
AST 5		5		2				5			5		5		5
AST 4		1		4				1			1		1		1
AST 3				3											
AST 2															
AST 1															
Total AST		**13**		**12**				**16**			**18**		**19**		**19**
AST/SC1															
AST/SC2															
AST/SC3															
AST/SC4															
AST/SC5															
AST/SC6															
Total AST/SC															
TOTAL		**47**		**44**				**59**			**69**		**76**		**79**

A.4 Annex IV: Human Resources - Qualitative

A. Recruitment policy

Statutory Staff

The Agency continues to enhance the management of selection procedures with a focus on improving time to hire, developing good practices in recruitment and streamlining processes. The acquisition of a modern e-recruitment tool from another EU Agency would definitively help.

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

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

<u>Assistant Job Family:</u>

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

<u>Operational Job Family:</u>

- Junior Officer/Administrator Job Category (staff providing junior expertise in a specific field of knowledge): typically, these posts are filled by grades AD5, FG IV 13
- Officer/Administrator Job Category (staff providing officer expertise in a specific field of knowledge): typically, these posts are filled by grades AD6-AD7, FG IV 14-18
- Lead Officer/Administrator (staff providing top level expertise in a specific field of knowledge): typically, these posts are filled by grades AD8-AD9
- Team Leader Job Category (staff providing operational excellence with some managerial responsibilities): typically, these posts are filed by grades AD7-AD10, FG IV 14-18
- Special Advisor Job Category (staff providing direct assistance in a specific field of knowledge): typically, these posts are filled by grades AD9-AD12.

<u>Managerial Job Family:</u>

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

- Executive Director (filled by grades AD14-15)

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

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

Non-Statutory Staff

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

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

B. Appraisal of performance and reclassification/promotions

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

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

Table 1 - Reclassification of temporary staff/promotion of officials

Category and grade	Staff in activity at 1.01.Year 2018		How many staff members were promoted / reclassified in Year 2018		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		2			
AD 9		3		1	10
AD 8		8		1	4
AD 7		1			
AD 6		10		2	5
AD 5		1			
Total AD					
AST 11					
AST 10					
AST 9					
AST 8					
AST 7		1			
AST 6		1			
AST 5		3		1	7
AST 4		5		1	7
AST 3		3		1	2
AST 2					
AST 1					
Total AST					
AST/SC1					
AST/SC2					
AST/SC3					
AST/SC4					
AST/SC5					
AST/SC6					
Total AST/SC					
Total		**42**		**7**	

Table 2 - Reclassification of contract staff

Function Group	Grade	Staff in activity at 1.01.Year 2018	How many staff members were reclassified in Year 2018	Average number of years in grade of reclassified staff members
CA IV	17			
	16	1	1	2
	15			
	14	7		
	13	7	2	3
CA III	10	2	1	6
	9	8	1	4
	8	2		
CA II				
CA I	2	1	1	6
Total		**29**	**6**	

C. Mobility policy

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

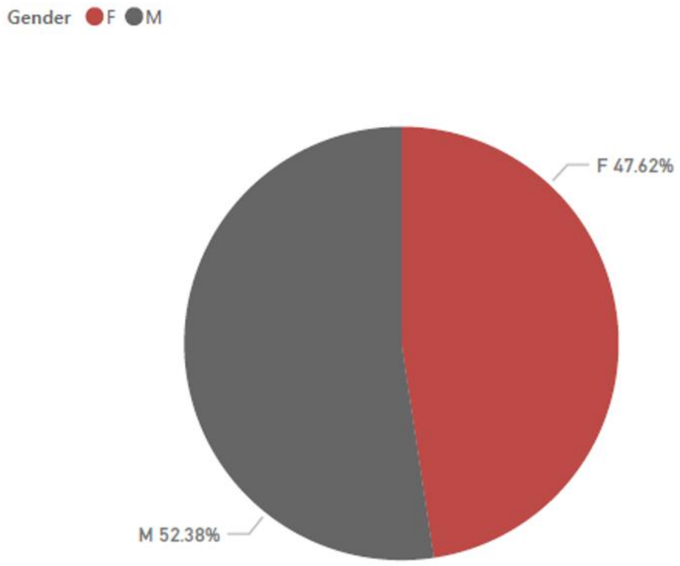
D. Learning and Development

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

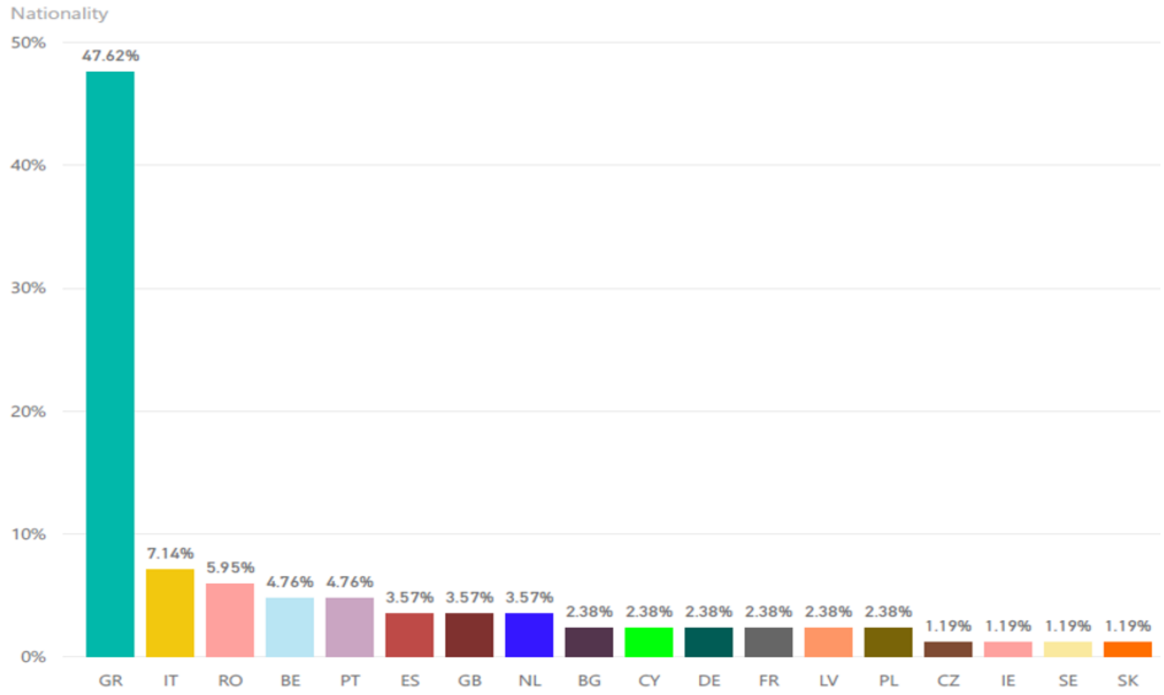
E. Gender and geographical balance

As of 31/12/2018 ENISA counts with 74 Staff members (44 TAs of which 32 are ADs and 12 are ASTs), 27 CAs and 3 SNEs.

The overall gender balance among ENISA staff shows a male prevalence that is understandable given the scope of the Agency's work. As a measure to promote equal opportunities, the terms of published vacancy notices prevent any kind of discrimination and the Selection Board's composition is balanced in term of gender and nationality as far as possible. In line with the European Commission's objective to achieve 40% female representation in managerial positions, the Agency nominated in 2016 and 2017 a French woman as Head of HR and a Swedish woman as Head of Finances and Procurement.



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



F. Schooling

A European School is located in Heraklion and is used by Staff members of ENISA. The rest of ENISA pupils attend various schools in Athens and in other MS based on service level agreement concluded with a number of international schools.

A.5 Annex V: Buildings

ENISA will continue to have two office spaces in Heraklion and Athens.

A.6 Annex VI: Privileges and immunities[37]

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

[37] Updates will be provided in next versions.

A.7 Annex VII: Evaluations

ENISAs uses an internal monitoring system (MATRIX) and is used for project management. Monthly reporting and the ENISA management team uses regularly this information. Moreover, ENISA have implemented a mid-term review procedure and regular monthly management team meetings.

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

A.8 Annex VIII: Risks Year 2020

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

A.9 Annex IX: Procurement plan Year 2020

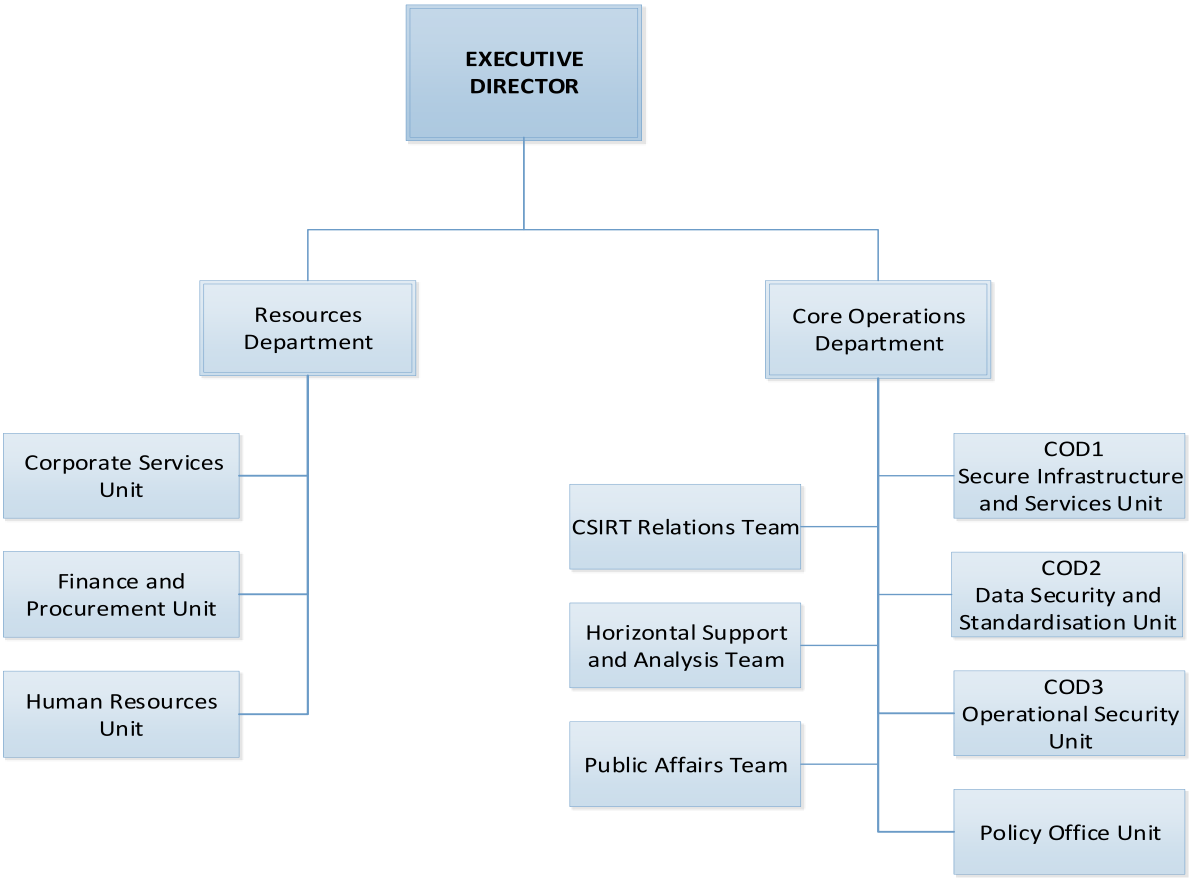
[To be added in the second part of 2019.]

A.10 Annex X: ENISA Organisation

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

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

The ENISA organisation valid at the end of 2018 is provided in the image below.

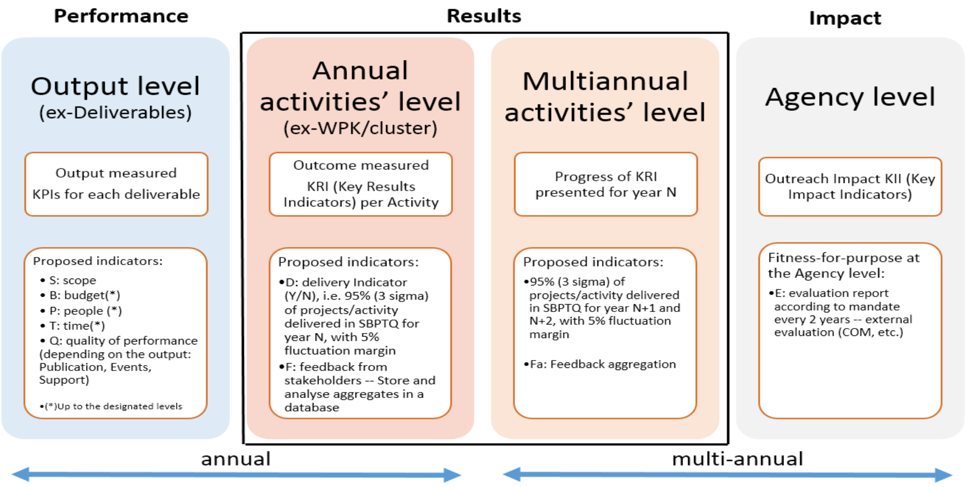

EXECUTIVE DIRECTOR
Resources Department
Core Operations Department
Corporate Services Unit
Finance and Procurement Unit
Human Resources Unit
CSIRT Relations Team
Horizontal Support and Analysis Team
Public Affairs Team
COD1 Secure Infrastructure and Services Unit
COD2 Data Security and Standardisation Unit
COD3 Operational Security Unit
Policy Office Unit

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

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

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

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


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:

a. Adherence to the scope of the deliverable or project
b. Budget (or financial resources) available to the output or project, remaining within prescribed levels with a ±5% margin
c. People (or human resources) available to the output or project, remaining within prescribed levels with a ±5% margin
d. Time available to carry out the output or project remaining within prescribed levels with a ±5% margin
e. Quality of performance depending on the type of output, according to the classification of output in the work program (being, publication, event, support).

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

a. Delivery indicator aiming at delivery of at least 95% against work program planning. This is equivalent to a 3σ (3 Sigma) organisation (reaching between 93.3% and 99,3%); clearly the Agency has historically proven its operational ability to deliver at much higher level, meeting 6σ (6 Sigma) specification requirements (at 99,99%). However allowing for a 3 Sigma level meets the above-mentioned deviation rate of ±5%.[38] The criteria used, being scope, budget, people, time and quality, they all refer to the proper execution of the project leading up to the production of output. This evaluation is done at the end of the project within ENISA.

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

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

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

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

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

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

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

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

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

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

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

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

Annex C: List of Acronyms

ABB: Activity Based Budgeting
APF: Annual Privacy Forum
BEREC: Body of European Regulators of Electronic Communications
cPPP: Cyber Security Public-Private Partnership
CE2020: Cyber Europe 2020
CEF: Connecting Europe Facility
CEP: Cyber Exercises Platform
CERT-EU: Computer Emergency Response Team for the EU Institutions, Bodies and Agencies
CEN: European Committee for Standardization
CENELEC: European Committee for Electrotechnical Standardization
CIIP: Critical Information Infrastructure Protection
CSCG: ETSI CEN-CENELEC Cyber Security Coordination Group
CSIRT: Computer Security Incidents Response Teams
CSSU: Corporate Stakeholders and Services Unit
COD: Core Operational Department
COM: European Commission
CSS: Cyber Security Strategy
CNW: CSIRTs Network
DG: EC Directorate-General
DG CONNECT: EC Directorate-General CONNECT
DPA: Data Protection Authorities
DPO: Data Protection Officer
DSM: Digital Single Market
E: Event, type of output i.e. conference, workshop, and seminar
EB: ENISA Executive Board
EC3: European Cybercrime Centre, Europol
ECA: European Court of Auditors
ECSM: European Cyber Security Month
ECSO: European Cyber Security Organisation
ED: Executive Director
EDO: Executive Directors Office
EDPS: European Data Protection Supervisor
eID: electronic Identity
eIDAS: Regulation on electronic identification and trusted services for electronic transactions in the internal market
ETSI: European Telecommunications Standards Institute
EU: European Union
FAP: Finance, Accounting and Procurement
FIRST: Forum of Incident Response and Security Teams
FM: Facilities Management
FTE: Full Time Equivalents
H2020: Horizon 2020
HoD: Head of Department
HR: Human Resources
IAS: Internal Audit Service
ICC & IAC: Internal Control Coordination and Internal Audit Capability
ICS/SCADA: Industrial Control Systems/Supervisory Control and Data Acquisition
ICT: Information and Communication Technologies
IS: Information Systems
ISP: Internet Service Providers
IXP: Internet exchange point
KII: Key Impact Indicator
KPI: Key Performance Indicator
LEA: Law Enforcement Agency
MFF: Multi Annual Financial framework
M2M: Machine to Machine
MB: Management Board
MS: Member State
NAPAC: National Public Authority Representatives Committee
NCSS: National Cyber Security Strategies
NIS: Network and Information Security
NISD: NIS Directive
NLO: National Liaison Officer
NRA: National Regulatory Authority
O: Output
OES: Operators of Essential Services
P: Publication, type of output covering papers, reports, studies
PDCA: Plan-Do-Check-Act
PETs: Privacy Enhancing Technologies
PPP: Public Private Partnership
PSG: Permanent Stakeholders Group
Q: Quarter
QMS: Quality Management System
R&D: Research and Development
RD: Resources Department
S: Support activity, type of output
SB: Supervisory Body
SCADA: Supervisory Control and Data Acquisition
SDO: Standard Developing Organization
SME: Small and Medium Enterprise
SO: Strategic Objectives
SOP: Standard Operating Procedure
SRAD: Stakeholder Relations and Administration Department
TF-CSIRT: Task Force of Computer Security Incidents Response Teams
TLR: Traffic Light Rating
TRANSITS: Computer Security and Incident Response Team (CSIRT) personnel trainings
TSP: Trust Service Provider
US: United States of America
WP: Work programme

Annex D: List of Policy References

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

Year	Reference	Policy/legislation reference. Complete title and link
2017		
	2017 Cybersecurity Strategy	JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN/2017/0450 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN
	Cybersecurity Act, Proposed ENISA regulation	European Commission, Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act''), COM(2017) 477, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN
	Council Conclusions on 2017 Cybersecurity Strategy	Council Conclusions of 20 November 2017 on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU -- http://www.consilium.europa.eu/media/31666/st14435en17.pdf
2016		
	The NIS Directive	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30, available at: ELI: http://data.europa.eu/eli/dir/2016/1148/oj
	COM communication 0410/2016 on cPPP	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0410
	COM decision C(2016)4400 on cPPP	COMMISSION DECISION of 5.7.2016 on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation, Brussels, 5.7.2016, C(2016) 4400 final, available at (including link to the Annex): https://ec.europa.eu/digital-single-market/en/news/commission-decision-establish-contractual-public-private-partnership-cybersecurity-cppp
	Joint Communication on countering hybrid threats	JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats a European Union response, JOIN/2016/018 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018
	General Data Protection Regulation (GDPR)	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88, available at: http://data.europa.eu/eli/reg/2016/679/oj
	LEA DP Directive	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131, available at: http://data.europa.eu/eli/dir/2016/680/oj
	PNR Directive	Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132–149, available at: ELI: http://data.europa.eu/eli/dir/2016/681/oj
2015		
	Digital Single Market Strategy for Europe (DSM)	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital

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

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

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

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

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