



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA PROGRAMMING DOCUMENT 2020–2022

Including Multiannual planning, Work
programme 2020 and Multiannual staff planning



NOVEMBER 2019

CONTACT

For contacting ENISA please use the following details:

info@enisa.europa.eu

website: www.enisa.europa.eu

LEGAL NOTICE

This publication presents the European Union Agency for Cybersecurity (ENISA) Programming Document 2020-2022 as approved by the Management Board in Decision No MB/2019/16. The Management Board may amend the Work Programme 2020-2022 at any time. This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2020 Reproduction is authorised provided the source is acknowledged.

Copyright for the image on the cover and internal pages: © Shutterstock For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

Luxembourg: Publication Office of the European Union, 2020

PDF ISBN 978-92-9204-324-7 ISSN 2467-4176 DOI 10.2824/52836 TP-AH-20-001-EN-N

Print ISBN 978-92-9204-330-8 ISSN 2467-4397 DOI 10.2824/95513 TP-AH-20-001-EN-C

Printed by Bietlot in Belgium



ENISA PROGRAMMING DOCUMENT 2020–2022

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TABLE OF CONTENTS

Foreword by the Executive Director	8
Mission statement	11
PART I GENERAL CONTEXT	15
PART II MULTI-ANNUAL PROGRAMME 2020–2022	19
ACTIVITY 1 – EXPERTISE. ANTICIPATE AND SUPPORT EUROPE’S KNOWLEDGE IN FACING EMERGING CYBERSECURITY CHALLENGES	19
Objective 1.1. Improving knowledge on the security of digital developments	19
Objective 1.2. Cybersecurity threat landscape and analysis	20
Objective 1.3. Research & development and innovation	20
ACTIVITY 2 – POLICY. PROMOTE NETWORK AND INFORMATION SECURITY AS AN EU POLICY PRIORITY	21
Objective 2.1. Supporting EU Policy Development	21
Objective 2.2. Supporting EU Policy Implementation	22
ACTIVITY 3 – CAPACITY. SUPPORT EUROPE IN MAINTAINING STATE-OF-THE-ART NETWORK AND INFORMATION SECURITY CAPACITIES	22
Objective 3.1. Assist Member States’ capacity building	22
Objective 3.2. Assist in the EU institutions’ capacity building	23
Objective 3.3. Awareness raising	24
ACTIVITY 4 – COOPERATION. FOSTER THE OPERATIONAL COOPERATION WITHIN THE EUROPEAN CYBERSECURITY COMMUNITY	25
Objective 4.1. Cyber crisis cooperation	25
Objective 4.2. Community building and operational cooperation	25
ACTIVITY 5 – CERTIFICATION. DEVELOP CYBERSECURITY CERTIFICATION SCHEMES FOR DIGITAL PRODUCTS, SERVICES AND PROCESSES	26
Objective 5.1. Support activities related to cybersecurity certification	26
Objective 5.2. Developing candidate cybersecurity certification schemes	27
ACTIVITY 6 – ENABLING. REINFORCE ENISA’S IMPACT	27
Objective 6.1. Management and compliance	27
Objective 6.2. Engagement with stakeholders and international relations	28
MONITORING THE PROGRESS AND ACHIEVEMENTS OF THE AGENCY. SUMMARIZING KEY INDICATORS FOR THE MULTI-ANNUAL ACTIVITIES	29
HUMAN AND FINANCIAL RESOURCE OUTLOOK FOR 2020-2022	29

PART III

WORK PROGRAMME YEAR 2020

31

ACTIVITY 1 – EXPERTISE. ANTICIPATE AND SUPPORT EUROPE'S KNOWLEDGE IN FACING EMERGING CYBERSECURITY CHALLENGES

31

Objective 1.1. Improving knowledge on the security of digital developments

31

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

31

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

32

Output O.1.1.3 – Building knowledge on Artificial Intelligence security

33

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

33

Output O.1.1.5 – Building knowledge on maritime security

34

Output O.1.1.6 – Building knowledge on cryptographic algorithms

35

Objective 1.2. Cybersecurity Threat Landscape and Analysis

35

Output O.1.2.1 – Annual ENISA Threat Landscape report

35

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

36

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

37

Output O.1.2.4 – Supporting PSIRTs and NIS sectoral incident response expertise

38

Objective 1.3. Research & Development, Innovation

38

Output O.1.3.1 – Supporting EU research & development programmes

38

Summary of the outputs and performance indicators in Activity 1 – Expertise

39

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

40

Objective 2.1. Supporting EU policy development

40

Output O.2.1.1 – Supporting policy developments in NIS Directive sectors

40

Objective 2.2. Supporting EU policy implementation

40

Output O.2.2.1 – Recommendations supporting implementation of the eIDAS Regulation

40

Output O.2.2.2 – Supporting the implementation of the work programme of the Cooperation Group under the NIS Directive

41

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

41

Output O.2.2.4 – Guidelines for the European standardisation in the field of ICT security

42

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

42

Output O.2.2.6 – Support the MS in improving the cybersecurity of 5G networks

42

Summary of the outputs and performance indicators in Activity 2 – Policy

43

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

44

Objective 3.1. Assist Member States' capacity building

44

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

44

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

44

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

44

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

45

Objective 3.2. Support EU institutions' capacity building

45

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

45

Output O.3.2.2 – Cooperation with relevant EU institutions, agencies and other bodies on cybersecurity initiatives

46

Objective 3.3. Awareness raising

46

Output O.3.3.1 – European Cyber Security Challenges

46

Output O.3.3.2 – European Cyber Security Month deployment

46

Output O.3.3.3 – Support EU MS in cybersecurity skills development

46

Summary of the outputs and performance indicators in Activity 3 – Capacity

47

ACTIVITY 4 – COOPERATION. FOSTER THE OPERATIONAL COOPERATION WITHIN THE EUROPEAN CYBERSECURITY COMMUNITY	48
Objective 4.1. Cyber crisis cooperation	48
Output O.4.1.1 – Planning of Cyber Europe 2020	48
Output O.4.1.2 – Support activities for cyber exercises	48
Output O.4.1.3 – Support activities for cybersecurity collaboration with other EU institutions and bodies	49
Output O.4.1.4 – Supporting the implementation of the information hub	49
Output O.4.1.5 – Supporting the EU Cyber Crisis Cooperation Blueprint	50
Objective 4.2. Community building and operational cooperation	51
Output O.4.2.1 – EU CSIRTs Network support	51
Output O.4.2.2 – Support the fight against cybercrime and collaboration across CSIRTs, LEA and other operational communities	51
Output O.4.2.3 – Supporting the operations of MeliCERTes platform	51
Summary of the outputs and performance indicators in Activity 4 – Community	52
ACTIVITY 5 – CYBERSECURITY CERTIFICATION. DEVELOPING SECURITY CERTIFICATION SCHEMES FOR DIGITAL PRODUCTS, SERVICES AND PROCESSES	53
Objective 5.1. Support activities related to cybersecurity certification	53
Output 5.1.1 – Support the European Cybersecurity Certification Group, potential subgroups thereof and the Stakeholder Cybersecurity Certification Group	53
Output 5.1.2 – Research and analysis of the market as an enabler for certification	53
Output 5.1.3 – Set-up and maintenance of a certification portal and associated services	53
Objective 5.2. Developing candidate cybersecurity certification schemes	54
Output 5.2.1 – Hands on tasks in the area of cybersecurity certification of products, services and processes	54
Output 5.2.2 – Tasks related to specific candidate schemes and ad hoc working groups	54
Summary of the outputs and performance indicators in Activity 5 – Certification	54
ACTIVITY 6 – ENABLING. REINFORCE ENISA'S IMPACT	55
Objective 6.1. Management and compliance	55
Management	55
Policy Unit	55
Internal control	56
IT activities	56
Finance and Procurement	56
Human Resources	57
Legal affairs, data protection and information security coordination	58
Objective 6.2. Engagement with stakeholders and international activities	59
Stakeholder communication and dissemination activities	59
International relations	61
List of outputs in the Work Programme 2020	62

ANNEX 1	
RESOURCE ALLOCATION PER ACTIVITY 2020–2022	65
ANNEX 2	
HUMAN AND FINANCIAL RESOURCES 2020–2022	68
ANNEX 3	
HUMAN RESOURCES — QUANTITATIVE	72
ANNEX 4	
HUMAN RESOURCES – QUALITATIVE	74
ANNEX 5	
BUILDINGS	80
ANNEX 6	
PRIVILEGES AND IMMUNITIES	81
ANNEX 7	
EVALUATIONS	82
ANNEX 8	
RISKS 2020	83
ANNEX 9	
PROCUREMENT PLAN 2020	84
ANNEX 10	
ENISA ORGANISATION	85
ANNEX 11	
SUMMARISING THE KEY INDICATORS FOR THE MULTIANNUAL ACTIVITIES	86
ANNEX 12	
LIST OF ACRONYMS	90



ANNEX 13
LIST OF POLICY REFERENCES

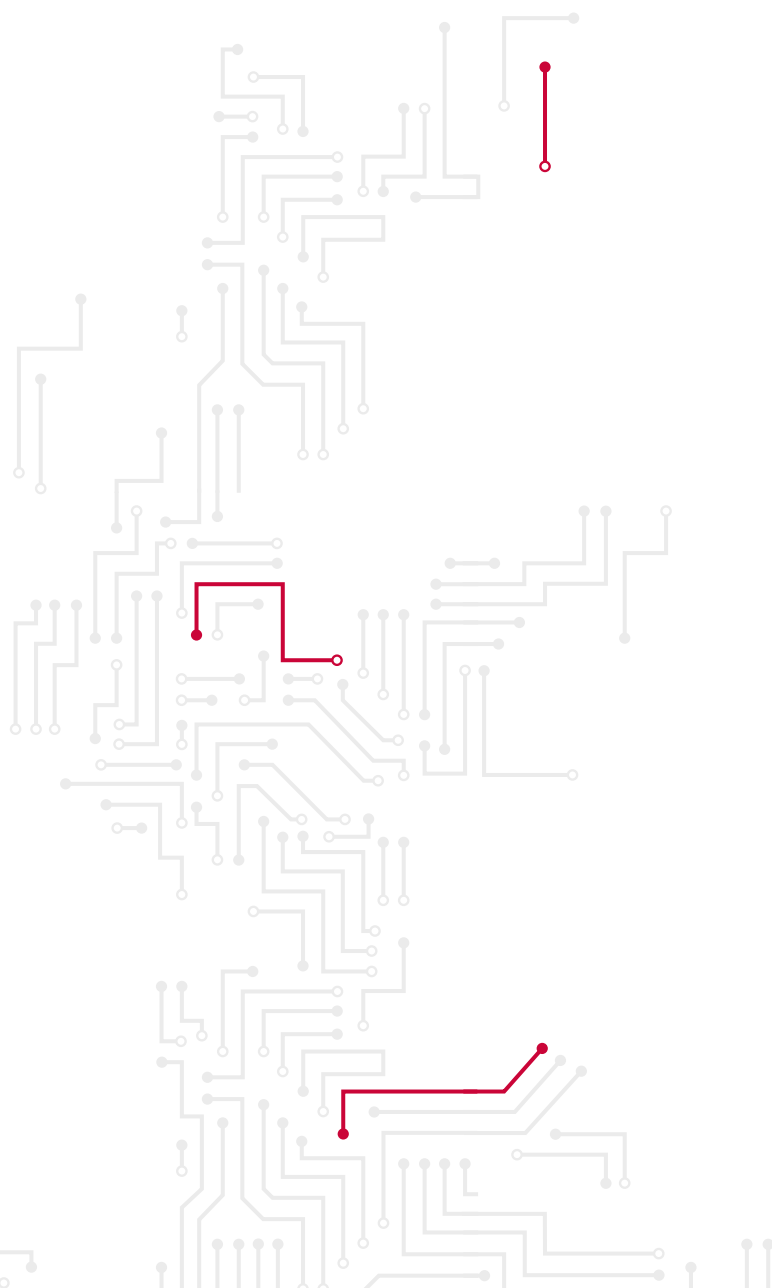
91

ANNEX 14
OUTPUT SYNERGIES

94

ANNEX 15
OUTPUT PRIORITIES

96





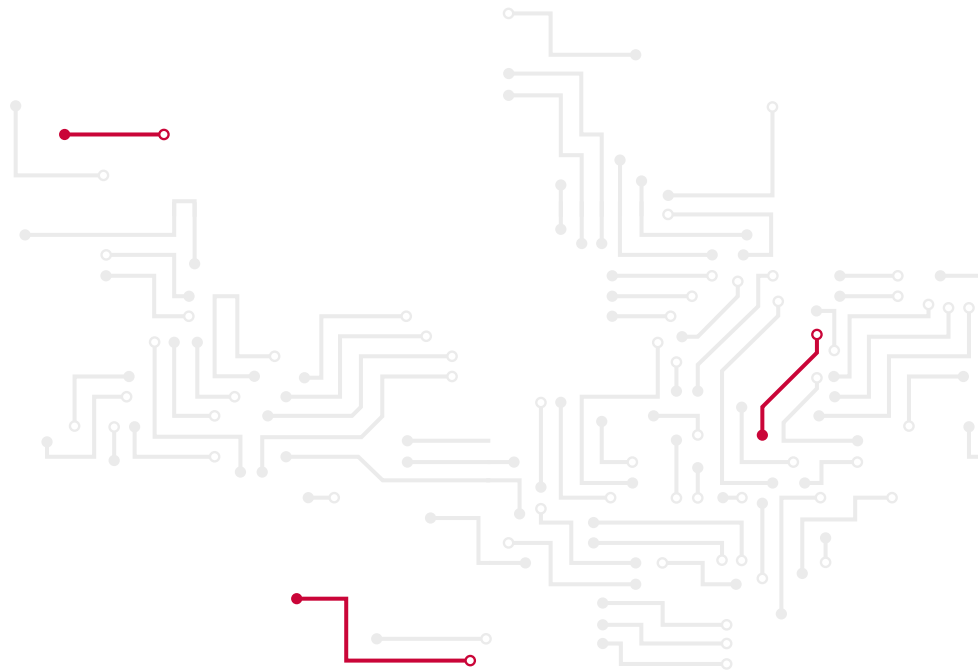
FOREWORD BY THE EXECUTIVE DIRECTOR

In June 2019 the new Cybersecurity Act (CSA) came into force giving ENISA a new and permanent mandate. It is a great pleasure for me to introduce the ENISA Programming Document 2020-2022, which is the first programming document that is entirely within the scope of the new mandate. In doing so, I would like to thank the previous Executive Director, Prof. Dr. Udo Helmbrecht for steering the Agency throughout the last 10 years and for overseeing the initial actions to put the CSA into effect.

Indeed, the Agency has taken a very proactive stance to the implementation of the CSA and has already made significant progress in developing the new areas of work foreseen by the act. In this respect, ENISA has laid the groundwork to fully implement the Cybersecurity Certification Framework. In parallel, the Agency has supported the European Union to respond to cybersecurity challenges connected to 5G, held cybersecurity exercises in preparation of the European Parliament elections. Additionally, it has been working hard to integrate concepts of the 'blueprint' into the cyber-crisis management approach and unveiling an innovative tool for knowledge management in this area, OpenSESAME, based on the principles of Artificial Intelligence.

Looking ahead, there are a number of significant cybersecurity challenges to which the EU must respond, if we are to achieve the goals that we have set ourselves in creating a strong digital Europe. The ENISA Threat Landscape analysis revealed that building up necessary skills and capacities is an important task to achieve this goal. Moreover, the report showed that the 'technical language' used by most cyberthreat intelligence is perceived as a hindrance in raising the awareness within the industry, within different policy areas and within the public at large. ENISA will tackle these issues as a matter of priority in the years to come.

Equally important are a number of social and economic challenges. ENISA will need to help the EU to respond to new complex developments such as 'fake news' and disinformation techniques. We also need to develop a deeper knowledge of the underlying economics of cybersecurity and use this knowledge to ensure that cybersecurity policy is supporting EU industrial policy. This will help setting the conditions for the EU industry to leverage the high level of expertise that the EU has in this area and to prosper in emerging markets. Finally, there are a number of technological challenges, which are questioning traditional approaches to cybersecurity due to a combination of high scalability requirements (e.g. IoT), short time-to-market and strong cost drivers. Examples of such technologies include not only IoT, but also AI, robotics and 5G networks. In the more distant future, Quantum Computing poses a threat to traditional cryptographic methods, whereas Quantum Safe Cryptography is preparing the community's response.



The tasks and actions outlined in the ENISA Programming Document 2020-2022 will help the Union to prepare and respond to these challenges, whilst making the most out of the new obligations arising from the CSA. Recent discussions on Digital Sovereignty and Digital Strategic Autonomy indicate that there is room to build on the successes of the Network & Information Security Directive and the Agency is well positioned to help and advise the EU institutions and the Member States in developing this important work.

These are only a few of the considerations that we will have to take into account over the next few years as we continue to work together with our stakeholders to create a stronger, more secure digital society. ENISA looks forward to working together with all of you with the firm belief that we can only meet the challenges of the future through cooperation and creating synergies .

Juhan Lepassaar
Executive Director

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 founded in 2004 to contribute to the overall goal of ensuring a high level of NIS within the EU by acting as a centre of expertise and supporting the Member States in capacity building.

In 2019, the mandate¹ of the Agency has been extended and the role of ENISA has been reinforced within 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: assess and improve Europe's knowledge in addressing emerging cybersecurity challenges.

- Policy: support cybersecurity policy making and implementation in the Union.
- Capacity: support capacity building across the Union (e.g. through trainings, recommendations and awareness raising activities).
- Cooperation: foster the cooperation within the EU cybersecurity community (e.g. by supporting the CSIRTs activities and network, coordination of pan-European cyber exercises).
- Certification: support the implementation of the cybersecurity certification framework for ICT products, services and processes.
- Enabling: reinforcing ENISA's impact and efficiency (e.g. through engagement with the stakeholders and international relations).

The area 'Certification' represents a new activity for ENISA and is an outcome of the Cybersecurity Act.

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

ENISA's approach is strongly impact driven, based on the involvement of all relevant stakeholder communities, with a strong emphasis on pragmatic solutions that offer a sensible mix of short-term and long-term improvements. The Agency will

¹ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15–69, available at: <http://data.europa.eu/eli/reg/2019/881/oj>

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 for a more agile and flexible approach to achieving its mission.

PRIORITIES

● **EU policy development and implementation:**

Proactively contributing to the development of NIS policies, 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 the aim to promote 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 reports on the current state of implementation of the EU legal framework.

● **Capacity building:**

Contributing to the improvement of EU and national public authorities' capabilities and expertise, such as incident response and 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, and by appropriately addressing regulatory issues related to information sharing.

● **Knowledge and information, awareness raising:**

Becoming the EU's key information hub 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

the aim to provide guidance to businesses and citizens across the EU.

Regularly organising awareness raising activities in coordination with the 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 European 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 (like Cyber Europe).

Supporting the operational cooperation as secretariat of the CSIRTs Network (as per NIS Directive provisions) by, for instance, ensuring the smooth functionality of the CSIRTs Network's IT infrastructure and communication channels and by guaranteeing a structured cooperation with CERT-EU, European Cybercrime Centre (EC3), EDA and other relevant EU bodies in line with the European Commission proposal for the Cybersecurity Act².

² 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>

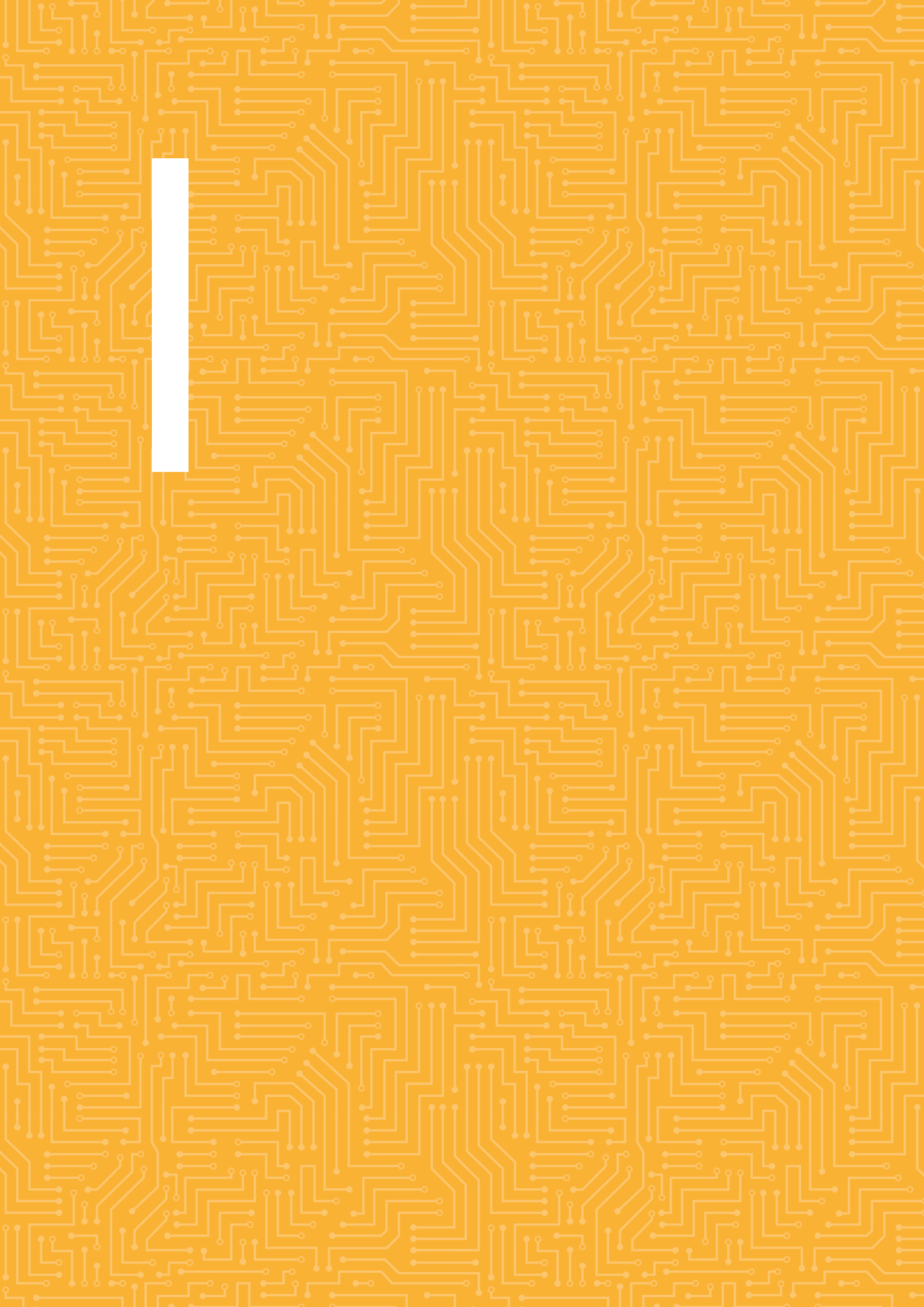
- **Support the European Commission and assist Member States regarding the EU cybersecurity Blueprint**

As presented in the European Commission's recommendation for a coordinated response to large-scale cybersecurity incidents and crises at the EU level³.

- **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 European 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 European Commission in its role as Chair of the European Cybersecurity Certification Group.

³ European Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises.



PART I

GENERAL CONTEXT

THREAT LANDSCAPE

2018 brought significant changes for the cyberthreat landscape and the forecasting capability of ENISA. These changes were triggered by 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 also been made by the defenders. Through the emergence of active defence, threat agent profiling has led to a more efficient identification of attack practices and malicious artefacts, thus leading to more efficient defence techniques and attribution rates. Initial successes have been achieved through the combination of cyberthreat intelligence (CTI) and traditional intelligence. This is a clear indication of the need to open CTI to other related disciplines to increase the quality of assessments and attribution. Finally, defenders have increased the levels of training to compensate skill shortage in the area of CTI. The high interest of stakeholders in such trainings is a clear indication 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 CTI. 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, thus affecting 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 a major focus for the defenders. Public organisations struggle with staff retention due to strong competition from the 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 due 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/best 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 evaluated and analysed against the content of the ENISA Threat Landscape Report 2018 (ETL 2018). Open issues based on these trends will be identified. Additionally, ENISA will propose measures to be taken in the areas of policy, business and research/education. They serve as recommendations and will be taken into account for future activities of ENISA and its stakeholders.

Regarding all these developments, ENISA has identified numerous activities to address current trends in the cyberthreat landscape and increase knowledge and capability levels for different stakeholder groups. The content of the present programme document aims at activities that will result in less exposure to the aforementioned cyberthreats.

POLICY INITIATIVES

Since its foundation 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 are high on the EU policy agenda, particularly 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 the Member States and EU institutions in reinforcing NIS across Europe. In particular, the recent adoption of the European Directive of the European Parliament and the Council on measures to ensure a high common level of network and information security calls for an increased commitment by ENISA to support a coherent approach towards NIS across Europe.

With the adoption of the NIS Directive (2016), the fields of action were extended to accompany the evolution of NIS in Europe. ENISA plays a key role in the following activities in particular:

- contributing to the NIS technical and operational cooperation by actively supporting cooperation between Member States CSIRTs within the European CSIRTs Network and the NIS Cooperation Group;
- providing input and expertise for collaboration between competent national authorities at policy level in the framework of the cooperation group established by the NIS Directive;
- supporting the strengthening of the NIS of EU institutions in close cooperation with CERT-EU and the institutions themselves.

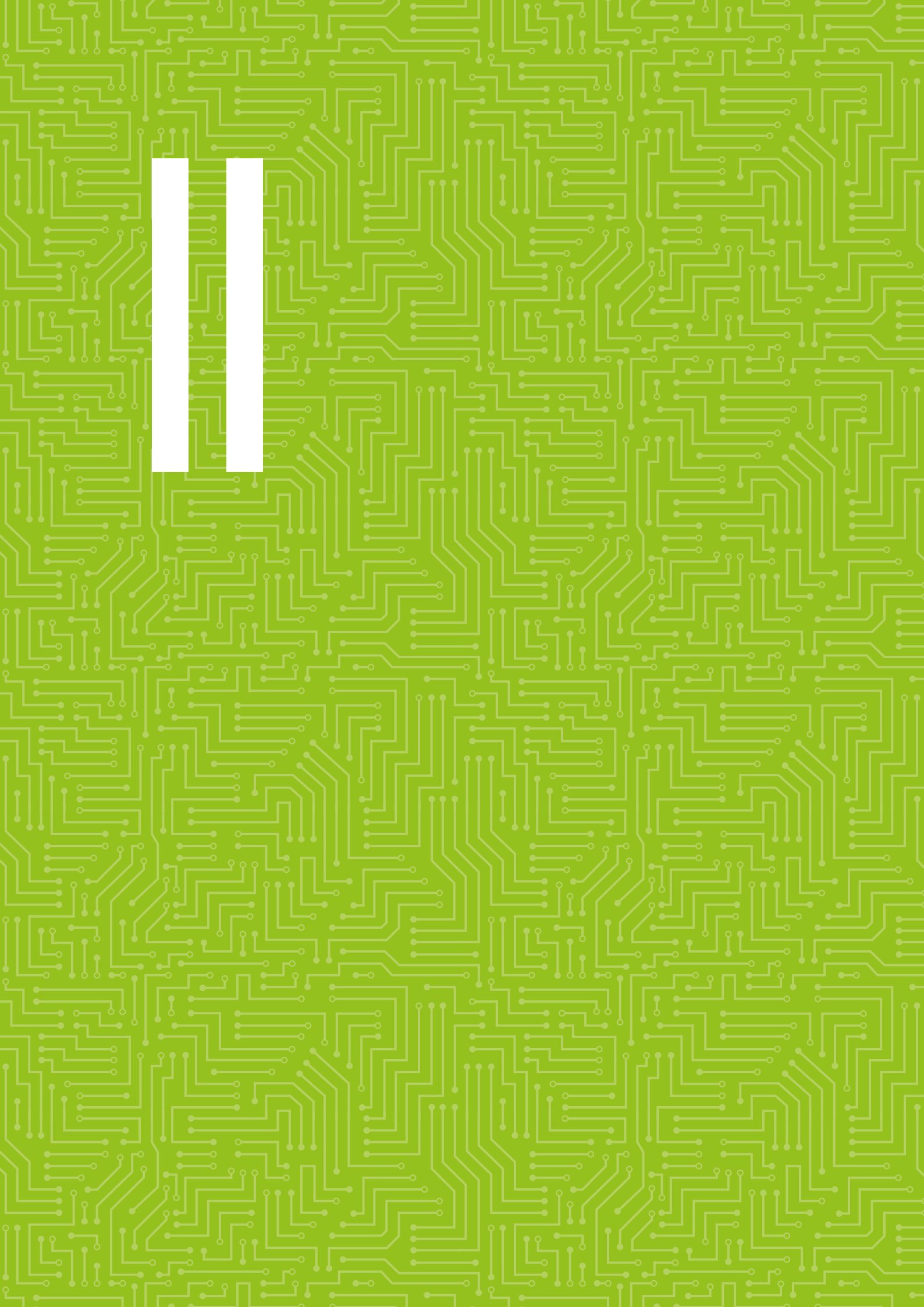
In parallel, ENISA will continue to contribute to the reinforcement of NIS as a driver of the DSM and more generally of economic growth in Europe, including the development of NIS and related ICT industries.

The publication of the new EU cybersecurity package on 13 September 2017 with its set of legislative and non-legislative measures has identified ENISA as a key pillar of the EU's ambition to reinforce cybersecurity across Europe, which is documented in the Cybersecurity Act⁴, which provides for the strengthening of ENISA.

In addition to strengthening ENISA, the Cybersecurity Act creates a framework for European Cybersecurity Certification schemes with the aim of creating a digital single market for ICT products, services and processes. ENISA will play a significant role in the preparation of the candidate schemes, contributing to the harmonisation of the EU cybersecurity certification.

⁴ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), available at: <https://eur-lex.europa.eu/eli/reg/2019/881/oj>





PART II

MULTI-ANNUAL PROGRAMME 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

Objective 1.1. Improving knowledge on the security of digital developments

Priorities

- Carry out regular stocktaking of EU expertise on the challenges of NIS related to existing or future services and technologies and making this information available to the EU NIS community;
- Among these challenges, focus on key issues to offer analyses and general recommendations;

- In particular, seek to explore issues related to software (e.g. mobile), ICS/SCADA, smart infrastructures and IoT, AI security and relevant technologies in sectors covered by the NIS Directive.

Guidelines

- Priority will be given to the collection and analysis of expertise provided by the competent authorities of the national NIS, close cooperation with them to support their stocktaking and the preparation of analyses and recommendations which will allow voluntary experts from these authorities and other relevant stakeholders to participate in their work;
- Focus on challenges of significant added value for the EU NIS community and on aspects that may affect the functioning of critical economic and societal functions with the EU, as foreseen in the NIS Directive (e.g. expertise relevant to essential service operators);
- Take a holistic approach encompassing the technical, organizational, regulatory and policy dimensions of NIS as well as different relevant approaches, including the user's perspective and work on a multiannual basis whenever possible to deepen understanding of the identified issues.

Added-value

- Provide European-wide visibility of the existing NIS expertise, in particular developed at national level;
- Foster common understanding of NIS challenges across the EU NIS community and highlighting best practices to address those challenges by

offering tailored, high quality and up-to-date analysis and recommendations;

- Raising awareness among operators, European institutions and national public authorities of the growing security challenges that should be addressed at technical and political level;
- Supporting the Agency's work listed under Activities 2 (Policy), 3 (Capacity), 4 (Cooperation) and 5 (Certification) by providing advice on challenges that may influence the development and implementation of EU NIS policy, national and European capacity building as well as crisis and CSIRT cooperation.

Objective 1.2. Cybersecurity threat landscape and analysis

Priorities

- Conducting an annual EU threat landscape analysis providing a general technical assessment of existing and expected threats and their causes;
- Prepare annual analyses of national incident reports in the context of the implementation of the telecommunications package, eIDAS Regulation and the NIS Directive;
- Disseminate relevant threat related information through relevant channels and networks, taking into account the sensitivity of the information;
- Regularly provide a concise overview on cyber threats as they have evolved in incidents. This information should provide a neutral overview of the results of the available open source evidence.

Guidelines

- Seek synergies between national incident reports in the above-mentioned analyses;
- Ensure that the EU threat landscape benefits from relevant sources of information, in particular vendor reports, national threat assessments, researchers, media etc.;
- Seek to improve visibility of these results to the EU NIS community by providing coherently generated materials for various stakeholders;
- Collect and analyse information on the threat landscape related to the sectors of the NIS Directive and publish regular reports on the EU cybersecurity situation;

Added-value

- Offer an independent EU-wide synthesis on technical threats of general interest to the EU, in particular in the context of the implementation of the NIS Directive (essential service operators, digital service providers);

- Improve general awareness of threats to national and European public and private entities and bodies and promote mutual understanding among national competent authorities of current and future threats;
- Establish a dialogue between relevant threat intelligence stakeholders in the form of an interaction model, including a community and an interaction platform;
- Assist stakeholders in developing threat intelligence/threat analysis capabilities ; support their activities and provide a threat analysis tailored to their needs;
- Support other activities by providing advice on threats that may affect EU cybersecurity;

Objective 1.3. Research & Development, Innovation

Priorities

- Assist Member States and the European Commission in defining EU priorities for R&D and deployment in the field of cybersecurity;
- Participation in relevant activities promoted by the Panel established by the proposed regulation⁵ establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the network of National Coordination Centres;
- Built on ENISA's support to the Member States and economic operators for cybersecurity preparedness and resilience as well as on certification and standardisation; contribute to research and deployment priorities and formulate technical requirements.

Guidelines

- Provide the secretariat of the National Public Authorities Committee of ECSO (NAPAC);
- Support cooperation between national public authorities on issues related to the definition of R&D and, where appropriate, liaise with other stakeholders represented within the ECSO;
- Participate in the activities of the proposed European Cybersecurity Industrial, Technology and Research Competence Centre and the network of National Coordination Centres.

Added-value

- Help to reduce the gap between research and implementation;

⁵ <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-establishing-european-cybersecurity-industrial-technology-and-research>

- Contribute to cybersecurity developments in the context of the forthcoming 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

Objective 2.1. Supporting EU Policy Development

Priorities

- Carry out a regularly updated stocktaking of current and future EU policy initiatives with NIS implications and make it available to the European Commission and national competent NIS authorities;
- Support the activities of the Cooperation Group in the field of new policy developments;
- Focus in particular on policies related to the sectoral dimension of NIS and on policies dedicated to cybersecurity to ensure coherence with the framework and principles agreed on in the NIS Directive;

- Seek to identify, as far as possible, all NIS challenges that may require policy developments at EU level;
- Build on this stocktaking and take into account the previously identified NIS challenges and offer advice to the European Commission and other relevant institutions of the Union on these policy developments.

Guidelines

- Work closely with the European Commission to take stock of current and future initiatives;
- Benefit from its work under Objective 1 on NIS challenges and threats to give advice on possible new policy developments;
- Promote dialogue between and with experts from national NIS competent authorities and other relevant stakeholders to develop sound and high quality expertise to advise on the developments of EU policies;
- Ensure the coherence of its work on DSM-related policy developments with the work carried out within the ECSO framework and, when appropriate, contribute to this work in accordance with its responsibilities with ECSO; regularly inform the competent national NIS authorities at a political level through the cooperation group established by the NIS Directive on issues of interest to the group.



Added-value

- Raising awareness of the EU-NIS community for the development of EU policies with a NIS dimension;
- Promote the integration of NIS aspects into key EU policies with a digital dimension;
- Contribute to ensuring coherence between future sectoral policy initiatives, including regulations with the framework and principles agreed on by the Member States and the European Parliament in the NIS Directive, and act as an “umbrella” of EU policy initiatives with a NIS dimension.

Objective 2.2. Supporting EU Policy Implementation

Priorities

- Support the cooperation group and assist the competent national NIS authorities in cooperating in the implementation of already agreed EU policies (legislations) with a NIS dimension;
- Focus on the NIS Directive, in particular regarding the requirements related to Operators of Essential Services (OES) (e.g. identification, security requirements, incident reporting) and on the eIDAS Regulation, taking into account the NIS aspects of GDPR (and more generally data protection) and the ePrivacy Regulation draft as it reflects the ENISA regulation;
- Support cybersecurity activities in the framework of the implementation of the European Electronic Communications Code;

Guidelines

- Establish structured dialogues, whenever possible on a multi-annual basis, with voluntary experts from competent national NIS authorities' to liaise with national stakeholders (e.g. OES);
- Aim to limit the number of dialogues to increase the participation of all Member States and in a spirit of efficiency, such as for the NIS of the OES, by promoting a cross-sectoral approach, gradually taking into account sectoral specificities;
- Regularly inform the competent national NIS authorities at a political level through the cooperation group and, in particular, carry out its stocktaking.

Added-value

- Support the Member States in the implementation of EU policies by providing high-quality recommendations based on the experience of the

EU NIS community and reduce duplication of the efforts across the EU;

- Support the activities of the cooperation group and of the MS in relation to the implementation of the NIS directive from a European perspective; promote a harmonised approach to the implementation of EU policies and in particular legislations.

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

Objective 3.1. Assist Member States' capacity building

- Advise and assist Member States in building national cybersecurity capacities based on national experiences and best practices;
- Focus on the NIS capacities foreseen in the NIS Directive, building on ongoing activities in the CSIRTs Network and national CSIRTs on which ENISA should continue to work on to promote the strengthening of the CSIRTs of the EU Member States';
- Develop national NIS capacity indicators, building on capacities foreseen in the NIS Directive and allowing an assessment of the state of the NIS capacity development within the EU;
- Identify and derive recommendations for other national NIS capacities that would contribute to strengthening EU NIS through dissemination throughout the EU NIS community, e.g. national cybersecurity assessments, PPPs for instance in the field of CIIP, national information sharing schemes, etc.;
- Providing support and guidance for the establishment of national and European Information Sharing and Analysis Centres (ISACs) in specific sectors.

Guidelines

- Carry out a regular stocktaking of national NIS capacity initiatives to identify trends and thus collect and analyse different approaches and practices;
- Work closely with experts from competent national NIS authorities to identify experiences and best practices for national NIS capacity building;
- Take into account developments and recommendations that may arise from the CSIRTs network and the cooperation group;

- Adopt a holistic approach to NIS capacities, ranging from technical to organisational to the political level;
- Give priority to identifying key trends at EU level and provide advice to individual Member States at their request when establishing generic NIS capacity metrics;
- Examine the development of tools and initiatives to make ENISA's recommendations more visible and effective (e.g. summer school, on-site trainings);
- Advise on how to improve private-private information exchanges (e.g. via ISACs) and on an ad hoc basis and, without prejudice to the achievement of its priorities under this objective, continue to support specific European ISACs.

Added-value

- Continue to support the development of national NIS capacities thus reinforcing the level of preparedness and response capacities of the Member States, which, in turn, contributes to the overall cybersecurity of NIS across the EU;
- Promote the exchange of best practices between the Member States;
- Structured cooperation with CERT-EU to provide technical assistance to Member States in the event of significant incidents and to support incident analysis; upon request, support the Member States in dealing with incidents and analysing vulnerabilities, artefacts and incidents;
- Facilitate cooperation between Member States in dealing with emergency response by aggregating national situation reports based on information provided to the Agency by the Member States;
- Indirectly contribute to capacity building of governments outside the EU by making the recommendation and training materials available on the Agency's 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) for cooperation within the CSIRT network and development.

Objective 3.2. Assist in the EU institutions' capacity building

Priorities

- Representation of the EU decentralised agencies on the CERT-EU Steering Board;

- Cooperation with relevant EU agencies on initiatives covering NIS dimension related to their mission;
- Support (upon request and in coordination with the institutions) capacity building for trainings, awareness raising, and development of education material.

Adopt a holistic approach to NIS capacities, ranging from technical to organisational to the political level

Guidelines

- Work with EU agencies to define NIS requirements;
- Capacity building through regular interactions (e.g. annual workshop) in cooperation with the ICT Advisory Committee of the EU agencies;
- Work with CERT-EU and other EU institutions and agencies (e.g. EC3, EDA, EEAS, EASA) and other bodies with strong NIS capabilities to support ENISA's activities under this objective;
- Strengthen links between the EU institutions and agencies and other bodies and cooperate in the dissemination activities related to cybersecurity capacity building and general cybersecurity awareness.

Added-value

- Support the development of the NIS capacities of European Union institutions and agencies, thus contributing to raising the overall level of cybersecurity of the NIS across the EU;
- Promote the exchange of best practices between EU agencies and a better definition of the NIS requirements to reduce duplication of the efforts and to encourage more systematic approaches to NIS;
- Complement CERT-EU's work on active cybersecurity for the EUIs and agencies through awareness-raising and other proactive measures, through advice on the "prevention dimension" of NIS.

Objective 3.3. Awareness raising

Priorities

- Work with the relevant national authorities to advise private sector on how to improve its own NIS through by developing key recommendations for the private sector cybersecurity ;
- Support the exchange of best practices on awareness and education between public and private sectors at European level;

Advise private sector on how to improve its own NIS through by developing key recommendations

- Organise the European Cybersecurity Month (ECSM) and the European Cybersecurity Challenge (ECSC) to make these events a place for EU cybersecurity awareness; pool, organise and make information on security of network and information systems, in particular on cybersecurity (provided by the EU institutions, agencies and bodies) publicly available through a dedicated portal ;
- Regularly carry out stocktaking of national awareness-raising initiatives;
- Build on 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 on existing work at national level on the private sector, on the basis of a regular stocktaking of national expertise on this issue (e.g. cyber hygiene) and on the work carried out under Activity 1 to provide high-quality, up-to-date and highly valuable recommendations for the benefit of the EU NIS community;
- Adapt its recommendations to specific target audiences (SMEs, large enterprises, NIS experts or non-experts) and adopt a holistic approach to NIS capacities, ranging from technical/operational to organisational to policy capacities;
- Establish a structured and sustainable (multi-annual) dialogue with volunteering experts from competent national NIS authorities on awareness-raising and communication responsible for the national dimension of the ECSM and ECSC; examine how appropriate communication channels can be used in the framework of the ECSM and ECSC;
- Adopt a holistic approach to awareness-raising and adapt its recommendations to specific target groups, from the citizens to public authorities.

Added-value

- Raising the private sector's awareness on the need to strengthen its NIS;
- Support the development of the NIS of businesses across the EU and support the competent national NIS authorities in their similar efforts for the private sector, thus helping to raise the level of overall cybersecurity of NIS across the EU;
- Enable the organisation of EU-wide events to increase visibility of cybersecurity and ENISA with the EU citizens, businesses, academia and the NIS community, including NIS students;
- Promote the harmonisation of tailor-made awareness-raising messages across the EU with increased impact, building on the strengths of existing national initiatives by sharing best practices;
- Strengthen cooperation between the Member States;

Facilitate the development of national awareness-raising initiatives at national level.

ACTIVITY 4 – COOPERATION. FOSTER THE OPERATIONAL COOPERATION WITHIN THE EUROPEAN CYBERSECURITY COMMUNITY

Objective 4.1. Cyber crisis cooperation

Priorities

- Further develop and organise Cyber Europe 2020, exploring new dimensions and formats to further prepare the Member States and EU institutions for cyber crises that may occur in the EU in the future;
- 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;
- Actively contribute to the implementation of the blueprint by supporting MS in integrating guidelines, mechanisms, procedures and tools at EU level into the national crisis management frameworks; the Agency will contribute to developing 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 raising wide situational awareness across the Union to testing cooperation plans for incidents;
- Integrate existing and future EU-wide crisis management orientations, mechanisms, procedures and tools into the existing crisis management framework of the MS;
- Closely follow the development of the CEF Cybersecurity DSI CSP and ensure a smooth handover to ENISA and support the voluntary adoption by the CSIRT community;
- Proactively develop its expertise in the field of cyber crisis management and exercises in cooperation with other EU 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 sustained dialogue with competent national NIS authorities;
- Support the development of tools and procedures (e.g. technical and operational SOPs) to support crisis management at EU level, to be tested in the exercises;
- Support its activities under Objective 4.2 regarding the CSIRTs network to ensure coherence in the

development of procedures and tools for the daily exchange of crisis management information;

- Explore the possibility of participating as an observer in other national or international exercises to benefit from lessons-learned, and 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 of the Management Board;
- Assess the impact of the organisation of previous exercises and build on these lessons-learned to support the development of future exercises and in particular to further develop the exercise platform.

Added-value

- Enable the organisation of EU-wide events to increase the visibility of cybersecurity and ENISA with other Union institutions, Member States, citizens, businesses and academia;
- Further strengthen cooperation between Member States and develop tools and procedures to support their response to cross-border crises, thereby raising the overall level of preparedness of the EU;
- Contribute to the development of the international dimension of its mandate;
- Support the development and testing of the plan for a 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 on its long experience in cyber crisis exercises and under objective 3.1 by building on its cyber crisis expertise by advising on the development of national cyber crisis capacities.

Objective 4.2. Community building and operational cooperation

Priorities

- Provide the secretariat and active support for the CSIRT Network foreseen in the NIS Directive;
- Ensure, among other things, a well-functioning and resilient CSIRT Network IT infrastructure and communication channels. Ensure structured cooperation with CERT-EU, EC3 and other relevant EU bodies;
- Use the development of the CSIRT core platform under the the “Connecting European Facility” (CEF) mechanism to support the functioning of the CSIRT Network and, upon request, advise Member

States' CSIRTs on projects to be proposed on future CEF calls for projects;

- Leverage the role of the Single Point of Contact (NISD), taking into account that it performs 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;
- Coordinate its activities with those carried out under objective 4.1 strengthening ENISA's expertise on cyber crisis management, to develop tools and procedures for the CSIRTs network, from daily information exchange on cyber crises.

Added-value

- Support an enhanced exchange of NIS information between CSIRTs and contribute to strengthening cooperation between Member States in the event of incidents or of a crises, thus contributing to improving the EU's overall preparedness and response capacity;

- Create the conditions for enhanced 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 to strengthen national CSIRT capacities.

ACTIVITY 5 – CERTIFICATION. DEVELOP CYBERSECURITY CERTIFICATION SCHEMES FOR DIGITAL PRODUCTS, SERVICES AND PROCESSES

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 European Commission in its role as Chair of the EU Cybersecurity Certification Group;



- Support the Stakeholder Cybersecurity Certification Group;

Guidelines

- Analysis of the main trends in the cybersecurity market; market observation;
- Content maintenance on a dedicated website;
- Development and maintenance of information on the EU cybersecurity certification framework through a dedicated portal; portal and related IT system maintenance;
- Organising stakeholder consultations and/or contributions to candidate schemes.

Added-value

- Support Member States in the implementation of EU policies by providing high quality recommendations based on the experience of the EU NIS community and reducing duplication of the efforts across the EU; providing up-to-date information on the certification schemes to the public;
- Support the deployment of the EU Cybersecurity Certification framework;
- Support cooperation between all stakeholders associated with the EU Cybersecurity Framework, including industry, governmental bodies, standardisation bodies, etc.

Objective 5.2. Developing candidate cybersecurity certification schemes

Priorities

- Support the work carried out under the EU Cybersecurity Certification Framework, including the provision of technical expertise to prepare candidate European cybersecurity certification schemes in functional application areas in accordance to the Union's rolling work programme for certification;
- Support the development and implementation of the Union's policy on standardisation, certification and market surveillance;
- Facilitate the adoption of risk-management standards for electronic products, networks and services and advise relevant stakeholders on cybersecurity certification framework technical security requirements;
- Focus on cybersecurity certification policies to ensure coherence with the framework and principles agreed on in the Cybersecurity Act.

Guidelines

- Promote dialogue within the framework of the work carried out under the Certification

Framework, with the European Cybersecurity Certification Group, the Stakeholders Cybersecurity Certification Group, ad hoc groups, competent national authorities etc., including the provision of technical expertise to prepare European cybersecurity certification schemes for candidates.

Added-value

- Support the development and implementation of the Union's standardisation (European and international, as appropriate) and certification policy;
- Contribute to the implementation of the Cybersecurity Act in accordance with the tasks assigned to the Agency and in collaboration with national certification authorities.

ACTIVITY 6 – ENABLING. REINFORCE ENISA'S IMPACT

Objective 6.1. Management and compliance

Priorities

- Optimise talent acquisition and retention to fulfill ENISA's mandate; establish an appropriate development management programme; ensure a safe and healthy working environment, supported by proportional and adequate social measures;
- Maximise the leaning and rationalisation of processes and tools in compliance with the EU regulatory framework and the use of best practices;
- Provide a learning environment for employees by offering a wide range of learning and development opportunities to achieve the organisation's objectives;
- 100% compliance with our financial and legal framework;
- Assess and implement the Agency's business requirements and internal strategy;
- Develop an appropriate internal control system for internal delivery optimisation, compliance, fraud prevention and management of potential conflict of interests;
- Maintain and improve the goal of preventing harassment and applying best practices for healthy work environments.

Guidelines

- Develop an HR strategy in line with the Agency's strategy, which focuses on talent management, engagement and retention and adapts postal capacity to the domain to to achieve ENISA's mandate objectives;
- Improve the effectiveness of recruitment and the internal process, in particular regarding speeding up and smoothing the recruitment process, thus contributing to improving ENISA's internal expertise;
- Strengthening a culture of openness, cooperation and exchange of knowledge between the Agency;
- Improve the collaboration with MS and other EU institutions in the secondment of national experts to ENISA;
- Seek other options to build up the adequate workforce, despite the current difficulties to attract professionals due to the overall market situation;
- Further improve financial processes monitoring and expect to maintain high commitment and payment rates to guarantee full implementation of WP and compliance;
- Adopt sophisticated finance management tools, aiming for adoption of AI in modern business processes;
- Enhance IT security for ENISA's systems, aiming for ENISA's internal systems to be state-of-the-art regarding cybersecurity;
- Improve the quality management system at ENISA.

Added-value

- Improve the overall quality and efficiency of ENISA's activities by strengthening the Agency's quality management system;
- Reduce risks in the Agency in several activities and management and optimisation of the use of financial and human resources;
- Create significant added value in all resource areas as a key pillar for meeting the expectations of internal and external stakeholders.

Objective 6.2. Engagement with stakeholders and international relations

Priorities

- Involve the experts of the competent national NIS authorities of the Member States in the preparation of the results;
- Proactively engage with other competent Union institutions (e.g. the European Commission), other

agencies or CERT-EU to identify possible synergies, avoid redundancy and offer advice based on ENISA's NIS expertise;

- Seek to increase and evaluate the added value and impact of its activities with the European NIS community;
- Communicate transparently with stakeholders, in particular with Member States, on activities to be carried out and inform them of their implementation;
- Contribute, when relevant and on an *ad hoc* basis, to the Union's efforts to cooperate with third countries and international organisations to promote international cooperation on NIS.

Guidelines

- When provided by the WP and whenever relevant on a multi-annual basis, establish structured dialogues with volunteering experts from national Member States to deliver its outputs (e.g. working groups such as on cyber crisis cooperation);
- Rely on the national Member States, which are primarily responsible for national public private cooperations, to engage with private sector;
- Further develop tools and procedures to facilitate and ensure transparency of the involvement of all stakeholders, in particular regarding the principles and modalities of the participation and consultation of national NIS competent authorities;
- Strengthen the network of liaison officers as the main exchange point for ENISA and Member States to achieve these priorities;
- Regularly carry out in-depth evaluations to assess mid- to long term impact of its action in certain areas of expertise.

Added-value

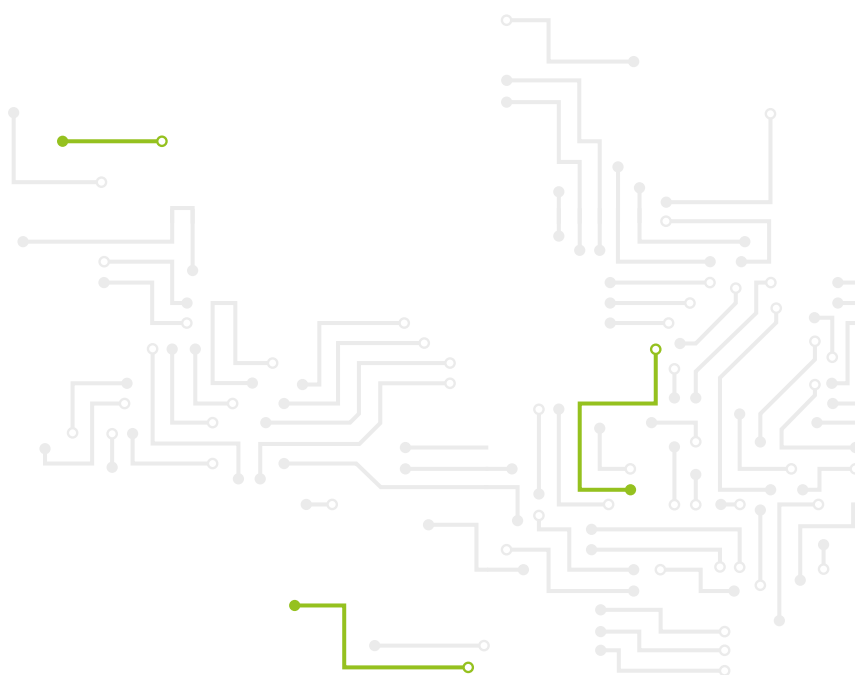
- Building trust and mutual expertise with Member State experts and other stakeholders and contributing to strengthening their compliance and involvement with ENISA's work;
- Building trust and cooperation with other EU institutions and contributing to strengthening their own NIS;
- Improving ENISA's understanding of 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, high-quality and up-to-date analyses and recommendations with high European added value.

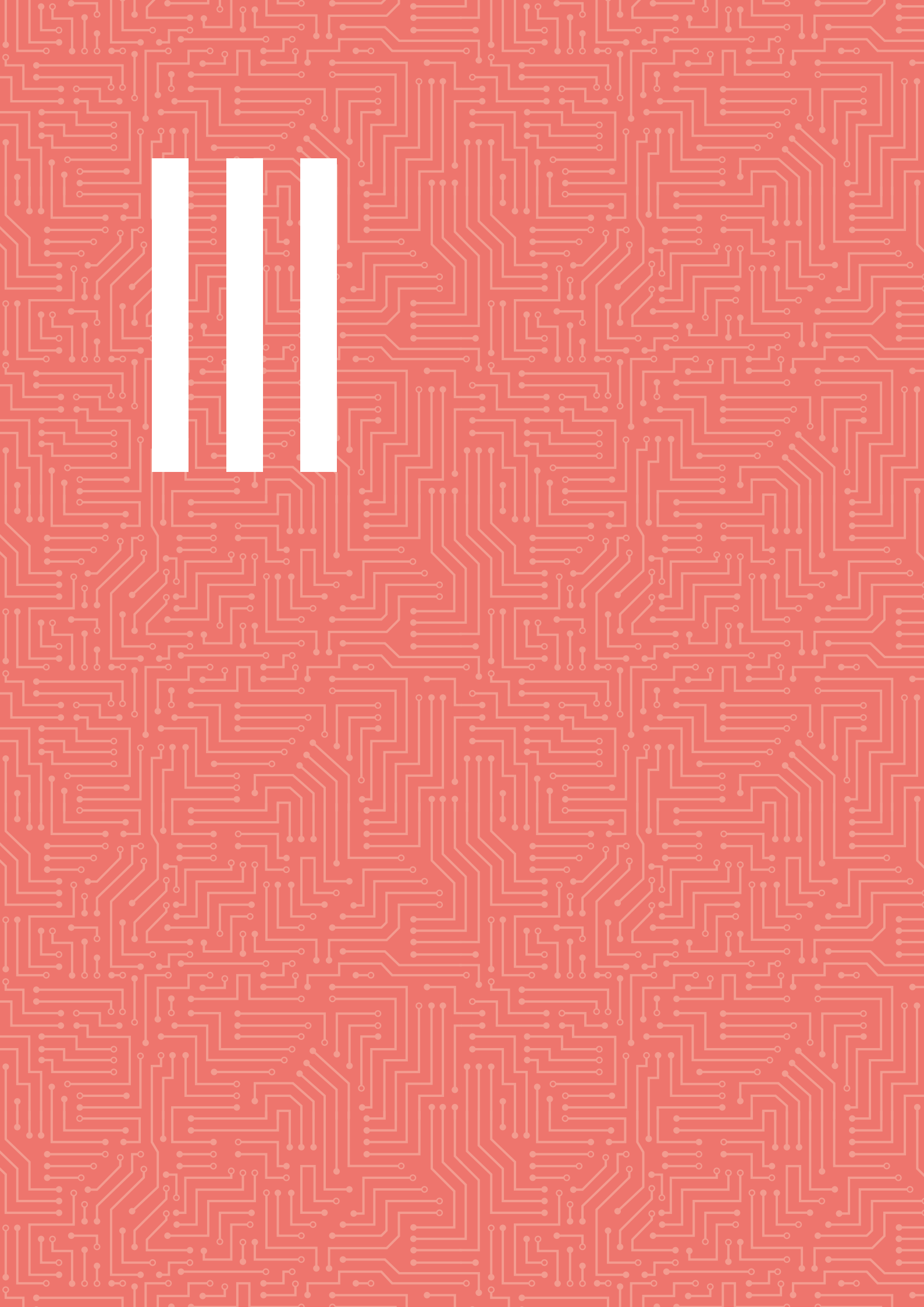
MONITORING THE PROGRESS AND ACHIEVEMENTS OF THE AGENCY. SUMMARIZING KEY INDICATORS FOR THE MULTI-ANNUAL ACTIVITIES

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

HUMAN AND FINANCIAL RESOURCE OUTLOOK FOR 2020-2022

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





PART III

WORK PROGRAMME FOR 2020

The ENISA Work Programme for 2020 follows the layout 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, added value of the activity, the main challenges for 2020 and a link to the multi-annual objectives.

The main outputs/actions for 2020 are listed for each objective. For each objective numerous outputs have been defined. For each output is structured as follows:

- A description of the specific actions and outcome which are expected to contribute to the achievement of the objective,
 - The type of output (in a summarises 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 for or collaboration with e.g. EU institutions, bodies or Member States, with reference to a specific activity that features defined and shared objectives.
 - Key performance indicators tailored to the type of output (in a summarising table at the end of each activity).
- Resources and budget, in a summarising table at the end of the section in aggregated form at activity level.

In the preparation of the Work Programme 2020, ENISA relied on the tasks and activities from the Cybersecurity Act (EU 2019/881), however using resources proposed in the impact assessment published as part of 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, creating, among other things, baseline IoT security recommendations⁶ (WP2017), sectoral work in Industry 4.0/smart manufacturing⁷ (WP2018), secure development

⁶ See <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>

⁷ See <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot>

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. Moreover, the Agency is in line with the priorities of the EC for the next 5 years⁸.

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 to these practices and standards to develop guidelines for improving the IoT security, focusing on its impact on the consumers and 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 meet these goals, the Agency will take existing EU policy and regulatory initiatives (the NIS Directive, the Internet of Things - An action plan for Europe⁹, the Communication on Building strong cybersecurity for the EU¹⁰, the Public Private Partnership (PPP) on cybersecurity¹¹, etc.) into account and contribute to them. ENISA will work with relevant stakeholders (public and private sector, national cybersecurity agencies, and 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, and provide relevant recommendations and good practices. Accordingly, it will consider defining e.g. secure IoT procurement guidelines to support consumers, IoT supply chain security guidelines or other means to raise 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 Connected and Automated Mobility (CAM)

The automotive industry is undergoing a paradigm change towards connected and autonomous vehicles. Smart cars that are already available today provide connected features for added value to enhance the car users' experience or improve their safety. With an increased connectivity (that the emergence of 5G is expected to promote further) novel cybersecurity risks and threats arise and need to be addressed. In light of the NIS Directive, in which 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 need for addressing the security of smart cars.

The Agency will continue its work on smart cars¹² (WP2016, WP2019) and monitor security practices and standards in the area of smart cars (e.g. UN-ECE dedicated TF on CYBER, ISO/SAE standardisation work), taking the emerging notions of connectivity and autonomy into consideration. 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. The Agency will review these practices and standards and highlight or suggest good practices and potential legislative actions required to guarantee security of smart cars, focusing on general safety as well as connectivity and autonomy.

To assist the European commission and the Member States in achieving these objectives, the Agency will evaluate and contribute to existing EU policy and regulatory initiatives (the NIS Directive, the European strategy on Cooperative Intelligent Transport Systems¹³, the C-ITS Platform of DG MOVE¹⁴, the High Level Group GEAR 2030¹⁵) as well as the planned European Commission Recommendation on Connected and Automated Mobility (CAM), the 3rd Mobility package¹⁶, the Communication on CAM and the relevant work of Euro NCAP. ENISA is in line with the cybersecurity effort of the joint initiative by DG MOVE, DG CNCT, RTD and DG GROW established under the 3rd Mobility package.

8 https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

9 See <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2009:0278:FIN>

10 See <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN>

11 See <https://ec.europa.eu/digital-single-market/en/news/commission-decision-establish-contractual-public-private-partnership-cybersecurity-cppp>

12 See <https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars>

13 See <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0766>

14 See https://ec.europa.eu/transport/themes/its/c-its_en

15 See https://ec.europa.eu/growth/content/high-level-group-gear-2030-report-on-automotive-competitiveness-and-sustainability_en

16 See https://ec.europa.eu/transport/modes/road/news/2018-05-17-europe-on-the-move-3_en

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

ENISA will take stock of existing initiatives and studies that are ongoing in the area of AI cybersecurity

Additionally, the Agency will validate the results of the study (e.g. via joint workshops) in collaboration with relevant stakeholders in the field of smart cars from the public sector such as the relevant European Commission service, JRC, competent authorities, national cybersecurity agencies, national road authorities, from the private sector including automotive manufacturers, OEMs, and 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 showcases of AI include smart manufacturing (robotics), autonomous driving, smart cities, etc. Even though undoubtedly beneficial, AI and its application on automated decision making – especially in safety critical deployments such as in autonomous vehicles – can offer new ways for manipulation and other attacks.

When considering security regarding AI, considerate needs to be considered that AI can be exploited to manipulate 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 pose a relevant risk that needs to be taken into account. The manipulation of data input in AI algorithms is also an area of concern for

cybersecurity, since intentional or unintentional modifications of can significantly affect the behaviour of the algorithms. Moreover, the evolutionary nature of AI algorithms and the need to perform verifications and even forensics in this complex field exacerbate cybersecurity concerns, especially in connection with their application in critical information infrastructures. Conversely, AI is becoming an important tool for cybersecurity itself, as it can be used to identify attack patterns and thus facilitates supervision of security management/policy implementation and allows for automated incident management etc.

The Agency will conduct a study on the challenges related to AI security taking relevant issues, risks and solutions into consideration. In doing so, ENISA will map relevant stakeholders and experts, engage with the wider community and validate the results of the study (e.g. via joint workshops) with relevant national and EU initiatives and competent authorities. Moreover, the Agency will interact with AI stakeholders from the public sector such as the relevant European Commission services, etc. ENISA will take stock of existing initiatives and studies that are ongoing in the area of AI cybersecurity such as the results of EU projects in this area (H2020) to avoid duplication of the efforts, but instead focus on providing a harmonized view of the ongoing works. ENISA will also support the EC in upcoming and ongoing policy initiatives related to the topic such as the coordinated European approach on artificial intelligence¹⁷.

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 highlighted that the healthcare sector has a relatively low level of maturity regarding cybersecurity. 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 Regulation¹⁸ (MDR) includes obligatory safety and security provisions for medical devices and the EC Communication on enabling digital transformation of healthcare in the digital single market¹⁹ as described in the 2018 communication of the European Commission on data

¹⁷ See https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

¹⁸ https://ec.europa.eu/growth/sectors/medical-devices/regulatory-framework_en

¹⁹ <https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering>

package²⁰. The Agency supports the actions taken by the EC to increase health information data sharing with a strong focus on cybersecurity.

Based on previous experience, the Agency will support healthcare organisations in enhancing their cybersecurity level by helping them assess risks in their healthcare information systems. This will enable healthcare organisations to identify vulnerabilities and evaluate risks for all assets in the healthcare ecosystem. The Agency will consider the evaluation of implementation scenarios such as ePrescription systems, remote patient healthcare, proactive/predictive approaches to healthcare, mHealth, cloud and big data for healthcare services. The goal is to provide a collection of best practices to ensure 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, competent NIS 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 fields of healthcare security (WP 2015, WP 2019), smart hospitals (WP 2016) and the NIS Directive implementation (WP 2017, WP 2019).

Output O.1.1.5 – Building knowledge on maritime security

The maritime sector plays a key role for the EU economy and society, accounting for a large segment of Europe's overall freight and passenger transport. However, with the introduction of innovative solutions based on ICT, the sector has been undergoing a digital transformation, which is why the cyber risk profile has changed. Combined with a significant increase in cyber attacks against key maritime entities such as ports and shipping companies, this change highlights the need for cybersecurity to be addressed in more detail in the maritime sector. As per the revised EU maritime security strategy action plan, cybersecurity is important for the sector²¹.

Accordingly, the Agency will provide maritime stakeholders (e.g. regulatory authorities, port authorities, service providers, shipping companies, vessel manufacturers, solution developers, etc.) with guidelines for best practices regarding security and

resilience when designing, developing and deploying services to minimise the systems' and services' exposure to all relevant cyber threat categories. The best practices will take both the current maritime ICT environment and the emerging trends in terms of business models and supporting ICT systems into consideration. ENISA will take stock of current practices and standards and develop best practices with a focus on resilience of critical services and user safety, while analysing specific use cases to determine possible attack scenarios.

A callout box with a red border and a white background, containing text in red and black. It is connected to the main text by a thin grey line.

ENISA will interact with relevant key stakeholders from the public sector such as DG MOVE, EMSA, competent national authorities, and from the private sector

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

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

Output O.1.1.6 – Building knowledge on cryptographic algorithms

In the revised cybersecurity strategy of the EU published in September²², the European Commission highlights “[...] the lack of European capacity on assessing the encryption of products and services used by citizens, businesses and governments within

²⁰ http://europa.eu/rapid/press-release_IP-18-3364_en.htm

²¹ https://ec.europa.eu/maritimeaffairs/policy/maritime-security_en

²² European Commission, Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU, JOIN(2017) 450, available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:450:FIN>

the 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”. Encryption is one of the most important technologies that fulfills the criteria of a security and privacy enhancing technology.

While acknowledging the importance of crypto technologies with regard to cybersecurity, particularly encryption is still a main focus regarding 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 collaborate on sharing existing approaches, best practices and knowledge. Due to international standardisation, technical specifications for cryptographic algorithms already exist; this should be the goal at European level, too. Moreover, at European level, the so called SOGIS-MRA Crypto catalogue²³, a comprehensive collection of cryptographic means agreed on by participating competent authorities of the Member States, is a first major achievement.

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

With regard to standardisation, ENISA should facilitate the establishment and adoption of European and international standards for risk management and for the security of ICT processes, products and services which 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 promote the findings of these groups by referring to them on its website. A similar arrangement could be utilized for relevant CEN/CENELEC standards groups (primarily JTC-13 as it begins its work).

Objective 1.2. Cybersecurity Threat Landscape and Analysis

Output O.1.2.1 – Annual ENISA Threat Landscape report

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 includes threat agents and typical attack vectors. Hence, the ETL is 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, and directly to ENISA under other EU legislation.

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

The dissemination, concise presentation and online availability of situational cyberthreat intelligence will be a major focus in 2020. The available situational cyberthreat intelligence will be linked to other relevant ENISA results (see also chapter Objective 1.2. NIS threat landscape description and analysis).

As a result, ETL stakeholders will be able to access and interact with ENISA cyberthreat information permanently. In 2020, ENISA will continue its cooperation with the CERT-EU on threat landscaping. This includes a collaboration with the relevant working group in the CSIRTs Network for information exchanges, use of CERT-EU services and organisation of common meetings/events. This work also helps maintaining and expanding synergies with related experts (i.e. ENISA ETL Stakeholder Group) and vendors (through MoUs).

23 https://www.sogis.org/uk/supporting_doc_en.html

CTI EU Event

In 2020, ENISA will continue supporting the relevant Cyberthreat Intelligence stakeholder community by supporting best practices for CTI and by providing an interaction platform. This is the main mobilization instrument for CTI stakeholders; it will facilitate the dissemination of CTI information of all kinds by ENISA (e.g. info note).

Maturing of the European cyber threat intelligence practice through expert/stakeholder participation

Based on its previous work analysing current and emerging threats, ENISA will promote best practices in the field of cyber threat intelligence (CTI) by means of defining a capability framework and a maturity model, in collaboration with the stakeholder community.

ENISA will prepare a CTI capability framework by providing hands-on guidelines on how organisations can revise their cyber resilience strategies by introducing technical and non-technical context to their defence capabilities. The proposed framework consists of a practical tool that helps organisations of any size and sector to establish a well-defined CTI program. It will show concrete requirements, a clear process, outputs and metrics to evaluate the impact. The aim of this tool is to promote a shift from a reactive to a proactive way of thinking regarding cybersecurity by cybersecurity becoming an integral part of the organisation'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 current state of the CTI program within an organisation. The purpose of this tool is to help organisations to evaluate the maturity of the CTI Program themselves and, ultimately, being able to define a roadmap for continuous improvement.

ENISA will promote knowledge and experience sharing activities between the members of the cyber threat intelligence community. As a key initiative, ENISA will organise an annual meeting/event (CTI-EU) that mobilises experts, academics and the industry to debate and plan the future of CTI.

Reporting on emerging cybersecurity threats

ENISA will identify best practices regarding future technological developments to support the research of emerging cybersecurity challenges and threats relevant to all organisations. From the outcome of this research, ENISA will present a methodology and

practical guidelines to streamline a process to create informed representations of possible future trends and scenarios. ENISA expects that the methodology will help organisations to promote internal awareness on emerging cybersecurity challenges and threats and define proactive mitigation strategies.

Using the methodology above, ENISA will analyse and report emerging cybersecurity challenges and threats via an annual research program. The consideration of future technological trends and challenges is part of the planning and knowledge management process of ENISA. The outcome of this research aims at facilitating the decisionmaking process in setting priorities for future ENISA work programs and defining thematic areas aligned with social and economic needs of citizens and organisations. The ENISA report on future cybersecurity challenges and threats is essentially a source of information about emerging technological trends that may potentially lead to security challenges and constraints. The report presents possible mitigation strategies and emerging security solutions that attempt to anticipate threats and minimize their impact. To produce this report, ENISA will conduct a research process over a whole year. It will include the input from a variety of sources and contributions from members of expert and stakeholder groups (e.g. researchers, academia, representatives from the civil society and industry). ENISA expects the report to promote an extensive discussion and raise awareness on the topics within the cybersecurity community and the society as a whole.

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

ENISA provides guidance on important NIS events and developments through information notes. Since 2018, the Agency has been producing two different types of 'CSIRT Info Notes' and 'General Info Notes'. This will be continued in 2020.

CSIRT Info Notes

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

General Info Notes

General Info Notes cover significant developments and announcements in the field of cybersecurity with the sole purpose of promoting general awareness and presenting actionable mitigation strategies. *General Info Notes* are not meant as a response to

incidents or vulnerabilities but rather as explanatory reviews, neutral and independent analyses of major events that have reached a certain level of public and media attention. For creating *General Info Notes*, ENISA will consult the CSIRTs Network but also other appropriate resources.

ENISA provides objective information regarding such events covering issues, points of action, mitigation measures, summaries, related practices, etc. Hence, the aim of these notes is to provide a neutral overview of the current state and raise awareness of the essence of the threat by an objective analysis shortly after the event.

Both types of information notes will be integrated into the cyber-threat information, thus functioning as a single knowledge hub.

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

Just as with the ETL, ENISA will continue to improve the dissemination efficiency of the produced CTI information notes. For this purpose, available dissemination channels will be used to enhance adoption among key stakeholders. In addition to the ENISA website, in 2020 information 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 types of legislative instruments, developing efficient reporting schemes across sectors and geographical borders is one of the objectives for ENISA in this sector. Such reporting schemes should be simple, pragmatic and relevant for the public and private sector respectively without increasing the cost of operation.

Current and future activities in this area include:

- Incident notifications in the telecom sector (Article 13a of the Telecoms framework directive to be replaced by Article 40 of the EECC); ENISA currently supports the activities of the Article 13a Expert Group dealing with general surveillance of security in the telecom sector and producing annual summary reports on telecom incidents. In this context, ENISA works closely with several industry groups and supports the Article 13a expert group in the analysis of cross-cutting security issues. The new EU Electronic Communications Code (EECC) to be adopted will require substantial work and support as the scope of monitoring and reporting and security breaches will expand.



- Incident notification for the trust services sector (Article 19 of the eIDAS Regulation): Electronic trust services are a growing sector and are becoming increasingly important with many cross-border dependencies. ENISA plays a key role in the collection and analysis of security incidents from across the EU. In 2020, ENISA will analyse security incidents and produce a consolidated, anonymised annual report. In addition, ENISA, in collaboration with the Member States, will gather experience from previous incidents and recommend best practices. In this context, ENISA also engages with the private sector and with relevant fora such as the FESA and the eID expert group.
- Incident notifications under the NIS Directive: In 2018, ENISA provided templates. ENISA will work with the European Commission and the Member States to exploit synergies in the different notification schemes. ENISA will also engage with the European Commission and competent national authorities to develop sectoral approaches to incident notification that best suit each sector. In this context, ENISA supports the efficient flow of information on mandatory and voluntary incident notifications to establish a common picture across sectors and the EU.

ENISA has extensive expertise in producing summary **incident reports** at EU level through the work with Member States and telecom 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 PSIRTs and NIS sectoral incident response expertise

For this particular output, ENISA, supporting the MS, will collect and analyse best practices for sectoral CSIRTs and product CSIRTs (PSIRTs) to support incident response (IR) expertise implementation according to the Annex I and Annex II requirements of the NIS Directive.

In addition to the above, the Agency will organise a validation workshop with the EU, Member States and sectoral stakeholders to present the results and gather feedback on current experiences with approaching incidents, threats and vulnerabilities including multiple stakeholders.

ENISA will also support the dissemination of PSIRT and sectoral IR best practices. This will enable stakeholders to better adopt NIS CSIRT requirements in their businesses and reinforce cooperation with product CSIRTs (PSIRT). All this will enable more efficient incident management practices and will thus

contribute to a more agile adaptation of established CSIRT expertise and collaboration practices on incidents, threats and vulnerabilities in the EU.

Objective 1.3. Research & Development, Innovation

Output O.1.3.1 – Supporting EU research & development programmes

ENISA will continue providing analyses 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 at showing where funded R&D activities in the context of H2020, TRANSITS and GEANT would achieve the greatest impact. ENISA will work in close cooperation with the respective European Commission services on cybersecurity aspects related to the General Data Protection Regulation. The Agency will also monitor and analyse cybersecurity related directives and initiatives in various sectors (e.g. space, maritime, defence, transport, automotive) and evaluate the specific threat landscape in these critical sectors.

ENISA will adapt the current best practices and guidelines for protecting EU systems and networks, services, IoT and cloud ecosystems as well as supply chains according to the evolving threats in addition to building specific use cases that can be adopted by the IT Security community.

Additionally, ENISA will continue supporting and advising the European Commission, organisations in this area, other agencies (e.g. EDA, ESA), industrial communities and the Member States to meet their goals by providing its concrete NIS policy expertise. The Agency will also make contributions regarding the proposal on the creation of the Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre²⁴. In this context, ENISA will work closely with the European Cybersecurity Research and Competence Centre for the network to be set up.

²⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1582271895127&uri=CELEX:52018PC0630>

Summary of the outputs and performance indicators in Activity 1 – Expertise		
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: Conference on IoT cybersecurity with relevant stakeholders, 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)
Output O.1.1.2 – Building knowledge on Connected Automated Mobility (CAM)	P: Recommendations for the security of CAM, Q4 S: Support the European Commission, MS and automotive industry to holistically address cybersecurity 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,
Output O.1.1.3 – Building knowledge on Artificial Intelligence security	P: Artificial Intelligence: Cybersecurity challenges, Q4 E: AI security workshop, Q3-Q4 S: Support the European Commission and MS in relevant EU initiatives, Q1-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: Best practices for cybersecurity 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. the publication (P) and/or workshop (E) and/or support (S)
Output O.1.1.5 – Building knowledge on maritime security	P: Guidelines for cybersecurity in the maritime sector, Q4 S: Support the Commission, MS and maritime industry to holistically address cybersecurity of the maritime sector, Q1-Q4	Engage 10 stakeholders from the maritime sector from 5 EU MS in the preparation of the study (P)
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	Publish 2 news items or dissemination materials covering public documents and activities of the groups/meetings attended.
Objective 1.2. Cybersecurity Threat Landscape and Analysis		
Output O.1.2.1 – Annual ENISA Threat Landscape report	P: Report and offer online information; 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 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 cybersecurity	P: Information notes on NIS, Q1-Q4	Coverage of all major incidents relevant to EU NIS policy priorities. Expand coverage to all of ENISA's key 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. 13a25 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. 1926 meetings S: Support MS and the EC in implementing NISD incident reporting requirements. P: Best practices for further development of the NISD incident notification frameworks across EU, Q4	More than 20 NRAs/EU MS to contribute in preparation of the report (Art. 13a) (P) More than 10 SBs/EU MS to contribute in preparation of the report (Art. 19) (P) Engage more than 10 MS in discussions related to implementing particularities of the NISD incident reporting framework (S).

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

26 Article 19 of the eIDAS regulation (2014).

Summary of the outputs and performance indicators in Activity 1 – Expertise		
Outputs	Type of output (P = publication, E = Event, S = Support)	Performance indicator
Output O.1.2.4 – Supporting PSIRTs and NIS sectoral incident response expertise	P: Best practices on sectoral CSIRT and PSIRT expertise and practices, 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 European Cybersecurity Research and Competence Centre. 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's work 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.

Taking into account 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 States and EU agencies to promote coordinated efforts for sectoral cybersecurity in the EU. Any planned activity in the field 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 the ongoing legislative process into consideration.

The Agency will provide support to the European Commission and the Member States regarding policies related to sectors of the NIS Directive by stocktaking of the different initiatives from the different sectors. In doing so, the Agency will map policies affecting the NISD sectors and the role and responsibilities of the involved actors. The results of this mapping will be validated by all related stakeholders. Moreover, upon request, the Agency will 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 to provide dependable trust and electronic identification services. Aspects to be covered will be discussed with the European Commission and Member States through the eIDAS experts group. Interaction with actors from the private sector will enhance the Agency's ability to make further meaningful contributions to this area. By implementing the Cybersecurity Act, ENISA will offer analytical support, thus supporting the efforts of the Member States and the European Commission in the field of electronic identity. To produce specific implementation guidelines and technical recommendations, a number of stakeholders and collaboration areas will be consulted to address operational aspects of trust service providers, conformity assessment bodies and supervisory authorities while leveraging past experiences to emphasise implementation and interoperability.

ENISA will also collaborate closely with the eIDAS Expert Group (Trust Services) and the Cooperation Network (established by the European Commission Implementing Decision 2015/296) to exchange information and share best practices. These recommendations will complement the existing knowledge base that ENISA already created for the trust service providers.

ENISA will take the recommendations and standards developed by CEN/CENELEC, ETSI, ISO and IEC into account and seek to avoid duplication

ENISA will take the recommendations and standards developed by CEN/CENELEC, ETSI and the ISO and IEC into account and seek to avoid duplication and conflict of the approaches. In this regard, ENISA will support the European Commission to assess applicable standards by reviewing them to decide to what extent they meet the requirements of the eIDAS Regulation. Furthermore, ENISA will continue to support the European Commission, as appropriate, with the implementation of specific areas of interest such as qualified time stamps, qualified website authentication certificates, mobile applications etc. Lastly, ENISA will support the European Commission with the implementation aspects and tasks related to Article 49 of the eIDAS as well as the review of the eIDAS Regulation to an extent that needs to be identified by the Commission.

Output O.2.2.2 – Supporting the implementation of the work programme of the Cooperation Group under the NIS Directive

ENISA has been supporting the European Commission and the MS with the development of the NIS Cooperation Group's 2018-2020 work programme. It will contribute to the discussions and assist the European Commission and MS in the development of the Cooperation Group's work programme 2020-2021. In this context, supporting the NIS Cooperation Group, ENISA will also analyse specific issues and draft working papers, consult with

competent authorities of the Member States' and collect and develop best practice recommendations.

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 discussed for the Cooperation Group's work programme.

ENISA will also take stock of experience gained in the first two years of the implementation of the NISD and will recommend best practices for the implementation of the Directive to the Cooperation Group and the European Commission.

Taking into account the evolving threat landscape and the experience gained from the implementation of the NISD, ENISA will continue supporting the European Commission and the Member States with the overview of the NISD implementation and its evaluation by the Member States and the European Commission. In this respect, ENISA will support the European Commission and the MS by leveraging the input from the Cooperation Group and the CSIRTs Network (in its capacity as the Secretariat for the CSIRTs Network, ENISA will facilitate the preparation of the next evaluation report for the Cooperation Group – Output 4.2.1) evaluating the implementation of the NISD and contribute to the discussions on the development of potentially forthcoming regulatory and/or policy initiatives.

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

Within the scope of its cybersecurity mandate, ENISA will support and promote trust and security in digital services regarding privacy and data protection. In close cooperation with institutional (European Commission, EDPS) stakeholders and the MS, including the European Data Protection Board (EDPB), ENISA will work within its mandate to support the technical analysis of cybersecurity measures, e.g. technical and organisational measures and mechanisms relevant to data protection by design and by default (such as for example pseudonymisation and anonymisation techniques),

security of processing, security and integrity of networks and electronic communication services, etc. ENISA will further extend its cooperation with the Data Protection Authorities of the Member States and with the EDPB and support their cybersecurity requirements in the field of personal data protection and privacy. Most importantly, ENISA will continue contributing in a technical capacity to the work of the EDPB, as it already did by supporting the European Commission since 2019.

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

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 a gap analysis available 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) and with international standardisation organisations (ISO and IEC) 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 primarily associated 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, GDPR, as well as the preparation for the upcoming ePrivacy Regulation, etc. This output will analyse gaps and, in particular, provide guidelines for the development or amendment of standards, facilitating the promulgation and adoption of NIS standards. ENISA provides its technical and organisational NIS know-how, which can be further leveraged to extend or assess standards to render them more appropriate to stakeholders. By bringing its concrete NIS policy expertise to the table, ENISA will produce “how to” and “what else” guides in to contribute to the European standardisation.

ENISA will thus, where appropriate, discuss that matter with the Member States, industry and standard developing organisations (e.g. ETSI, CEN, CENELEC), as

well as European Commission services and agencies with policy competence.

Output O.2.2.5 – Supporting the implementation of the 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 was adopted in 2018 and is expected to bring more harmonisation at EU level and several improvements regarding the security such as:

- broadens the scope of application to include 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 of the Member States with the transition, the new supervision tasks, and liaise with relevant industry players to support an effective, efficient and streamlined implementation of the security requirements (Article 40) of the EECC. ENISA will build on the Article 13a Expert Group and its contacts to the private sector to define guidelines and best practices.

As the competent authorities for the EECC of many Member States are 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.

Output O.2.2.6 – Support the MS in improving the cybersecurity of 5G networks

Given the actions regarding 5G in 2019, a number of upcoming activities for 2020 are envisaged. For these activities, ENISA will deliver technical content in support of EU-wide 5G actions. Thus, ENISA’s contribution is the provision of technical evidence needed for policymaking. ENISA is ready for follow-up activities under its remit, following the discussions between the EU Members States and with the European Commission regarding the toolbox initiative.

Summary of the outputs and performance indicators in Activity 2 – Policy		
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 sectoral initiatives related to NIS Directive, Q4 S: Supporting European Commission, EU Agencies, MS with policy developments related to NISD sectors, Q1-Q4 E: Two workshops with stakeholders from sectors, Q2-Q4 S: Supporting European Commission, EU Agencies, MS and/or private sector with the sectoral 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. P: The future of digital identity and prospects of digital identity ecosystem, Q4. E: Trust Services Forum, Q2	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 to 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 S: Support the work of the 2018-2020 Cooperation Group Work Programme as well as its Work Streams, Q1-Q4	Engaging at least 12 MS in ENISA's contributions to the implementation of the NIS Directive (S) 10 MS to participate in the 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 European Commission, and other authorities such as the EDPS, and MS including the EDPB), Q4 E: Validation Workshop, Q4 E: APF 2020, Q2/Q3	At least 5 representatives from different bodies/MS to 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 reviewing the guidelines of at least 5 representatives of European Standard Developing Organizations (SDOs) and relevant services of the European Commission and/or agencies More than 60 participants from relevant communities
Output O.2.2.5 – Supporting the implementation of the European Electronic Communications Code (EECC)	E: Workshop with public and private sector stakeholders S: Support the European Commission, the competent authorities in the implementation of European Electronic Communications Code, Q1-Q4	At least 10 MS and 5 providers to participate in the activities/workshop (P,E) related to the new EECC
Output O.2.2.6 – Support the MS in improving the cybersecurity of 5G networks	S: Support the Cooperation Group in assessing the implementation of the 5G toolbox, including the recommendations review foreseen for October 2020, Q1-Q4 S: Support BEREC Telecom regulators and private sector in the implementation of the 5G toolbox, Q1-Q4 P: Technical guidelines for the toolbox . Q1-Q4 P: Threat Landscape / Risk Assessment Report follow-up, Q1-Q4 P: Update of the 2014 Technical Guidelines on Security Measures for the Telecom Sector, Q4	Engage stakeholders from at least 10 MS in the activity (P)

ACTIVITY 3 – CAPACITY. SUPPORT EUROPE MAINTAINING STATE-OF-THE-ART INFORMATION SECURITY NETWORK AND 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 field aim at maintaining and extending the collection of best 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 national incident response preparedness of the Member States by providing best practice guidance on key elements of NIS capacity building with a focus on CSIRT/PSIRT/OES trainings and services to improve the skills of the operational teams and their personnel. ENISA will further build on the successful work in the field of 'training methodologies'.

In detail, the Agency will continue to provide updated training materials according to the findings of the stocktaking study for trainings in NISD sectors. As a result ENISA will be able to provide a new set of a training materials based on emerging technologies to reinforce the MS' operational skills and CSIRT/PSIRT capacities to efficiently manage cybersecurity events. A special emphasis is placed on supporting the MS and EU bodies with concrete guidance (like best practice materials) and concrete actions (like trainings). ENISA will also offer, upon request, direct support to individual 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.

The Agency will provide continuous support and development of TRANSITS trainings, which is a positive and important aspect for the capacity building of the MS. This activity is based on the recently developed materials and infrastructures for on site 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's priority for the MS is to adopt a national NIS strategy and to monitor its implementation. Since 2017, all 28 MS have published a national NIS strategy. However, in order to align the objectives of the existing National Cyber Security Strategies (NCSS) with the requirements of the NISD, many MS need to update their current NCSS.

ENISA will continue assisting EU MS to develop their capabilities in the area of NCSS. The Agency can build on its work from previous years and will assist the MS to deploy existing best practices in the relevant fields and offer targeted assistance on specific NCSS objectives (e.g. CIIP, creation of PPPs etc.). A priority will be to support the MS to create a NCSS that is in line with 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 the MS and examine best practices and new potential incentives such as the sectoral NCSS.

ENISA will continue supporting the MS in evaluating their NCSS and their NIS initiatives. The Agency will update its NCSS assessment methodology and validate it with the help of public and private stakeholders. Then, ENISA will make this assessment methodology available to the MS to use whenever needed for implementation.

Finally, ENISA will enhance the NCSS map with additional valuable information related to the NISD to create an information hub. As for the past 6 years, ENISA will organise the annual NCSS workshop focusing on the validation of the study's findings.

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

In 2020, ENISA will focus its efforts on supporting the MS to enhance their incident response capabilities by assisting them with their CSIRT maturity assessments and enhancements, for example with CSIRTs Network members' peer review maturity evaluation. In addition, the Agency will continue to monitor the 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 national incident response capabilities of the Member States by providing recommendations and advisory on key requirements of NIS capability building with a focus

on the development and efficiency of national and sectoral CSIRTs. ENISA will also offer, upon request, direct support to individual Member States to evaluate and improve their incident response capabilities.

The main objectives of this output in 2020 is to help MS and other ENISA incident response stakeholders, such as EU institutions, bodies and agencies, to develop, implement and enhance their incident response capabilities and services to meet the increasing challenges of securing their networks. Another objective of this output is to further develop and apply ENISA's recommendations for CSIRT baseline capabilities, maturity assessments and corresponding tools. As a continuous effort, ENISA will continue supporting cross-border CSIRT community projects, tool development and the global dialog about common issues and challenges regarding the topic of incident response.

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.²⁷ 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 regarding EU focused ISACs. It is for the obvious choice for ENISA to continue its activities from the last 10 years to coordinate, in conjunction with CEF funding, the further development and implementation of EU ISACs in the next decade. ENISA is already cooperating with the European Commission to develop the ISAC facilities manager concept, which is based on proposals to develop ISACs references in the CEF Telecom 2018 Work Programme²⁸.

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

- EU Energy ISAC: ENISA plays a key role in the development and professionalisation of this ISAC. ENISA is a full member and responsible for providing expertise through organising webinars and educational sessions for its members. In September 2017 and November 2019, it hosted an ISAC meeting in Athens. The EE-ISAC members are preferably operators.

- EU Financial Institutions ISAC: This ISAC is the oldest one and ENISA has been actively involved for many years. It supports the ISAC, for example by hosting the mailing list. ENISA's involvement is mainly to legitimise EU participation. ENISA is an observer.
- EU Rail ISAC: ENISA facilitates 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 this ISAC. ENISA offers experience and support.

The September 2017 Joint Communication states: "Some first steps have been taken regarding specific critical sectors such as aviation and energy through the creation of EASA and by developing information sharing and analysis centres. The European Commission will fully contribute to this approach with support from ENISA. An acceleration is needed, particularly, with regard to sectors providing essential services as identified in the NIS directive."

ENISA will support the MS during the entire lifecycle of national/European ISACs by engaging all relevant stakeholders: competent national 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 and EU sectoral ones. The Agency will also consider utilising its sectoral expertise that it has acquired through past and current efforts to offer support (upon request) to ISACs by sharing knowledge, e.g. in the form of 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.

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 has participated as a Member of the Steering Board of CERT-EU, as the representative of EU decentralised 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 particularly 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 to the CERT-EU steering board on the evolution of services required by the agencies.

27 <https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services>

28 <https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2018-cef-telecom-calls-proposals>

Output O.3.2.2. – Cooperation with relevant EU institutions, agencies and other bodies on cybersecurity initiatives

ENISA has increased the 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 keep intensifying its cooperation efforts on cybersecurity with EU institutions and agencies and other relevant bodies regarding 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 ⁽²⁹⁾ (including EASA, EC3, CERT-EU, EDA — including civil/defence cooperation, EEAS, etc.). In addition to the organisation of exercises in close collaboration with Activity 4 (in particular O.4.1.1, O.4.1.2, O.4.1.3 and O.4.1.5), the relevant EU Agencies will closely collaborate regarding the establishment of common standard operating procedures to support the EU Cyber Crisis Cooperation Framework.

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

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

²⁹ 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>

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

The Agency will also continue supporting to plan and develop the European Cyber Security Challenge 2020. The goal for 2020 will be to further increase the interest in this type of event by promoting excellence in the form of cyber competitions. In the future, the ECSC's final competition could be followed by the creation of a 'Team Europe' that will represent Europe in potential international competitions. To this 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 activities to raise cybersecurity awareness like the European Cyber Security Month (ECSM). The ECSM addresses disparity of cybersecurity practices across Member States in two stages. The first stage is to support the Member States to increase awareness and optimise the behaviour of their citizens to achieve a solid foundation. The second stage should help to further lower cybersecurity risks by increasing the maturity of the citizen's behaviour at the European level.

ENISA and the European Commission can achieve the objectives of the European Cyber Security Month by utilising the pan-European campaign to ensure all Member States are actively committed to the European Cyber Security Month and that the industry is involved as well. The proposed pillars remain the same: support a multi-stakeholder governance approach; encouraging common public-private activities; assess the impact of activities, optimising and adapting to new challenges.

Output O.3.3.3 – Support EU MS in cybersecurity skills development

ENISA will promote a series of new activities regarding cybersecurity 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 at enhancing cybersecurity skills among EU citizens, in general, and cybersecurity experts, in particular. As part of this program, a skill development scheme and maturity model will be defined based on existing and similar frameworks and initiatives.

Summary of the outputs and performance indicators in Activity 3 - Capacity		
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>P: Operational training material development and customisation to the needs of a NISD Sector (details on operational category can be found on ENISA training website), Q4</p> <p>S: Dedicated training space and technical lab development, Q4</p> <p>P: Delivery of a training session of the NISD Sector with customised training material mentioned above, Q4</p> <p>S: TRANSITs (European CSIRT training event) support, Q4</p>	<p>At least one training material developed to support operational practices of CSIRTs in Europe.</p> <p>At least 5 CSIRTs to contribute to and validate the training material.</p> <p>At least one NISD critical sector covered in the training session.</p> <p>Support at least 3 TRANSITs events.</p>
Output O.3.1.2 – Support EU MS in the development and assessment of NCSS	<p>S: Support the MS in NCSS development and assessment, Q1-Q4</p> <p>E: 1 workshop with EU MS on NCSS development, Q2-Q4</p>	<p>At least 3 MS supported in the implementation of NCSS lifecycle (S).</p> <p>Engage stakeholders (competent national authorities or private sector) from at least 12 EU MS (E).</p>
Output O.3.1.3 – Support EU MS in their incident response development	<p>S: Supporting enhancement of CSIRTs capabilities and maturity in Europe, Q4</p> <p>P: CSIRT and IR landscape in Europe; updated status report, Q4</p> <p>P: CSIRT online inventory update – European interactive map of CSIRTs, Q2 & Q4</p> <p>S: CSIRT online inventory tool enhancement, Q4</p> <p>P: Online tool development for ENISA CSIRT maturity assessment, Q4</p> <p>S: Continue activities and involvement in CSIRT structures (e.g. FIRST, TF-CSIRT-TI, NATO NCIRC, GFCE including CEF MeliCERTes project), Q1-Q4</p>	<p>Identify and report on the number of MS supported and the type of support provided</p> <p>Two CSIRT inventory updates</p> <p>Provide an updated report on CSIRT and IR landscape in Europe</p> <p>Support or advisory provided at least to two CSIRTs to enhance their team's maturity.</p> <p>ENISA supports at least 2 international CSIRT or taskforce initiatives in community fora like FIRST, TF-CSIRT-TI or GFCE.</p>
Output O.3.1.4 – ISACs for the NISD Sectors in the EU and MS	<p>P: Specifications for a toolkit for ISACs, Q4</p> <p>S: Support relevant public and private stakeholders in establishing EU and national ISACs, Q1-Q4.</p> <p>S: Support EU (including European Commission's CEF initiative) and MS ISAC activities, Q1-Q4</p>	<p>At least 3 ISACs supported (S).</p> <p>Engage at least 12 organisations representing at least 3 sectors from at least 8 MS in this activity (P)</p>
Objective 3.2. Assisting EU institutions in capacity building		
Output O.3.2.1 – Liaison with the EU agencies on operational issues related to CERT-EU's activities	<p>S: Attending CERT-EU SB meetings</p> <p>S: Liaison with EU agencies using CERT-EU services notably through ICTAC</p>	<p>Consultation with EU agencies and representing their views at CERT-EU SB level.</p>
Output O.3.2.2 – Cooperation with relevant EU institutions, agencies and relevant bodies on cybersecurity initiatives	<p>P: Report on the cooperation activities with relevant union bodies, Q4</p> <p>S: Cooperation in organising events, conferences, workshops co-organized with EU institutions, agencies and relevant bodies on cybersecurity initiatives</p> <p>S: Contribute to the EU work on digital sovereignty as required, Q2 -Q4</p>	<p>Engage the relevant EU stakeholders (including EASA, EC3, CERT-EU, EDA, EEAS, etc.)</p> <p>Engage 10 stakeholders in the workshop and in the preparation of the recommendations.</p>

Summary of the outputs and performance indicators in Activity 3 – Capacity		
Outputs	Type of output (P=publication, E=Event, S=Support)	Performance indicator
Objective 3.3. Awareness raising		
Output O.3.3.1 – Cyber Security Challenges	S: European Cyber Security Challenge support, Q1-Q4 E: ‘Award workshop’ for winners of the European Cyber Security Challenge 2020 (ENISA promotes best of the best), Q2-Q3	At least two additional EU MS to 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 MS and at least 10 partners and representatives from different bodies/ MS to participate in/support ECSM 2020 (private and public sectors).
Output O.3.3.3 – Support EU Member States in the development of cybersecurity skills	P: Stocktaking of existing services and programmes in the EU that aim at enhancing cyber security skills among EU citizens, and cyber security experts, Q4	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, the so-called Cyber Europe 2020 (CE2020). In 2019, ENISA will prepare the plan for the CE2020. This exercise will closely follow up and build on the experiences 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 to better capture how incidents are being managed and how cooperation works in real life. The exercise will include explicit scenarios for the CSIRTs network, single point of contacts and competent authorities established under the NIS Directive. It will also focus on at least one essential sector. The exercise will also be designed to offer the opportunity to train the different aspects included in the Cyber Crisis Collaboration Blueprint, that was developed in collaboration with the European Commission, while also taking into account the recommendations provided by the NIS Cooperation Group (e.g. 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 resources, in 2020, ENISA will also expand the role of the observers (introduced in 2018) to add more value for the exercise overall.

The high-level exercise programme brief will include the strategic dimensions of the exercise and will be prepared based on the experiences from CE2019. To drive the whole planning process ENISA will assemble a group of planners from the participating countries to jointly develop a detailed exercise plan (ExPlan) in 2020. ENISA will involve planning group during the whole process and incorporate their input to create a consented plan. The exercise planning will avoid overlaps with other major related activities.

ENISA will consult the MS and seek approval of ENISA’s Management Board after consultation with the Cooperation Group and the CSIRTs Network on a possible joint EU-NATO cyber exercise in the coming years.

Output O.4.1.2 – Support activities for cyber exercises

In 2014, ENISA started the development of the Cyber Exercise Platform (CEP). The 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 materials will be developed to keep up the interest of the stakeholders and make the CEP a central tool for cybersecurity exercising for all stakeholders. The CEP platform enables ENISA to enlarge the user base and thus offer the operational cyber security communities opportunities to exercise and gain experience and increase their knowledge . One way to develop exercise incident materials is to engage the expert 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 to develop cybersecurity collaboration tasks based on an agreed roadmap.

In particular, ENISA will further develop 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 collaborate with the aforementioned organisations to build capacities and synergies in the areas of training, education 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 overload³⁰. 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 EU³¹, ENISA serves as "the focal point for information and knowledge in the cybersecurity community". As

30 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>

31 <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN>



a result, ENISA is in a unique position to leverage its network to gather information, process it and promote 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 prepare the EU Cybersecurity Technical Situation Report on incidents and threats on a regular basis, based on publicly available information, its own analysis and shared reports by the Member States' CSIRTs (on a voluntary basis) or NIS Directive Single Points of Contact, the 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 available to the relevant instances of the Council of the EU, the European Commission, the HRVP and the CSIRTs Network.”

To support the creation of these reports and to process the massive amounts of inputs they require in a meaningful way, ENISA has initiated the development of a tool that acts as a cybersecurity news sources aggregator, provides awareness and assists threat analysts in drafting cybersecurity reports in 2018. A first prototype is in place and has been reviewed by experts from ENISA, different EU institutions and the private sector to validate its added value for their work. In 2019, the next development phase will commence to get a ready to use product by the end of 2019 or beginning 2020. The tool is using the latest developments in AI and natural language processing to facilitate the creation of EU cybersecurity reports by providing a specialized cybersecurity search engine, that monitors trending news regarding cybersecurity 24/7 and has immediate access to ENISA's own work on relevant subjects. Additional functionalities and improvements will be added periodically according to the latest technological evolutions and the users' needs.

For this particular output, ENISA will rely on the experiences gained drafting the former EU Cybersecurity Technical Situation Reports with the prototype to further develop the Natural Language Processing features for the tool to transition from paragraph-based proposals to the production of meaningful sentences. Similarly, this experience will be leveraged to improve the Machine Learning algorithms of the prototype to significantly increase the number and type of information sources to be monitored.

Output O.4.1.5 – Supporting the EU Cyber Crisis Cooperation Blueprint

ENISA will support the European Commission on the implementation and improvement 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 European Commission's guidance and experiences from the EU PACE exercise, ENISA will drive initiatives to mitigate identified gaps in cooperation between:

- EU cybersecurity 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 handling and mitigation of cyber oriented crises.


ENISA will drive working groups to initiate or continue developing procedures in the context of the blueprint, from defining emergency directories and update processes to structuring cooperation activities during crises. This are the priorities named listed in the Blueprint.

ENISA will assist the 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 facilitate information exchange 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 to support the European 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 functionality by suggestions to improve cooperation and trust building between CSIRTs. The Agency will also support this cooperation, upon request by the members of the CSIRTs Network, by developing best practices and providing guidance in the area of operational community efforts such as on information exchange and secure communication. In particular, the Agency will be proactive in stimulating discussions within the network and providing content to support discussions on policy and technical initiatives according to the CSIRTs Network's own work programme.



The Agency will continue collaborating with other operational EU bodies to ensure a structured cooperation in line with the provisions of the Cybersecurity Act.

Trust and mutual respect is an important asset for CSIRT operations. Therefore, ENISA will continue to improve the level of trust in the network by offering trust building exercises and events in coordination with the CSIRTs Network governance. ENISA will take an active role in facilitating consensus between all Member States who participate in the CSIRTs Network in accordance with the NIS Directive.

The Agency will further provide, improve, develop and secure the CSIRTs Network infrastructure and tools including its alignment with MeliCERTes instances for CSIRTs Network member's smooth collaboration and administration use (e.g. CSIRTs Network portal and other communication means).

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 affected agencies (e.g. CEPOL, Eurojust) to support the cooperation between the CSIRT and the law enforcement communities and the extensions that this collaboration may have to other affected communities of stakeholders. ENISA is likely to continue its analysis and the production of training materials based on such analyses to lower the barriers for cooperation across these communities.

In addition, the Agency will continue collaborating 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 provisions of the Cybersecurity Act. The goal of the cooperation can be to reach joint policy outcomes to sustain the fight against cyber-crime; as such an interactive discussion format to identify root causes for limitations regarding cooperation can be considered, alongside trainings and joint workshops.

Output O.4.2.3 – Supporting the operations of MeliCERTes platform

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

Any particular CSIRT needs to maintain its data within the MeliCERTes framework. Some of the data must be vetted by the centralized workflow – such as the mandate or memberships in CSIRT communities – 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 to maintain the underlying team data and references. In this regard, also centralised workflows to maintain the Central Trust Circles (CTCs) of the MeliCERTes platform. In close cooperation with the CSIRTs Network, ENISA, will closely collaborate with the potential contractor of MeliCERTes II.

Summary of the outputs and performance indicators in Activity 4 – 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% of EU/ EFTA Member States and countries to 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 has to be 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 3 major 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 Cyber Crisis Cooperation Blueprint	S: Emergency directories and processes for cooperation activities during crises	At least 3 stakeholders of the blueprint are consulted.
Objective 4.2. Community building and operational cooperation		
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: Facilitate preparation of the next evaluation report for the cooperation group, Q1-Q4 P: 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, Q1-Q4 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: Further support for CNW specific information exchange and secure communication issues (according to the CSIRTs Network Action plan), Q4 S: Active secretariat support and engagement during annual Cyber SOPEX 2020 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 emanating from the 2019 A report on cooperation P: Optional training material based on such report E: Annual ENISA/EC3 workshop for national and governmental CSIRTs and their LEA counterparts, Q4 S: Structured cooperation with CERT-EU.	At least 5 MS CSIRT representatives, 5 MS law enforcement representatives and EC3 to participate in the preparation of the roadmap. At least 15 MS to 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 into account the legislative and policy developments in the area of EU Cybersecurity Certification and acting within the boundaries of its competence, ENISA will continue working to meet the requirements for the certification framework for ICT security products and services by for instance promoting mutual recognition or harmonisation of certification practices up to a certain level, in line with the Cybersecurity 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 in 2019, ENISA will provide support to the European Commission and the Member States in the policy area of EU cybersecurity certification framework within the scope of the Cybersecurity Act. ENISA will stimulate the interaction and involvement of stakeholders of the Member States, public policy and the industry in the emerging EU certification framework.

According to its new role defined by the Cybersecurity Act, ENISA will support the European Commission by joining the process of drafting a work programme for certification. By interacting with the European Commission, ENISA could assist in gathering requirements from the private sector and institutional stakeholders to facilitate the European Commission efforts based on an annual plan.

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 to facilitate 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 the European Cybersecurity Certification Group, potential subgroups thereof and the Stakeholder Cybersecurity Certification Group

Supporting the European Commission in its role as chair of the European Cybersecurity Certification Group, ENISA also helps with the organisation of the European Cybersecurity Certification Group and potential subgroups by providing services (to be determined with the European Commission) like support for the secretariat, organisational aspects etc. ENISA will also carry out its tasks as co-chair with the Commission of the Stakeholder Cybersecurity Certification Group, and provide secretariat services.

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. The implementation of SOG-IS as a scheme into the EU cybersecurity certification framework is a priority task for ENISA. Other areas of interest will gradually follow when developing the Union Rolling Work Programme and via requests addressed to the Agency. The aim of ENISA is to support public policy in EU cybersecurity certification to protect citizen rights (e.g. consumer rights, personal data, privacy etc.) and public interests (e.g. public purchasing in the MS by means of public procurement). Additionally, 5G will require particular attention to achieve the policy objectives. Provided there is a suitable prioritisation on the Union Rolling Work Programme for cybersecurity certification, ENISA will shift requests and Union Rolling Work Programme priorities to the scheme promulgation process. Additionally, a market analysis on the EU cybersecurity certification framework's impact on manufacturers and service providers is another area of interest.

Output 5.1.3 – Set-up and maintenance of a certification portal and associated services

There are technical and organisational tasks associated with setting up and maintaining a portal. An IT platform in support of the EU cybersecurity certification framework goes beyond the scope of a portal as it must accommodate the needs of all stakeholders involved (document management, user management, consultations) and enable the presentation of dependable information on certification schemes as required by the regulation.

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 comprehensive set of services that include planning, data collection, consultations, drafting and reviewing. ENISA will have developed a general methodology to prepare candidate cybersecurity certification schemes. ENISA will support by planning and prioritising and it will provide lists of stakeholders to give input and offer consultations. ENISA will develop a feedback mechanism for affected stakeholders e.g. standardisation organisations. ENISA will continue

to hold its EU Cybersecurity Certification Conference once or twice a year.

Output 5.2.2 – Tasks related to specific candidate schemes and ad hoc working groups

In accordance with the Rolling Work Programme or on request in accordance with the Cybersecurity Act, ENISA will develop candidate cybersecurity certification schemes based on the work from 2019 and its own knowledge as well as the input received from stakeholders. ENISA will support the lifecycle of the dedicated ad hoc working groups. ENISA will also follow up with its candidate schemes until they have been submitted to and accepted by the European Commission for formal consideration and eventual approval.

Summary of the outputs and performance indicators in Activity 5 – Certification		
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 the European Cybersecurity Certification Group, potential subgroups and the Stakeholder Cybersecurity Certification Group	S: Support the European Commission in the ECCG S: Support the SCCG along with the European Commission E : 1-4 ECCG and SCCG meetings p.a. E: 8 subgroup meetings	Planning and execution of tasks related to meetings; European Commission feedback
Output O.5.1.2 – Research and analysis of the market as an enabler for certification	P: 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 maintenance of a Certification portal and associated services	S: Tasks include review of requirements, implementation updates and 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 drafting, preparation and consultation process of the scheme (at least 10 private and or public organisations) At least 60 event participants from relevant stakeholders
Output O.5.2.2 – Tasks related to specific candidate schemes and ad hoc working groups	P: Numerous schemes produced throughout the year S: Support for the ad hoc working groups	Produce drafts of at least 2 schemes per year or 50% of the ones requested and prioritised by ECCG and the European Commission for 2020

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.

In 2020, the **Management Board (MB) 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 the commitment and other requirements.

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

The **Resources Department (RD)** oversees a variety of programs, projects and services related to the overall management of the Agency, supporting the Executive Director decisions in areas such as personnel, finance, procurement, purchasing, technology, facility management, health, safety, security, protocol, liaison with local authorities, MeliCERTes infrastructure, etc.

The aim of the RD is to support the Agency with the best possible level of efficiency and the best use of the resources made available to 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, protection of whistleblowers, declarations of interests, prevention of harassment, etc. are addressed within this activity.

RD strives to maintain and enhance the Agency's efficiency and effectiveness of the and to continuously contribute to ENISA's strategy both internally and externally by seeking optimal solutions for fulfilling ENISA's mandate and providing the necessary assurance of compliance.

The aim is to enable the Agency to minimize the resources needed with adequate and modern procedures and tools to maximise the intended outcome of the work programme and statutory commitments.

The Core Operations Department (COD)

coordinates the delivery of the Agency's core activities. As such, the main role of the COD is to take on activities A1-A5 of this work programme. The COD also includes the Policy Unit and the Public Affairs Team. COD also supports the Advisory group.

Policy Unit

The Policy Unit reports into the Head of Core Operations. Through the Policy unit, the Agency initiates and develops strategic cooperations with active relevant stakeholders from the cybersecurity community. For instance, the Agency engages in policy and strategy discussions with political decision makers (by participating or organizing e.g. EU MEP activities).

Furthermore, the Agency engages and develops strategic relationships with e.g. specific industry sectors at decision making level, and identifies the strategic issues regarding cybersecurity. The Policy Unit will also be able to support different institutions and bodies with regard to policy initiatives related to cybersecurity. Some of the results of these activities of the Policy Unit have been published as opinion papers on ENISA webpage.

Planning the Agency's activities, including the Single Programming Document preparation and coordination of the Work Programme are part of the Policy Unit's tasks.

The Policy Unit also includes the Public Affairs Team.

The Public Affairs Team (PAT) reports into the Head of the Policy Unit and is responsible for coordinating all communication activities, including media and press activities such as press releases, news items and interviews to enhance the reputation, visibility and the public image of the Agency. It supports the entire Agency with regard to publications, social media promotion, website management, public affairs activities and awareness campaigns. PAT is also responsible for establishing ENISA's corporate visual identity.

PAT also plays a major role in supporting events attended by the Agency, ensuring that ENISA is well represented from a public affairs perspective.

Quality management is part of the Policy Unit. 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 is being applied accordingly. Besides these activities, more details of the activities delivered by the Policy Unit and Public Affairs team are listed in Objective 6.2 – Engagement with stakeholders and international activities.

Internal control

ENISA aims at implementing the new COSO framework as well as its new requirements to be aligned 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 to provide independent and objective assurance to the Senior Management, Executive Director and the Management Board.

IT activities

During 2020 it is expected that the Agency has a new fully operating datacentre and, in partnership with other EU Agencies, a Disaster Recovery site at its disposal, which will enhance the availability of IT services. It will also help the Agency to be prepared for any challenges that may arise.

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

For 2020 and following up on the actions of 2019, the Agency will be heavily investing in strengthening its capabilities in the areas of information security and cybersecurity to continue its policy of having the best security posture possible.

IT supports all internal electronic infrastructures of the Agency, including, but not limited to core applications for business use and operation systems.

MeliCERTes. In 2020, ENISA will be running the central component of MeliCERTes. MeliCERTes will be the primary collaboration platform for CSIRTs of participating Member States as well as a means to improve EU MS preparedness, cooperation and coordination to improve cyber threat and cross-border incident response. The MeliCERTes project will be run in close cooperation with the EC and MS. The EC will get a new contract for several areas of the project for the near future. The long term sustainability and development of this project will be analysed in collaboration with all stakeholders involved.

Finance and Procurement

The Agency plans to upgrade its internally developed electronic tools used for Procurement to simplify and further automate its tasks related to tendering and contracting. This is deemed necessary due to the expected increase of the volume of the work based on a significantly increased operational budget. It is anticipated that the further development of the in-house systems should be outsourced. The aim is to

Summary of Outputs in Activity 6.1 – IT activities

Task	Objective	Level of completion 2020	Level of completion 2021	Level of completion 2022
Keep ENISA systems safe from cybersecurity incidents (from exterior) – detect, prevent, react and recover from threats	Security	100%	100%	100%
ENISA IT managed servers patched in time	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%

Summary of Outputs in Activity 6.1 – Finance and Procurement

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%

optimise the use of resources, enhance the internal control of all financial and procurement processes, to provide better reporting and subsequently a high level of transparency and efficiency. Internal policies are in constant evolution to ensure compliance with the Financial Regulation and Procurement rules. In line with the internal efficiency increase, the Agency upskills the internal guidelines and trainings to guarantee a clear guidance for internal use and to optimise the available resources.

Budget management identified the need to upgrade the supporting IT system (ENISA will look for best practices at other EU agencies).

Human Resources

The ultimate goal of HR is to attract, select, develop and retain highly qualified staff, to optimise organisational structures, to promote a safe working environment (which includes prevention of harassment), to create a culture that reflects ENISA's vision and values in which staff can reach their full potential and help 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 successfully manage ENISA statutory staff and external staff (e.g. trainees) in

Summary of Outputs in Activity 6.1 - Human Resources

Task	Objective	Level of completion 2020	Level of completion 2021	Level of completion 2022
Efficient management of selection procedures	Improve 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	4 months	4 months
Turnover of staff	Maintain a low 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%

compliance with the Staff Regulations/CEOS on a day-to-day basis. Additionally, investments and efforts are focusing on different projects such as the acquisition of an E-Recruitment tool, the development and adoption of a missions electronic tool used by the EC (MIPS) in close collaboration with the European Commission's services of SYSPER.

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. Legal Affairs' tasks also include dealing with complaints to the European Ombudsman and representing the Agency before the European Court of Justice of the European Union.

Data protection compliance tasks and data protection office

The main tasks of the Data Protection Officer (DPO) include³²:

³² 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

- Inform and advise ENISA on 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 point of contact for EDPS on issues related to the processing of personal data; cooperate and consult with EPDS whenever needed.

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 to secure the confidentiality, integrity and availability of the information systems of the Agency. The CISO is instrumental in incident handling and incident response as well as monitoring security events. The CISO also leads the security trainings for the Agency's



staff and provides security guidance on all IT projects, including the evaluation and recommendation of technical controls. In 2020, the CISO will contribute to these goals by:

- Developing assurance frameworks to demonstrate ongoing improvements of the information security management system. This includes:
 - developing KPIs
- Monitoring and reporting the following to the 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's staff
- Implementing new systems and tools that support improvements regarding information security.

Objective 6.2. Engagement with stakeholders and international activities

Stakeholder communication and dissemination activities

In 2020, ENISA will continue to focus on key activities and engage the increasing number of stakeholders.

This includes the different groups of stakeholders such as institutions, academia, industry, citizens, etc. In its engagement with the stakeholders, the Agency is guided by certain principles such as objectiveness, openness, transparency and inclusiveness.

Dissemination and outreach

The Agency will continue developing different tools and channels including the website and with a strong emphasis on social media. Dissemination activities are the responsibility of the Stakeholders Communication Team that will define the appropriate level of outreach activities to make ENISA's work available for all interested entities and to provide added value for Europe.

ENISA's reputation for quality and trust is of paramount importance to all stakeholders. It is highly important that all European citizens have trust in ENISA and its work. The cybersecurity challenges are increasing all over the globe and Europe is no exception. With this objective ENISA's reputation needs to be reinforced continuously. The outreach to promote the Agency's work is essential to create a NIS culture across the several actors in Europe. ENISA is aware of that and will work with everyone who is interested to reach the citizens that want to get information about the Agency's work.

Numerous activities that will increase the cybersecurity awareness across Europe are planned with different Member States to fulfill ENISA's mandate, mission and strategy until the end of 2020.

Summary of Outputs in Activity 6.2 – Dissemination and Outreach

Area	Metric	Increase Relative to Previous Year		
		2020	2021	2022
Volume of media material published by the Agency	Number of press communications published	10%	10%	10%
Number of social media items	Number of social media items published	20%	10%	10%
Number of social media followers	Number of social media followers	20%	15%	15%
Number of corporate events	Number of corporate events	10%	10%	10%
Website traffic	Number of page views/visits/unique visitors/returning visitors	15%	10%	10%

Summary of Outputs in Activity 6.2 - Internal communications

Area	Metric	Level of completion		
		2020	2021	2022
Maintain staff informed on ENISA Activities (internal communications)	10 staff meetings per year	100%	100%	100%
Team building activities	Events with participation of all staff	2	2	2

Internal communications

Within the RD, internal communications activities aim at keeping all those working within the Agency informed and enabling both management and staff to effectively and efficiently fulfill their responsibilities. A strong corporate culture improves staff engagement and ultimately supports the implementation of the work programme. 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.

ENISA Advisory Group

In 2020, ENISA will continue to support the ENISA Advisory Group and the group's contribution to the ENISA Work Programme.

The Advisory Group is composed of recognised experts representing the relevant stakeholders such as the ICT industry, providers of publicly available electronic communications networks or services, SMEs, essential service operators, consumer groups, academic experts in the field of cybersecurity, and representatives of competent authorities in accordance with Directive (EU) 2018/1972 of European standardisation organisations, as well as of law enforcement and data protection supervisory authorities.

The Advisory Group is a statutory body of ENISA pursuant to Article 21 of the Cybersecurity Act (Regulation (EU) No 2019/881). The Management Board, acting on a proposal by the Executive Director, sets up the ENISA Advisory Group for a tenure of 2.5 years.

The role of the Advisory Group is to advise ENISA regarding ENISA's performance, excluding Title III of the Cybersecurity Act which concerns the Cybersecurity Certification Framework. It shall advise the Executive Director on the creation of a proposal for ENISA's annual work programme and on ensuring communication with the relevant stakeholders on all related issues. During Q2 2020 a new Advisory Group will take office.

National Liaison Officer Network

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



A strong corporate culture improves staff engagement and ultimately supports the implementation of the work programme

ENISA will build on these activities with the NLO Network as an additional 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 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's deliverables, upcoming ENISA project related tenders, news, working groups entailing requests for identification of experts in the MS, vacancy notices, and events organised or supported (for example as co-organiser, etc.) by ENISA as well as time-sensitive information.

- The Agency will maintain and share information on all relevant ENISA projects and activities (e.g. unit responsible for the project, relevant tender results, etc.) with the NLO network while maintaining and expanding available online resources when appropriate.

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

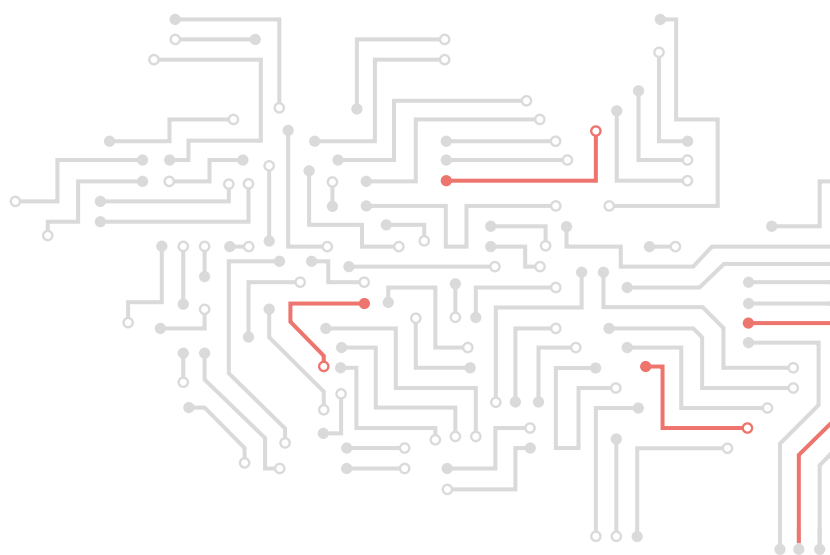
Under the executive director's guidance and initiative, ENISA will seek to strengthen contacts at an international level in line with the relevant provisions of the new Cybersecurity Act.




List of outputs in the 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 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 report
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 PSIRTs and NIS sectoral incident response expertise
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 technical 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
Output O.2.2.6 – Support the MS in improving the cybersecurity of 5G networks
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 Cyber Crisis Cooperation 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 the European Cybersecurity Certification Group, potential subgroups thereof and the Stakeholder Cybersecurity Certification Group
Output 5.1.2 – Research and analysis of the market as an enabler for certification
Output 5.1.3 – Set-up and maintenance of a certification portal and associated services
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 schemes and ad hoc working groups



A large, bold, white capital letter 'A' is centered in the upper half of the image. The background is a solid light blue color, overlaid with a dense, repeating pattern of white circuit board traces and nodes, resembling a printed circuit board (PCB) layout. The traces are thin and form a complex, interconnected network of lines and small circles, creating a textured, technical appearance.

A

ANNEX 1

RESOURCE ALLOCATION PER ACTIVITY 2020–2022

The upcoming sections of this Annex present the development of the past and current situation, as well as the distribution of resources and budget for the six activities of the WP2020.

Overview of the past and current situation

The WP 2020 is following the COM guidelines and MB's decisions. It 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 continued in the area of cybersecurity certification.

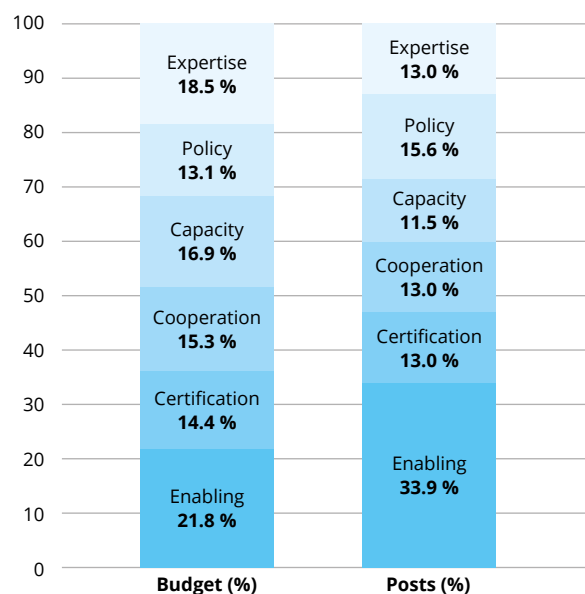
ENISA's budget comparing the years 2018 and 2019 is increasing due to the new mandate of the Agency and the scope of its new tasks.

As already presented, for 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. The past and current human and financial resources 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.

WP Budget and posts distribution (ABB)



The Agency applies a strict policy on ratio between “administrative support and coordination” staff and “operational” staff following the methodology set by the European Commission on the benchmarking

exercise. The European Commission levels up the overhead (administration support and coordination) up to 25%. The table below reflects the situation at ENISA:

Yearly ratio between “administrative support and coordination” staff and “operational” staff

Type	2016	2017	2018	2019	2020
Total Administrative Support and Coordination	19.04%	19.27%	22.89%	18.37%	17.54%
Administrative Support	15.47%	15.66%	19.28%	15.30%	14.91%
Coordination	3.57%	3.61%	3.61%	3.07%	2.63%
Total Operational	66.66%	66.27%	62.65%	69.39%	69.30%
Top Operational Coordination	7.14%	7.23%	7.23%	5.10%	4.39%
General Operational	59.52%	59.04%	55.42%	64.29%	64.91%
Total Neutral	14.29%	14.46%	14.46%	12.24%	13.16%
Finance and Control	14.29%	14.46%	14.46%	12.24%	13.16%

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 the draft Cybersecurity Act, to be allocated to the new Activity 5 on cybersecurity certification.

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

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

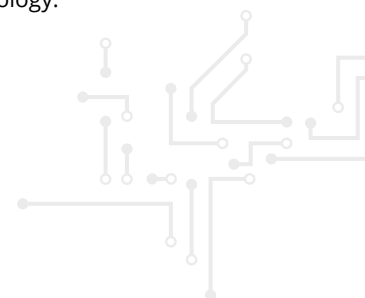
Overview of activities budget and resources

The budget and posts distribution is based on the Activity Based Budgeting (ABB) methodology of the Agency, which is in 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 estimation of necessary resources for each ENISA activity, the Agency needs to split the budget forecast into direct and indirect budget. The following assumptions are used based on 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 re-distributed 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 in the next page presents the allocation of financial and human resources to activities of the Agency based on the above ABB methodology.



Allocation of financial and human resources

WP2020	Total ABB budget (EUR)	Total ABB posts (FTEs)
Activity 1 – Expertise. Anticipate and support Europe’s knowledge in facing emerging cybersecurity challenges	4 035 288.27	14.45
Activity 2 – Policy. Promote network and information security as an EU policy priority	2 859 961.59	17.29
Activity 3 – Capacity. Support Europe in maintaining state-of-the-art network and information security capacities	3 682 690.26	12.78
Activity 4 – Cooperation. Foster the operational cooperation within European cybersecurity community	3 330 092.26	14.45
Activity 5 – Cybersecurity certification. Developing cybersecurity certification schemes for digital products, services and processes.	3 134 204.48	14.45
Activity 6 – Enabling. Reinforce ENISA’s impact	4 746 882.76	37.58
Total	21 789 119.62	111.00

ANNEX 2

HUMAN AND FINANCIAL RESOURCES 2020–2022

TABLE 1. EXPENDITURE OVERVIEW IN EURO

Expenditure	2019		2020	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1	9 387 948	9 387 948	12 041 486	12 041 486
Title 2	2 677 000	2 677 000	2 986 000	2 986 000
Title 3	4 868 004	4 868 004	6 761 633	6 761 633
Total Expenditure	16 932 952	16 932 952	21 789 120	21 789 120

Commitment appropriations

Expenditure	Executed budget 2018	Budget 2019	Draft budget 2020 Agency request	VAR 2020/2019	Envis- aged in 2021	Envis- aged in 2022
Title 1. Staff Expenditure	7 232 638	9 387 948	12 041 486	28%	13 343 500	13 875 000
11 Staff in active employment	5 443 399	6 794 000	10 181 000	50%	11 295 000	11 763 000
– of which establishment plan posts						
– of which external personnel						
12 recruitment expenditure	384 923	968 948	445 000	-54%	342 000	277 000
13 Social-medical services and training	74 541	325 000	250 000	-23%	305 000	375 000
14 temporary assistance	1 329 775	1 300 000	1 165 486	-10%	1 401 500	1 460 000
Title 2. Building, equipment and miscellaneous expenditure	1 637 468	2 677 000	2 986 000	12%	3 114 000	3 205 000
20 Building and associated costs	931 134	1 100 000	1 180 000	7%	1 234 000	1 234 000
21 Movable property and associated costs	29 882	58 000	99 000	71%	99 000	99 000
22 Current administrative expenditure	75 932	104 000	176 000	69%	201 000	201 000
23 ICT	600 520	1 415 000	1 531 000	8%	1 580 000	1 671 000
Title 3. Operational expenditure	2 702 890	4 868 004	6 761 633	39%	6 868 902	7 140 157
30 Activities related to meetings and missions	672 570	1 043 324	1 410 000	35%	1 421 124	1 426 512
32 Horizontal operational activities	367 257	614 680	1 001 633	63%	1 048 778	1 138 645
36 Core operational activities	1 663 063	3 210 000	4 350 000	36%	4 499 000	4 575 000
Total expenditure	11 572 955	16 932 952	21 789 120	29%	23 426 402	24 220 157

Payments appropriations

Expenditure	Executed budget 2018	Budget 2019	Draft budget 2020 Agency request	VAR 2020/2019	Envis- aged in 2021	Envis- aged in 2022
Title 1. Staff Expenditure	7 232 638	9 387 948	12 041 486	28%	13 343 500	13 875 000
11 Staff in active employment	5 443 399	6 794 000	10 181 000	50%	11 295 000	11 763 000
– of which establishment plan posts						
– of which external personnel						
12 recruitment expenditure	384 923	968 948	445 000	-54%	342 000	277 000
13 Social-medical services and training	74 541	325 000	250 000	-23%	305 000	375 000
14 temporary assistance	1 329 775	1 300 000	1 165 486	-10%	1 401 500	1 460 000
Title 2. Building, equipment and miscellaneous expenditure	1 637 468	2 677 000	2 986 000	12%	3 114 000	3 205 000
20 Building and associated costs	931 134	1 100 000	1 180 000	7%	1 234 000	1 234 000
21 Movable property and associated costs	29 882	58 000	99 000	71%	99 000	99 000
22 Current administrative expenditure	75 932	104 000	176 000	69%	201 000	201 000
23 ICT	600 520	1 415 000	1 531 000	8%	1 580 000	1 671 000
Title 3. Operational expenditure	2 702 890	4 868 004	6 761 633	39%	6 868 902	7 140 157
30 Activities related to meetings and missions	672 570	1 043 324	1 410 000	35%	1 421 124	1 426 512
32 Horizontal operational activities	367 257	614 680	1 001 633	63%	1 048 778	1 138 645
36 Core operational activities	1 663 063	3 210 000	4 350 000	36%	4 499 000	4 575 000
Total expenditure	11 572 955	16 932 952	21 789 120	29%	23 426 402	24 220 157

TABLE 2. REVENUE OVERVIEW IN EURO

Revenues	2019	2020	2021	2022
	Revenues estimated by the Agency	Revenues estimated by the Agency	Revenues estimated by the Agency	Revenues estimated by the Agency
EU contribution	15 910 000	20 646 000	22 248 000	23 023 000
Other revenue	1 022 952	1 143 120	1 178 402	1 197 157
Total revenues	16 932 952	21 789 120	23 426 402	24 220 157

Revenues	2018 Executed budget	2019 Revenue estimated by the Agency	2020 As requested by the Agency	VAR 2020/2019	Envis- aged 2021	Envis- aged 2022
1 Revenue from fees and charges						
2 EU contribution	10 529 000	15 910 000	20 646 000	30%	22 248 000	23 023 000
of which Administrative (Title 1 and Title2)						
of which operational (Title 3)						
of which assigned revenues deriving from previous years' surpluses	-38 436					
3 Third countries contribution (incl. EFTA and candidate countries)	248 626	382 952	503 120	31%	538 402	557 157
of which EFTA	248 626	382 952	503 120	31%	538 402	557 157
of which Candidate Countries						
4 Other contributions	685 662	640 000	640 000	0%	640 000	640 000
of which delegation agreement, ad hoc grants						
5 Administrative operations	109 707	0	0		0	0
6 Revenues from services rendered against payment						
7 Correction of budgetary imbalances						
Total revenues	11 572 995	16 932 952	21 789 120	29%	23 426 402	24 220 157

TABLE 3. BUDGET OUTFURN AND CANCELLATION OF APPROPRIATIONS. CALCULATION OF BUDGET OUTFURN IN EURO

Budget outturn	2016	2017	2018
Revenue actually received (+)	11 034 366	11 223 387	11 572 995
Layments made (-)	9 860 776	9 901 545	10 345 736
Carry-over of appropriations (-)	1 176 717	1 376 730	1 348 657
Cancellation of appropriations carried (+)	38 616	90 916	108 302
Adjustment for carry over of assigned revenues appropriations from previous year (+)	3 127	49 515	124 290
Exchange rate differences (+/-)	-180	-12	-689
Adjustment for negative balance from previous year (-)			
Total	38 436	85 535	110 505

Cancellation of appropriations

- Cancellation of Commitment Appropriations
In 2018, Commitment Appropriations were cancelled for an amount of EUR 1,751.66 representing 0.02 % of the total budget. ENISA demonstrates a commitment rate of 99.98 % of C1 appropriations of the year at the end of the year (31/12). The consumption of the 2018 budget at the end of the year shows the capacity of the Agency to fully implement its annual appropriations. The same level commitment rate is maintained for nine years in a row. The payment rate reached 88.56 % and the amount carried forward to 2019 is EUR 1,232,263.40 representing 11.42 % of the total C1 appropriations 2018.
- Cancellation of Payment Appropriations
No payment appropriations were cancelled.

- Cancellation of Payment Appropriations
Carried over (Fund source "C8" – appropriations carried over automatically from 2017 to 2018.)
The appropriations of 2017 carried over to 2018 were utilised at a rate of 92.33 % (automatic carry-overs) which indicates a satisfactory capability of estimation of needs. From the amount of EUR 1,411,440.51 carried over, the amount of EUR 108,302.57 was cancelled, due to the fact that the estimated expenditure deviated from the amount actually paid. This cancellation represents 1 % of the total budget.

ANNEX 3

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 budget for year 2019	Envisaged in 2020	Envisaged in 2021	Envisaged in 2022
Officials	AD								
	AST								
	AST/SC								
TA	AD	34	29	34	32	43	51	57	60
	AST	14	13	13	12	16	18	19	19
	AST/SC								
Total		48	42	47	43	59	69	76	79
CA GFIV		28	17	28	16	28	28	28	28
CA GF III		2	11	5	10	2	2	2	2
CA GF II			0	0	0	0	0	0	0
CA GFI			1	0	1	0	0	0	0
Total CA		30	29	33	27	30	30	30*	30
SNE		6	3	3	3	9	12	12	12
Structural service providers									
TOTAL		84	74	83	73	98	111	118	121
External staff for occasional replacement						5	5	5	5

* While the Agency acknowledges the decrease of CAs (minus 3) and increase of SNEs for 2020-2022, ENISA promotes a more flexible approach in the use of CAs as agreed by the EU Agencies Network, notably because the use of CAs shall be used as FTE and not headcounts in accordance with the wording of Article 33(2) of the Financial Regulations referring to estimate of number of contract staff expressed in full-time equivalent. The management of CAs is by nature a budget related notion being key for the Agency as a flexible resource allowing the adaptation to business needs focusing on results to achieve and Work programme.

Table 2. Multi-annual staff policy plan year 2020 – 2022 (including staffing evolution proposal to offer career path possibilities to staff)

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	
	OF	TA	OF	TA	OF	TA	OF	TA	OF	TA	OF	TA	OF	TA	OF	TA
AD 16																
AD 15		1		1				1				1				1
AD 14													1			
AD 13													1		2	
AD 12		3		3				6				6		5		4
AD 11													2		2	
AD 10		5		3				5				5		3		4
AD 9		10		4				12				12		12		11
AD 8		15		8				19				21		22		22
AD 7				3								3		8		8
AD 6				8								3		3		6
AD 5				1												
Total AD		34		31				43				51		57		60
AST 11																
AST 10																
AST 9																
AST 8														1		2
AST 7		2		1				3				4		4		3
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		43				59				69		76		79

ANNEX 4

HUMAN RESOURCES – QUALITATIVE

A. RECRUITMENT POLICY

Statutory Staff

The Agency continues to enhance the management of the selection procedures focusing on improving time to hire, developing best 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 strategic approach for HR focusing on competency-based interview's questions, tailor-made trainings for Board Member selection, alignment of competencies across the organisation per job profile, targeted recruitment procedures for specialised profiles, transversal recruitment procedures where reserve lists could be used to fill vacant positions across all departments/units, specific dissemination of job vacancies at ENISA, etc.

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

Assistant job family:

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

Operational job family:

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

Managerial job family:

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

The established type of posts are in line with Annex I and Article 80 of the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union, while the recruitment grades are in line with Article 3 of the MB Decision/12 of the ENISA on the general implementation provisions on

the procedure governing the engagement and use of temporary staff under Article 2(f) of the CEOS and EC Decision C(2011) 1264.

ENISA evaluates the available options with all due care to not recruit at excessive grade levels and in line with the Establishment Plan. Nevertheless, in some cases, the recruitment of experts set above the entry grade was used as the only solution to attract the right profile(s) and to ensure nationality balance (e.g.: TA/AD12 Lead expert for certification). In the same logic, the use of the AST/SC grade for secretarial positions, while being in place since the 2014 Staff Regulations Reform, would negatively impact the attraction and retention of qualified and geographically diverse staff.

Concerning the duration of employment, the typical duration was a long-term contract of three years, renewable for another limited period of five years with a second renewal for an indefinite period. While it remains the case for Contract Agents (3+5+indefinite), the duration for contracts of Temporary Agents was amended³³ to improve the attractiveness and retention. Hence, the typical duration for newly recruited Temporary Agents is an initial 5-year contract with the possibility to be renewed for an indefinite period. However, all contract renewals are subject to an assessment of the performance of the staff member, the 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 the past, ENISA used short-term contract agents (two years, renewable once for a maximum one year) but came to the conclusion that this type of contract does not meet the long-term needs of the Agency in delivering the objectives. It does not mean that depending on the business needs and the volatility of the workforce market, the Agency won't make use of this possibility again.

Non-Statutory Staff

ENISA welcomes Seconded National Experts (SNEs) as an opportunity to foster the exchange of experiences and knowledge of the Agency's working methods and to widen the expert 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 of time. 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. ENISA is applying a qualitative performance management based on the European Commission Model.

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 enables 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 reclassification are two different exercises.

³³ ED Decision 16/2019 of 20 February 2019

Table 1. Reclassification of temporary staff/promotion of officials

Category and grade	Staff in activity at 01.01.2018		How many staff members were reclassified in 2019		Average number of years in grade of reclassified/promoted staff members
	officials	TA	officials	TA	
AD 16					
AD 15		1			
AD 14					
AD 13					
AD 12		3			
AD 11					
AD 10		3			
AD 9		2			
AD 8		10		2	2.5
AD 7		3			
AD 6		7		2	4.25
AD 5		1			
Total AD		30			
AST 11					
AST 10					
AST 9					
AST 8					
AST 7		1			
AST 6		2			
AST 5		2			
AST 4		6		1	2
AST 3		2		1	5
AST 2					
AST 1					
Total AST		13			
AST/SC1					
AST/SC2					
AST/SC3					
AST/SC4					
AST/SC5					
AST/SC6					
Total AST/SC					
Total		43		6	

Table 2. Reclassification of contract staff

Function group	Grade	Staff in activity at 01.01.2018	How many staff members were reclassified in 2019	Average number of years in grade of reclassified staff members
CA IV	17			
	16	1		
	15	1		
	14	11		
	13	3		
CA III	11	1		
	10	2	3	6
	9	7	1	5
	8	2		
CA II				
CA I	3	1		
Total		29	4	

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), like all other Agencies, to offer mobility possibilities to the Agency employees by assuring a continuation of careers and grades. Additionally, ENISA is also open to mobility between the agencies and the EU Institutions.

- Mobility within agency: since January 2019, 13 staff members were moved under Article 7 of Staff Regulations.
- Mobility among agencies: in 2019, 1 staff member was recruited under Inter-Agency Mobility Call.

- Mobility between agency and Institutions: in 2019, 3 former ENISA staff members moved to EU agencies and 1 former employee moved to an EU Institution.

D. LEARNING AND DEVELOPMENT

The Agency is striving for excellence when it comes to staff development. 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.

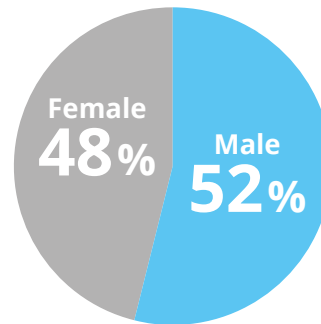
E. GENDER AND GEOGRAPHICAL BALANCE

The overall gender balance among ENISA staff shows a slight 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 terms of gender and nationality as far as possible. In 2019, the Agency had 2 women HoUs (Head of HR unit and Head of Finances and Procurement unit) and 6 women coordinating teams.

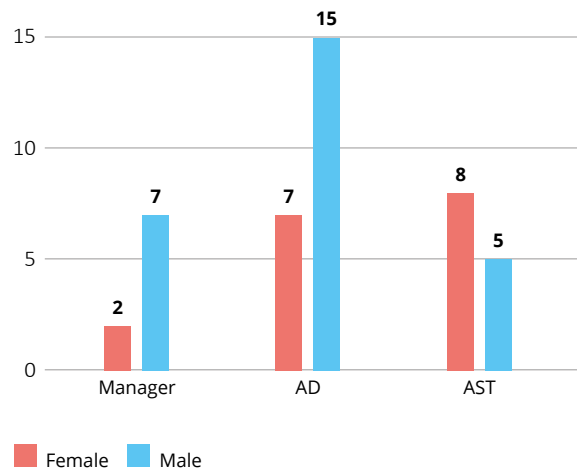
With regard to the geographical balance, while there is no quota system in operation, when recruiting, the Staff Regulations require to strive for a broad balance among nationalities and to adopt necessary measures if there is imbalance between nationalities among staff. ENISA is paying great attention to this requirement. However, ENISA is facing the same challenges (as reported by the European Commission for the European Civil Service and as with some other EU Agencies with low coefficient correcteur) in attracting and retaining some nationalities. This is mainly due to the specific labour market where ENISA operates and high salaries in the private sector which ENISA is cannot compete with due to low corrector coefficient. Hence, ENISA is facing challenges in increasing its visibility on the market as an employer of choice. Moreover, ENISA is not offering an accredited European School in Athens and, at the same time, partners of the staff members lack the possibility to find a job, which makes the situation even more difficult for ENISA to attract staff from some specific nationalities. ENISA is committed to ensure a diverse workforce representation, however strives to retain staff from some nationalities on the abovementioned consideration.

The graphics reflect the situation as for 31.12.2018.

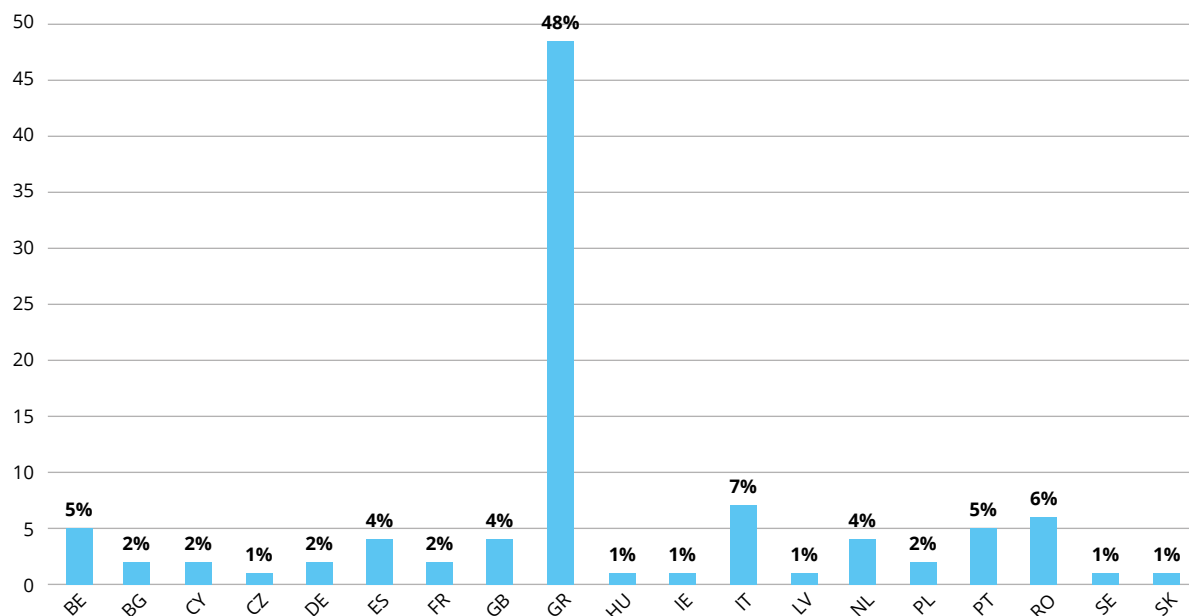
Per Gender



Gender Distribution for Establishment Plan job category (TAs)



Per Nationality



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 agreements concluded with a number of international schools.

2019-2020 school year	CRECHES	SCHOOLS
ATHENS	15	32
HERAKLION	0	5

ANNEX 5

BUILDINGS

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

A new seat agreement between ENISA and the Hellenic Authorities entered into force on the 04/10/2019. As per the new seat agreement signed by ENISA and the Hellenic Authorities, the Agency will continue having premises in Athens and Heraklion as it had under the previous agreement. However, the permanent seat of the Agency is now in Athens having the majority of its staff there. The premises of ENISA in Athens are privately owned and rented by the Agency, while the premises in Heraklion are located in a public building made available by the Hellenic Authorities. The payment of rents for the premises in Athens and Heraklion are covered by the Hellenic Authorities who provide up to 640 000 euro per year.

The current building in Athens will not suffice to accommodate all the new staff that will be joining the Agency in virtue of the new Mandate with the additional challenge that the current renting contract expires on 31/12/2021 with no possibility for extension. ENISA is in constant contact with the Hellenic Authorities to find suitable premises to accommodate all staff in the near future.

ANNEX 6

PRIVILEGES AND IMMUNITIES

Agency privileges	Privileges granted to staff	
	Protocol of privileges and immunities / diplomatic status	Education / day care
In accordance with Art. 23 of Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019, 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.	<p>In accordance with Article 35 of Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019, 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.</p> <p>The Greek Government and ENISA signed a seat agreement on 13 November 2018, which was ratified by Greek Law 4627/2019 on 25 September 2019 and is applicable to ENISA and its staff.</p>	A public School of European Education, Type 2, was founded in 2005 by the Greek government in Heraklion, Crete, for the children of ENISA's staff. There is no European School operating in Athens.

ANNEX 7

EVALUATIONS

ENISA uses an internal monitoring system (MATRIX) that is also used for project management. ENISA's management team regularly uses this information, which is also used for monthly reporting. Moreover, ENISA has implemented a mid-term review procedure and monthly management team meetings.

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

ANNEX 8

RISKS 2020

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

ANNEX 9

PROCUREMENT PLAN 2020

2020 procurement planning	Direct budget (EUR)	Procurement (tendr) procedure required	Launch dates	All other expenditure
Activity 1 – Expertise. Anticipate and support Europe’s knowledge in facing emerging cybersecurity challenges	1 070 000	885 000	Q1-Q4	185 000
Activity 2 – Policy. Promote network and information security as an EU policy priority	540 000	430 000	Q1-Q4	110 000
Activity 3 – Capacity. Support Europe in maintaining state-of-the-art network and information security capacities	1 010 000	780 000	Q1-Q4	230 000
Activity 4 – Cooperation. Foster the operational cooperation within European cybersecurity community	830 000	660 000	Q1-Q4	170 000
Activity 5 – Cybersecurity certification. Developing cybersecurity certification schemes for digital products, services and processes.	900 000	720 000	Q1-Q4	180 000
Activity 6 – Enabling. Reinforce ENISA’s impact	1 211 633	631 000	Q1-Q4	580 633
Total	5 561 633	4 106 000		1 455 633

ANNEX 10

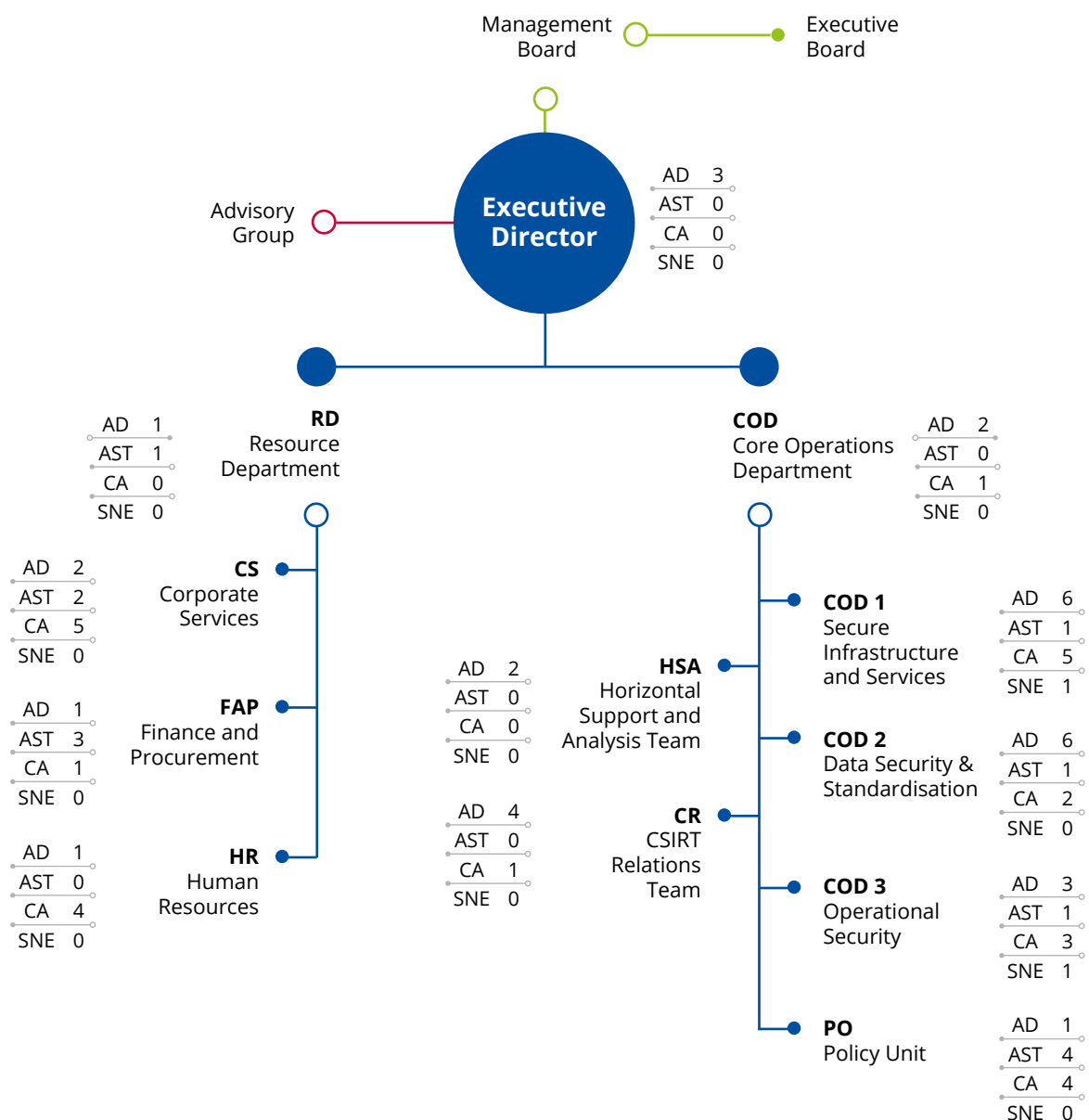
ENISA ORGANISATION

As provided in the Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019, the bodies of the Agency comprise:

- A Management Board: The Management Board ensures that the Agency carries out its tasks under conditions that allow it to serve in accordance with the founding Regulation.
- An Executive Board: The Executive Board prepares decisions to be adopted by the Management Board on administrative and budgetary matters.

- An Executive Director: The Executive Director is responsible for managing the Agency and performs his/her duties independently.
- An Advisory Group: The AG advises the Executive Director in the performance of his/her duties under this Regulation.
- A National Liaison Officers Network: The NLOs facilitate the exchange of information between ENISA and the EU Member States.

The ENISA organisation valid as of 01.11.2019 with active staff is as follows:



ANNEX 11

SUMMARISING THE KEY INDICATORS FOR THE MULTIANNUAL ACTIVITIES

In line with the prescribed European Commission approach, the Agency is in an ongoing process to improve the standing of its key indicators for the purpose of improving measuring and reporting better matching the deliverables of its annual work programme.

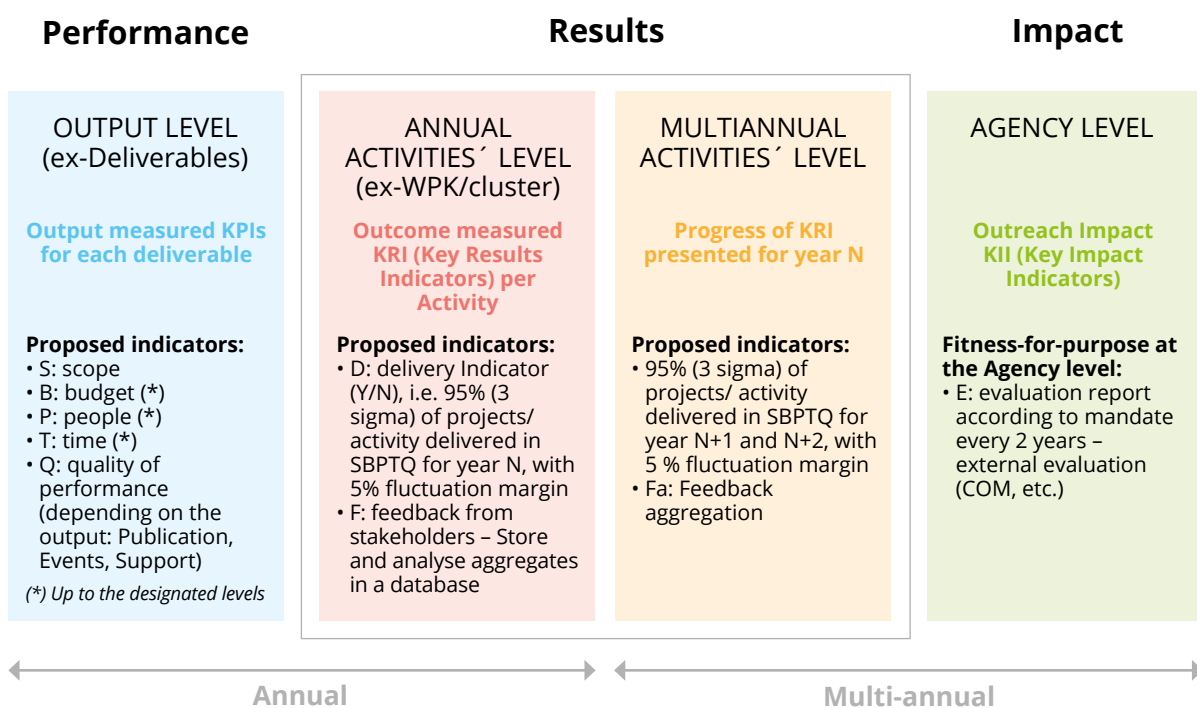
The purpose of the key indicators for ENISA is to provide the metrics to measure the performance, results and impact of the Agency's outcome, output and impact. Key indicators seek to better depict policy dynamics on network and information security, an area of policy that still is under development at 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

by taking the capability of the Agency to report into account as well as the need to avoid any unnecessary burden on the Agency. The Agency's capability to report reflects effort, organisational measures and tools available (or that can be obtained relatively easily). Measuring operational performance that concerns the policy raison d'être of the Agency remains the focal point for the key indicators introduced. The key notions and main vectors of annual and multi-annual measurements are presented hereunder.

Key indicators at ENISA seek to measure:

- Performance that is a concern at the output level when deliverables are produced. Metrics used are project management-based and they include:
 - a. Adherence to the scope of the deliverable or project;



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					

- b. Budget (or financial resources) available to the output or project, remaining within prescribed levels with a $\pm 5\%$ margin;
 - c. People (or human resources) available to the output or project, remaining within prescribed levels with a $\pm 5\%$ margin;
 - d. Time available to carry out the output or project remaining within prescribed levels with a $\pm 5\%$ margin;
 - e. Quality of performance depending on the type of output, according to the classification of output in the work programme (being, publication, event, support).
- Results that are a concern at the annual and at multi-annual activities' level. The indicators used are as follows:
 - a. Delivery indicator aiming at delivering at least 95% matched with the work programme planning. This is equivalent to a 3σ (3 Sigma) organisation (reaching between 93.3% and 99.3%); clearly the Agency has historically proven its operational ability to deliver at a 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 $\pm 5\%$.³⁴ The criteria used, i.e. scope, budget, people, time and quality, all refer to the proper execution of the project leading up to the production of the 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 gathered on a multi-annual basis by the Agency.

³⁴ 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.

- 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.

Feedback is collected by using surveys. It is envisaged that the website's deliverables section will be leveraged to gather targeted feedback against each deliverable. However, this will only be made available in 2018 the earliest.

The key indicators broken down at the output level, the activities level and the Agency level, are presented in the previous page.

Below you can find an example of output related indicators to be collected regarding the key types of Agency output, namely, publication, event, support.

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

- Green reflects a 5% deviation, which means that planning/performance is appropriate and within prescribed levels.
- Yellow reflects a 20% deviation, which means that planning/performance needs to be revisited.
- Red reflects a deviation above 20%, which means that planning/performance needs a thorough review.

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

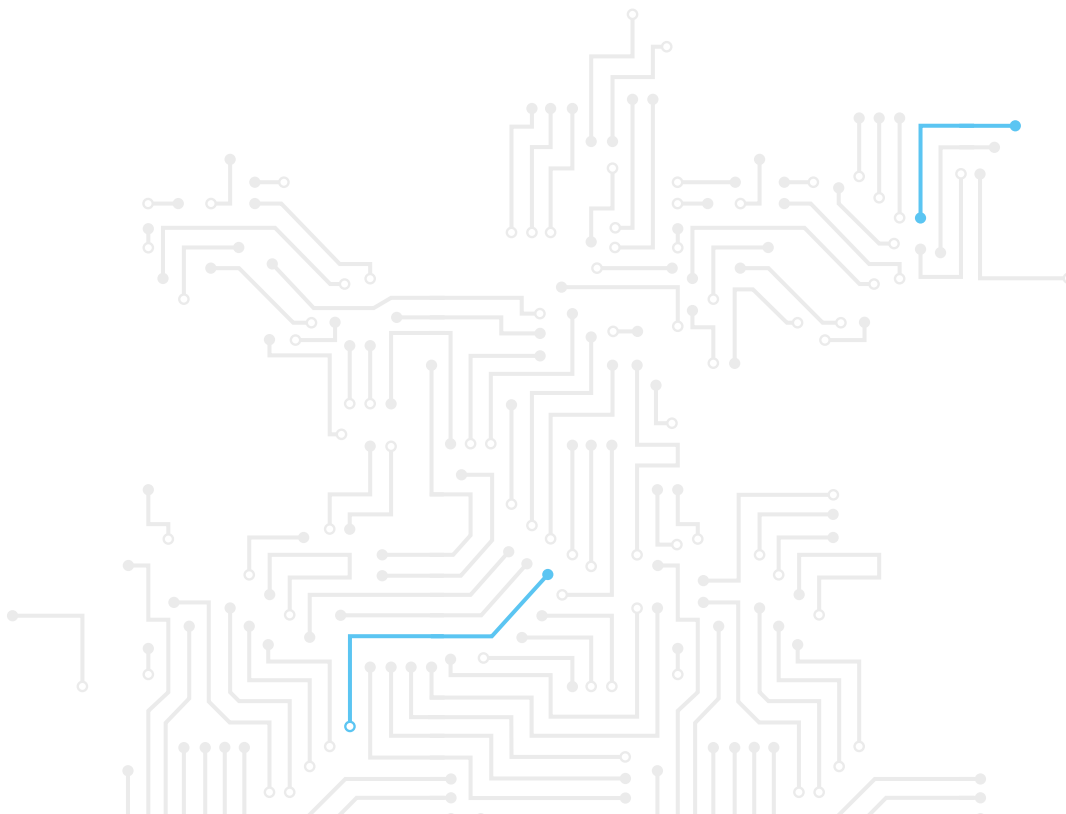
* Publication e.g. methods for security and privacy cost analysis

** Event e.g. WS on privacy and security

*** Support e.g. NIS portal

Below you can find an example of outcome related indicators to be collected regarding 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	Multiannual activity x,y,z evolution
Delivery related	e.g. output instantiations 70% Green 20% Yellow 10% Red	e.g. output instantiations 80% Green 10% Yellow 10% Red	e.g. output instantiations 90% Green 10% Yellow 0% Red	In each 3 year period we gather feedback 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 gather feedback on a per activity level: 50% positive 41% neutral 9% negative



ANNEX 12

LIST OF ACRONYMS

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

ANNEX 13

LIST OF POLICY REFERENCES

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

Reference	Policy/legislation reference. Complete title and link
2019	
Recommendation on Cybersecurity of 5G networks	Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks C(2019) 2335 final, available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58154
Cybersecurity Act	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15–69, available at: http://data.europa.eu/eli/reg/2019/881/oj
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
Draft Cybersecurity Act	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

Reference	Policy/legislation reference. Complete title and link
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 EUROPEAN 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 EUROPEAN 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 European 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 of the EU conclusions on the European 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 the EU 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	European 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	European 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

Reference	Policy/legislation reference. Complete title and link
2012	
Action Plan for an innovative and competitive Security Industry	Communication from the European 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 EUROPEAN 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 European 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 European 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

ANNEX 14

OUTPUT SYNERGIES

	0.1.1.1	0.1.1.2	0.1.1.3	0.1.1.4	0.1.1.5	0.1.1.6	0.1.2.1	0.1.2.2	0.1.2.3	0.1.2.4	0.1.3.1	0.2.1.1	0.2.2.1	0.2.2.2	0.2.2.3	0.2.2.4	0.2.2.5	0.2.2.6	0.3.1.1	0.3.1.2	
0.1.1.1																					
0.1.1.2												●									
0.1.1.3																					
0.1.1.4												●									
0.1.1.5												●		●							
0.1.1.6											●										
0.1.2.1																			●		
0.1.2.2																					
0.1.2.3																	●	●			
0.1.2.4																			●		
0.1.3.1						●															
0.2.1.1	●		●	●																	
0.2.2.1																●					
0.2.2.2					●													●		●	
0.2.2.3																●					
0.2.2.4													●		●						
0.2.2.5									●									●			
0.2.2.6						●		●					●				●				
0.3.1.1										●											
0.3.1.2														●							
0.3.1.3										●									●		
0.3.1.4										●		●									
0.3.2.1																					
0.3.2.2																					
0.3.3.1																					
0.3.3.2																			●		
0.3.3.3							●												●		
0.4.1.1																					
0.4.1.2																					
0.4.1.3																					
0.4.1.4							●														
0.4.1.5																					
0.4.2.1										●											
0.4.2.2										●											
0.4.2.3																					
0.5.1.1																					
0.5.1.2																					
0.5.1.3																					
0.5.2.1																●					
0.5.2.2																●		●			

ANNEX 15

OUTPUT PRIORITIES

The table below highlights the outputs, which, according to ENISA should be considered as high priority. The Agency will seek to minimise the effects of any budgetary or resource restrictions on high priority outputs.

List of Outputs in the WP2020	High Priority
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 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 report	●
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 PSIRTs and NIS sectoral incident response expertise	
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 technical 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	●
Output O.2.2.6 – Support the MS in improving the cybersecurity of 5G networks	●
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	●

List of Outputs in the WP2020	High Priority
Output O.3.1.4 – ISACs for the NISD Sectors in the EU and Member States	●
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 Cyber Crisis Cooperation 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 the European Cybersecurity Certification Group, potential subgroups thereof and the Stakeholder Cybersecurity Certification Group	●
Output 5.1.2 – Research and analysis of the market as an enabler for certification	●
Output 5.1.3 – Set-up and maintenance of a certification portal and associated services	●
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 schemes and ad hoc working groups	●



NOTES



ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity.

We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities.

Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu

ENISA

European Union Agency for Cybersecurity

Athens Office

1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion Office

95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu



Publications Office



ISBN 978-92-9204-324-7