European Union Agency for Cybersecurity

DECISION No MB/2020/1 of the Management Board of the European Union Agency for Cybersecurity (ENISA) endorsing the draft Programming Document 2021-2023, the draft Statement of estimates 2021 and the draft Establishment plan 2021

THE MANAGEMENT BOARD OF ENISA,

Having regard to the 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)[1], in particular Article 15.1.(c), Article 24.3., Article 24.4., and Article 29.7;

Having regard to the Decision No MB/2019/8 on the Financial Rules applicable to ENISA in conformity with the Commission Delegated Regulation (EU) No 2019/715 of 18 December 2018 of the European Parliament and of the Council, in particular Article 32;

Having regard to Commission Communication C(2014) 9641 final, on the guidelines for programming document for decentralised agencies and the template for the Consolidated Annual Activity Report for decentralised agencies dated 16.12.2014.

Whereas:

(1) The Management Board should produce, on the basis of the draft drawn by the Executive Director, a statement of estimates of revenue and expenditure for the following year which will be forwarded by the Management Board to the Commission by 31 January 2020;

(2) The Management Board should endorse the draft programming document by 31 January 2020;

(3) The Agency should send the draft programming document to the Commission, the European Parliament and the Council no later than 31 January 2020;

(4) The Agency has a new Executive Director since mid-October 2019 while a new policy agenda is being rolled out by the new European Commission appointed at the end of November 2019;

(5) In November 2019, the Agency started a process to develop a new strategy for the next years.

[1] *OJ L 151, 7.6.2019, p. 15–69*

HAS DECIDED TO ADOPT THE FOLLOWING DECISION:

Article 1

The Programming Document 2020-2022 is endorsed as set out in the Annex 1 of this decision.

Article 2

The Statement of estimates of revenue and expenditure for the financial year 2021 and the Establishment plan 2021 are endorsed as set-out in Annex 2 and Annex 3 of this decision.

Article 3

The present decision shall enter into force on the day its adoption. It will be published on the Agency website.

Done at Athens on 3 February 2020.

On behalf of the Management Board,

[signed]

Jean-Baptiste Demaison

Chair of the Management Board of ENISA

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA PROGRAMMING DOCUMENT 2021-2023

Including Multiannual planning,
Work programme 2021 and
Multiannual staff planning

VERSION: DRAFT V3, FEBRUARY 2020

DOCUMENT HISTORY

//DRAFT ONLY - DELETE THIS SECTION AND PAGE UPON FINAL PUBLICATION

Date	Version	Modification	Author
January 2020	V1	First draft sent for MB consultation.	ENISA
January 2020	V2	Draft for MB consultation/adoption.	ENISA
February 2020	V3	Draft for MB adoption	ENISA

Table of contents

INTRODUCTION

ABOUT THIS VERSION

[*the aim of this section is to guide and inform the reader of the context and of the limitations of the January 2020 version of the draft WP2021 and will be significantly reviewed, with a changed focus, before adopting the final WP*]

This draft version of WP2021 is prepared in a unique context for the agency. With the EU Cybersecurity Act, Regulation (EU) 2019/881 (CSA), that entered into force in June 2019, the Agency has a new permanent mandate, with strengthened roles and responsibilities. This gives the agency an opportunity and an obligation to assess, review and re-think the strategy of the agency, to readjust its Work Programme and resource planning and to identify possible synergies and efficiency gains. Furthermore, the agency has a new Executive Director since mid-October 2019 while a new policy agenda is being rolled out by the new European Commission appointed at the end of November 2019.

Thus, in the context of this initial draft Work Programme of 2021, the following considerations should be taken into account:

Firstly, at the request of its Management Board (MB), the agency embarked in November 2019 in a process to develop a new strategy for the next years. While this process is designed to gather input and expertise from within the agency as well as from its main statutory stakeholders, this also means that the process will require several months before the final document is agreed, finalized and adopted by the Management Board. Therefore, the structure of the draft WP2021, might need to be adjusted once the strategy is finalised.

Secondly, the draft WP2021 aims to build an agile work programming framework which takes into account the changed role and tasks of the agency, its transformation from a temporary body, into an agency with a permanent mandate and institutionalized roles, with recurring and multiannual statutory tasks that stem from the Union's regulatory framework. Moreover, other statutory bodies, have also now an important role to help to define the tasks the Agency undertakes:

- The NIS Cooperation Group (NISCG) and CSIRT network established according to the NIS Directive (EU) 2016/1148 (NISD), through particularly their multiannual rolling Work Programmes;
- The European Cybersecurity Certification Group (ECCG) established with the CSA and in particular the 3-year Union Rolling work programme for European cybersecurity certification shemes (to be adopted by the European Commission by 28 June 2020);

The work programme of the NISCG set up by the NISD should become available during the preparation of this draft document (end of January 2020), however the Union rolling work programme will only be available during the summer of 2020. When adopting the WP2021, the management board will thus also need to consider and build synergies with these other statutory frameworks.

Thirdly, there are also number of other activities that must be carried out as requests addressed to the Agency as indicated in the CSA, NISD, EEC or eIDAS regulation. However, since 2013, the agency has responded to various requests pursuant to Article 14 of its previous Founding

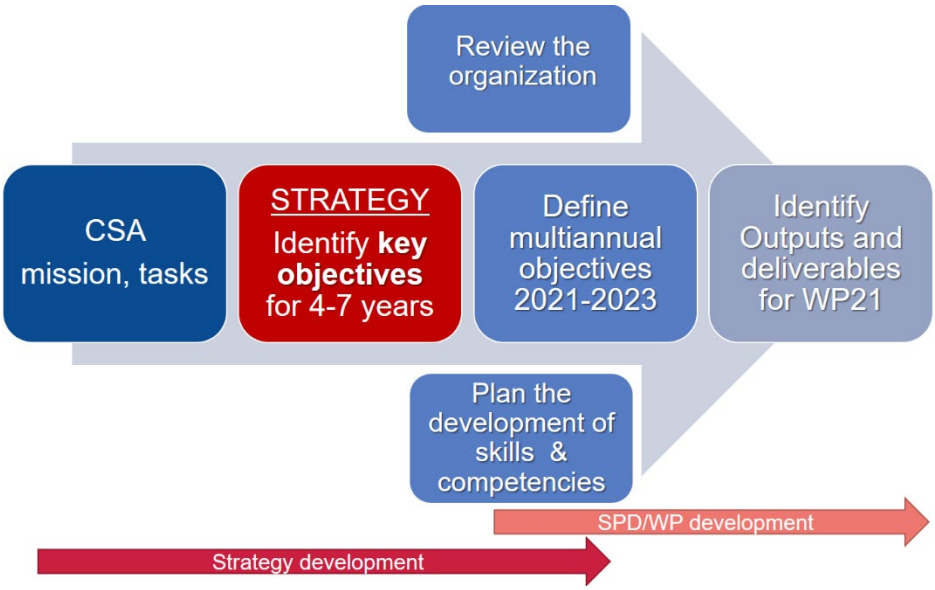
Regulation (EU) 526/2013. This provision has been replaced by request mechanisms within the framework of the specific tasks of the Agency as described in Title I, Chapter II of the CSA.

The following actors are able to make requests to the agency pursuant to the Cybersecurity Act:

- Member States of the EU (Arts. 6, 7, and 8);
- European Commission (Arts. 7 and 11);
- European Data Protection Board (Art. 5)
- Other EU institutions/bodies (Arts. 5 and 7).

This context requires more agility from the agency compared with previous years. While this document is designed to comply with the requirements listed by the Financial Framework regulation and the external dependencies, it is also allowing enough flexibility to adjust to the strategy that is now in the process of being developed.

The upcoming strategy of the agency will provide key objectives and priorities for the future.



While other goals are to be achieved to reflect the strategy discussion i.e. the reorganisation of the Agency and the development of a plan for skills and competencies to improve efficiency and synergies, for the purpose of this document, it should be noted that the strategy, once finalized, will require certain adjustments in the agency's Single Programming Document.

In the draft SPD2021-2023/WP2021, the activities of ENISA are described in two main parts:

i. Activities directly related to the implementation of the core statutory tasks, as outlined in Articles 5 to 12 of the CSA and stemming from regulatory obligations outlined above (NISD, CSA, EEC, eIDAS etc). For each of these tasks the agency identified key multiannual objectives, defined the expected results and performance indicators for the multiannual planning section. However, it should be noted that this part of the document, as well as the WP21 dedicated section, will need to be adjusted also depending on the adoption of the rolling work programmes of ECCG and NISCG; Furthermore, the ENISA strategy will give input to the ENISA WP2021 and provide strategic priorities as well as revised targets and indicators and where possible, clustering of various activities to build synergies and achieve efficiency gains. For the WP21 section, some of the outputs cover more than one CSA article, however, to simplify the allocation of resources, such outputs are allocated to one of the CSA articles.

ii. Other cross cutting activities. For this part of the document, that refers to internal management cross-cutting issues, a similar presentation with previous years was followed. However, the sections which cover actions to deliver cross-cutting activities (2.2. and 3.2.) will also need to be reviewed not only due to the ongoing development of ENISA's new Strategy, but also due to announced reorganisation of the agency (foreseen in Spring 2020), and the pending work done via three internal processes, mainly the upcoming review from the Task Force on Internal Controls (due in January 2020), Task Force on HR, recruitment and talent management (in February 2020) and from the Task Force on IT systems audit and inventory (Spring 2020).

The initial allocation of financial and human resources are presented in the Annexes of the document.

MISSION STATEMENT

[to be updated once the new Strategy is adopted]

According to Article 3 of the Cybersecurity Act, regulation (EU) 2019/881, the mission of the EU Agency for Cybersecurity is to achieve: "*a high common level of cybersecurity across the Union, including by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. The agency shall act as a reference point for advice and expertise on cybersecurity for Union institutions, bodies, offices and agencies as well as for other relevant Union stakeholders.*"

SECTION I. GENERAL CONTEXT

[as the aim of this section would be to give the reader and understanding of the relevant context as it should appear in October/November 2020, it will need to be reviewed in the next version according to the technical, legal, political and societal developments]

With the publication of Cybersecurity Act in 2019, the agency became a key instrument for realising the EU's ambition of significantly reinforcing cybersecurity across Europe. The CSA foresaw the strengthening of the agency, a process which started already well in advance of 2019, gathered pace in 2020 and will need to continue in the years to come.

As a new task, CSA set up a framework for European Cybersecurity Certification schemes with a view to creating a digital single market for ICT products, services and processes. The agency has started to execute this function fully in 2020. In particular, ENISA has started to work on two candidate schemes respectively for common criteria and cloud services. The Agency will continue to develop its role in the preparation of the candidate schemes, thereby contributing to the harmonisation of EU cybersecurity market, and building trust among market participants and strengthening the dialogue with cybersecurity industry, research and innovation communities.

The CSA also supports and expands the agency's tasks set up in the NIS Directive and other Union's legislative instruments like eIDAS, GDPR, European Electronic Communication Code etc. The agency will need to anticipate and stand ready to contribute to the development of Union law and policies in the years to come, including by providing expertise and technical input and standing ready to step into and help to fulfil new tasks, should it be called to do so by Union's institutions and Member States.

In September 2018, the European Commission proposed a Regulation setting up a European Cybersecurity Competence Centre and Network[1]. The [draft] Regulation ensures full cooperation and complementarity with ENISA. In particular, ENISA will have an important role in contributing to the Competence Centre's strategic role in coordinating Cybersecurity technology -related investments by the Union, Member States, and industry.

The European Commission has highlighted cybersecurity as one of the crucial policy areas for the next years. On 27 November 2019, during the plenary session in Strasbourg, President von der Leyen presented the views and objectives of the European Commission 2019-2024, noting that[2]:

"/…/ cyber security and digitalisation are two sides of the same coin. This is why cyber security is a top priority. For the competitiveness of European companies we have to have stringent security requirements and a unified European approach. We have to share our knowledge of the dangers. We need a common platform, we need an enhanced European Cybersecurity Agency. That is the only way we can strengthen trust in the connected economy and boost resilience to dangers of all kinds. We can do all this if we act together, if we build on our European values. And by doing so I am confident that Europe will play a leading role in the digital age. Europe can do it!"

[Paragraph about the technical challenges to be added, in next version, after the Threat Landscape Report 2020 is published]

[1] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018 (COM/2018/630 final).
[2] Ursula von der Leyen President-elect of the European Commission, Speech in the European Parliament Plenary Session, as delivered, available at: https://ec.europa.eu/info/sites/info/files/comm-2019-00612-00-00-en-tra-00_0.pdf , pages 9-10.

SECTION II. MULTI-ANNUAL PROGRAMMING 2021 – 2023

This section reflects the objectives and priorities of the agency for the multiannual planning 2021-2023. The activities of the agency are described in two parts – part I – implementation of core tasks of the agency and part II – the cross cutting activities.

For the core tasks of the agency, as listed in the Cybersecurity Act, a new approach is followed compared with previous work programmes. For each of the Articles 5 - 12, multiannual objectives are listed together with expected results/added value for ENISA contributions.

For the cross cutting activities of the agency, an approach in line with previous years is followed, where priorities and the expected added value of the Agency's work in achieving these priorities are presented.

[The future ENISA strategy will give input to both parts of the multiannual section of the SPD 2021-2023, to provide detailed descriptions, priorities as well as targets and indicators]

Annual outputs for WP2021 derive from the tasks of the CSA, and are listed in the order of the articles and multiannual objectives and are presented in Section III.

2.1.IMPLEMENTATION OF CORE TASKS OF THE CYBERSECURITY ACT

Multiannual strategic objectives are identified and associated to the core tasks of the agency defined in Article 5 to Article 12 in CSA. For each of the strategic objectives, ENISA has identified the added value / expected results and KPIs.

The allocation of human and financial resources is made at the level of CSA articles and are presented in Section III and in the annexes.

The following table summarizes the multiannual planning for the core tasks of the agency.

Multiannual planning 2021-2023, core tasks. Tentative[3] (*) objectives, link to CSA article, expected results and KPIs

Multiannual Objective	CSA Art.	Expected results / added value	KPI
Assist in the development of EU Policy (existing and new)	Article 5	Policy makers make use of agency's outputs. Common level of cybersecurity across Union & MS	Degree of acceptance of contributions etc citations, references Uptake of agency's recommendations
Support the development and implementation of EU law (EECC, NISD, eIDAS, GDPR) and build synergies with other relevant policy initiatives	Article 5	Improved common EU framework and coherent implementation of relevant regulatory provisions	Uptake of agency's recommendations and good practices. Measure stakeholders satisfaction of agency's services delivered
Assist EU MS and private sector in developing knowledge and capacities for cybersecurity (e.g. vulnerability, CSIRTs, PSIRTs, ISACS, Cyber Exercises, Trainings, NCSS)	Article 6	Achieve a common level of maturity among MS. Contribute to a more secure EU	Uptake and implementation of agency's recommendations and good practices Measure stakeholders satisfaction of agency's services delivered
Assist MS and EU institutions and bodies, in cyber crises cooperation at technical, tactical and strategic levels (Blueprint, Cyber Europe, CSIRTs Network)	Article 7	Advance & improve operational cooperation to respond to EU cyber crises and incidents. Improve information sharing across operational communities. Contribute to a more secure EU	Structured information sharing taking account of the needs of each community. Faster response and cooperation against incidents and attacks Uptake of agency's recommendations and good practices Usage of agency's infrastructure and expertise
Support the preparation and promotion of cybersecurity certification schemes.	Article 8	Improvement of cybersecurity of products, services and processes developed and deployed in the internal market. Common understanding across EU MS	Number of candidate schemes delivered in relation to number of requests.
Perform market analysis in the area of cybersecurity and cybersecurity certification	Article 8	Better understanding of the internal market as regards cybersecurity in order to further foster its development	Uptake and use of analysis recommendations Measure stakeholders satisfaction of agency's services delivered
Perform analyses and develop good practices on emerging technologies	Article 9	Better understanding of emerging threats and risks. Faster response to threats and faster policy development	Uptake of recommendations Timely adoption of measure to address emerging security challenges based on agency's outputs
Raise public awareness of cybersecurity risks, cyber-hygiene and cyber-literacy	Article 10	Behaviour and use of cyber security practices by the public, raised to a mature common level.	Survey of cybersecurity practices (EU barometer) across EU
Assist MS and EC in identifying major R&D priorities	Article 11	Early identification of security challenges in order to have a quicker response to emerging risks and cyber threats.	Uptake of recommendation by the EU Competence Centres and R&D community
Assist MS and EC in international cooperation priorities of the Union	Article 12	Foster EU cybersecurity values and priorities internationally	Instantiations of strategic international partnerships

[3] (*) the multiannual objectives, expected results and KPIs will be updated and re-structured in accordance with the future ENISA strategy as already explained in the 'About this version' Section at the beginning of this file.

2.2. CROSSCUTTING ACTIVITIES. REINFORCING THE AGENCY

[to be reviewed including taking account the agency's cross-cutting values as outlined in the new strategy]

The objectives that are part of the Cross cutting activities are steamed from CSA Article 3 and Article 32 of the Framework financial regulation.

Article 3 of the CSA (paragraph 4), specifies that "*ENISA shall develop its own resources, including technical and human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation.*"

Article 32 of the Framework Financial rules are applicable to ENISA.

2.2.1. Strategic Objective 1 – Agile and knowledge base agency

The Agency's goal is to build an attractive workplace for hiring and retaining talent.

ENISA will invest in people: recruiting the right talent, providing the training and learning that is needed, creating the right organisational structures and providing an optimal work environment.

The Agency will focus on managing and developing talent effectively by stimulating a collaborative working, both internally and externally, and making further improvements to administrative processes, in order to support exploitation of external and internal synergies new and more effectives way of working, to meet the agency's strategic and multiannual objectives.

2.2.2. Strategic Objective 2 – Efficient and effective management of resources and assets

The Agency will continue to strive towards strengthening its management of financial resources and assets (including IT tools and buildings), with the aim of ensuring accuracy and efficiency in its operations and therefore contributing to the transparency and accountability towards its stakeholders.

2.2.3. Strategic Objective 3 – Respect of legal and financial framework. Compliance, risk management and quality

The Agency will seek to meet its obligations targets and commitments stemming from EU regulations, applicable laws and management policies and guidelines.

Multiannual planning 2021-2023, cross cutting activities. Tentative[4] (*) objectives, link to CSA article, expected results and indicators

Multi-Annual Objective	CSA Art.	Expected results / added value	Indicators
Agile and knowledge base agency	3	• Best expertise in house • Motivated staff • Attract, develop, retain talent • Sharing knowledge management • Collaborative ways working • Internal and Institutional Mobility	• Absenteeism • Turn-over rate • % use of collaborative tools • Evaluation of internal/external deliverables/services • Staff survey (measurement of satisfaction) • New initiatives proposed/driven by staff • Mobility rate, and number of secondments and rotations • Training Hours/employee
Efficient and effective management of resources and assets	**3**	• Optimal use of financial and human resources and expected output • Optimal tools and processes to enhance expected outcome • Lean and green organisation • Synergies with other EUIS	• FTE Actual vs planning • Budget vs planning, including reduced budgetary transfers and Q4 de-commitment rates • Progressive reduction of use paper/toners • Progressive reduction of travel carbon footprint • Staff survey • Benchmark with other agencies • Shared services with other EUIS
Respect of legal and financial framework. Compliance, risk management and quality	**3 & 32 (FFR)**	• Accountability and respect for public funds	• Entries in the Register of Exceptions • Compliance with Internal Audit Recommendations • Observations from European Court of Auditors • [Quality control on delivery of core tasks KPIs] • Number of improvement identified ex-ante and ex post levels

2.3.MONITORING THE PROGRESS AND THE ACHIEVEMENTS OF THE AGENCY

The Agency developed in the past key indicators to provide the metrics to measure against performance, results and impact of the Agency's outcome, output and impact. While tentative aimed results, added value and performance indicators are indicated in this section, the final presentation will be provided in a later version. A revised methodology regarding Key Performance Indicators (KPIs), and Key Impact Indicators (KII) will be provided in the future version of SPD2021-2023.

2.4.HUMAN AND FINANCIAL RESOURCE OUTLOOK FOR THE YEARS 2021-2023

Annex 1 provides the outlook of resources and budget allocation for 2021, while an allocation of human and financial resources is already tabled in section III for the purpose of WP2021.

[4] (*) the multiannual objectives, expected results and KPIs will be updated and re-structured in accordance with the future ENISA strategy as already explained in the 'About this version' Section at the beginning of this file.

SECTION III. WORK PROGRAMME YEAR 2021

The Work Programme for the year 2021 follows the lay out presented in the multi-annual programming Section II, where the activities are described in two parts:

- the implementation of the core tasks of the agency and
- the cross cutting activities.

For the first part, where the implementation of core tasks is described, the outputs are presented in the order of the CSA articles 5 – 12, in a form of table. Several Outputs are identified that might cover activities in more than one CSA article. Each output is described by one or more deliverables. The deliverables have associated KPIs [to be added]. Where a particular area covers more than one article in CSA, the outputs planned are listed usually under the first article that is covered and information is added not mark the link to other article(s).

The indication for the human and financial resources is also done at the level of the article, the first one covering aspects of the specific area/output.

As already mentioned in the document, the presentation of the WP21 outputs is subject to revision once the new ENISA strategy is adopted. As such in the future versions, the outputs might be clustered in another way, to be align with the future strategy.

The second part, with the cross cutting activities, is still to be added. This part is subject to revision when the new strategy becomes available.

3.1. DELIVERING CORE TASKS OF THE CYBERSECURITY ACT

3.1.1. Work Programme 2021 outputs

This part of the Work programme 2021 is described as Outputs linked to the strategic outputs defined by ENISA building on the tasks described in the CSA. As already presented, one or more strategic objectives are associated with each CSA article describing ENISA tasks (Articles 5-12). For each article/ strategic objective, in a form of a table, one or more outputs are identified.

Each Output is described by one or more deliverables. The type of deliverable can be publication /paper /report (P), organisation of an event or workshop (E), or a support (S) activity. In the following table the associated KPIs for each output are introduced and in the second part of the section the Outputs are described.

Work programme 2021. Tentative list of Outputs and Deliverables, Type (P – publication, S – support, E – Event) and associated resources in the order of the CSA tasks[5] (*)

Output No.	Art. in CSA	Multiannual Objective	Name of Output	Deliverables	Type	Link to CSA	KPI 2021	Multi-Annual Goal (3 Years)
1	5	Assist in the development of EU Policy (existing and new)	Providing assistance on policy development	Opinion papers and support activities, ENISA Threat Landscape and Thematic Threat Landscape reports, Support the EC and MS in policy initiatives concerning emerging technologies cybersecurity.	P, S	Art 5 (1), Art 5 (2), Art 6 (1) (a), Art 6 (1) (c), Art 7 (6), Art 8 (3), Art 8 (5), Art 8 (7), Art 9, Art 9c), Art 10 (a), Art 11 (a), Art 11 c)	(a) CTI Maturity Framework defined and agreed by core stakeholders (b) Classification of threats defined and agreed by core stakeholders	(a) CTI maturity framework adopted and used by key stakeholders (b) Threat classification adopted and used by key stakeholders
2	5	Support the development and implementation of EECC, NISD, eIDAS, GDPR and build synergies with other relevant policy initiatives	Supporting and learning from key implementation measures	Support the NISCG by: (a) assessing the implementation of the NISD security requirements, (b) specific knowledge building sessions, (c) creation of work streams for all sectors. Reports on the implementation of Union policy on electronic identity and trust services, support for MS and Trust services forum. Annual Incident Reports, Good practice guides for NIS sectoral incident response expertise, workshops. Provision of reports on implementation mechanisms of cybersecurity aspects of data protection, support for EDPB and Technical Committees, Annual Privacy Forum	P, S, E	Art 5	(a) Evidence that the ENISA is asked to support high majority of the CG WS. (b) Feedback from the Cooperation group on a case-by-case basis on ENISA's support (survey and/or evaluation forms) (c) Majority of MS sharing information on incidents providing input to the Annual reports	(a) ENISA recognised as a key supporting mechanism for the CG as evidenced by annual KPIs. (b) Effective and efficient mechanisms for involving ENISA including criteria for success.
3	5	Support the development and implementation of EECC, NISD, eIDAS, GDPR and build synergies with other relevant policy initiatives	Telecom Security and activities related to EECC/5G	Support for implementation of the 5G toolbox practices and for implementation of the ECCC	P, S	Art 5	(a) Agreement on role and responsibilities of ENISA (b) Number of successful implementations of toolbox activities involving ENISA (c) Feedback of MS via survey	(a) Approach to 5G integrated into the global approach to telecommunications security (b) Key 5G issues identified and mitigating initiatives underway
4	5	Support the development and implementation of EECC, NISD, eIDAS, GDPR and build synergies with other relevant policy initiatives	Vulnerability disclosure policies	Guidelines on vulnerability disclosure policies	P	Art 5 (2) (3), Art 6 (1) (a) (j) and (2) (a)	(a) Policies agreed and accepted by the relevant communities	(a) Feedback from communities that policies are improving disclosure.
5	6	Assist EU MS and private sector in developing knowledge and capacities for cybersecurity (e.g. vulnerability, CSIRTs, PSIRTs, ISACS, Cyber Exercises, Trainings, NCSS)	NISD Capacity Building	Support MS in developing NCSS, Good practice guides on the implementation and evaluation of NCSS. Good practice guide(s) for cybersecurity, knowledge building and supporting activities for a sectorial approach to NISD. Facilitation of NISD Sectoral ISAC and general support activities	P, S, E	Art 5, Art 6, (art4.2), art6, art. 9	(a) Clear capacity building objectives agreed for NISD sectors (b) Modified guidelines on NCSS showing evolution (i.e. influenced by the NISD) (c) Support existing sectorial ISAC activities and with the assistance of the Facilities Manager to develop ISACs in at least two new sectors.	(a) NISD implementation 'drilled down' to the sectorial level with defined plans and follow-up mechanisms. (b) NCSS that reflect the sectorial approach in a consistent manner (c) To setup an effective toolbox/platform for EU sectorial ISACs with the Facilities Manager and to achieve a smooth transition to ENISA

[5] (*) The order of the outputs, their names, the description of deliverables and associated KPIs will be updated based on the future ENISA strategy as already explained in the 'About this version' Section at the beginning of this file.

Output No.	Art. in CSA	Multiannual Objective	Name of Output	Deliverables	Type	Link to CSA	KPI 2021	Multi-Annual Goal (3 Years)
6	6	Assist EU MS and private sector in developing knowledge and capacities for cybersecurity (e.g. vulnerability, CSIRTs, PSIRTs, ISACS, Cyber Exercises, Trainings, NCSS)	Capacity building and CSIRT related activities	CSIRT capacity building: a) Further develop training offering and support, b) deliver operational training, c) CSIRT status reports, d) Carry out evaluations. Reports workshops and community building activities. CSIRT LEA report on aspects of cooperation	P, E, S	Art 6 (1) (a), Art 7 (2) and MoU EC3	(a) Training approach and multi-annual plan agreed. (b) 2021 trainings delivered on time and in budget. (c) Evaluations for trainings show a clear benefit and explain how the training improves operational effectiveness. (a) Tailored knowledge in incident response for NISD sector	(a) Improved CSIRT capabilities as demonstrated by a set of evaluations over 2021 to 2023. (a) Established basic to advanced level of expertise in incident response for all NISD sectors
7	6	Assist EU MS and private sector in developing knowledge and capacities for cybersecurity (e.g. vulnerability, CSIRTs, PSIRTs, ISACS, Cyber Exercises, Trainings, NCSS)	Supporting and planning Cyber Exercises	Planning and supporting activities for Cyber Exercises	P, E, S	Art 6, Art 7, Art 12	(a) Feedback from MS on Cybersecurity Exercise confirms that objectives were met	(a) Cybersecurity Exercises are an integrated component of the blueprint (b) Other exercises are subject to organised request mechanism and support NIS strategic goals
8	7	Assist MS and EU institutions and bodies, in cyber crises cooperation at technical, tactical and strategic levels (Blueprint, Cyber Europe, CSIRTs Network)	CSIRTs Network secretariat and tools	Support and tooling for NISD CSIRTs Network Secretariat	P, S, E	Art 6 (2) Art 7 (3) (4) (6) (7) (a) (b) (c) (e), Art 7 (3)	(a) An agreed structured approach to tooling across all N/G CSIRTs (b) Documented feedback from CSIRTs explaining how this will improve operations	(a) An agreed community approach to selecting, operating and decommissioning tools. (b) Evidence that such tools and support result in effective operations.
9	7	Assist MS and EU institutions and bodies, in cyber crises cooperation at technical, tactical and strategic levels (Blueprint, Cyber Europe, CSIRTs Network)	Support activities for EU Cyber Crisis Cooperation Blueprint	Support activities for Cyber Crisis Management in the EU. Situational awareness 24/7 including supporting the implementation of the information hub	S	Art 6, Art 7, Art 9, Art 12	(a) SOPs agreed at the community level (CSIRTs, Agencies, MS) (b) Roadmap defined for integrating these SOPs	(a) All communities use a rationalised set of SOPs, that achieve the common goal whilst recognising the needs of each individual community.
10	7	Assist MS and EU institutions and bodies, in cyber crises cooperation at technical, tactical and strategic levels (Blueprint, Cyber Europe, CSIRTs Network)	Support operational cooperation within CSIRTs Network and with LEA	NISD CSIRTs Network exercises, comchecks and maturity assessment. Liaison with the EU agencies on operational issues related to CERT-EU's activities	P, S	Art 7 (3) (6) (7) (a) (b) (c), Art 7 (3) (5) (6) (7) (e), Art 6 (1) (d) (g) (2), Art 7 3 and 4 (a)	(a) Documented comchecks showing both successful and unsuccessful aspects. (b) Improvement plans based on the comchecks results	(a) Clear processes for running and responding to comchecks (b) Strong working relationships between the CSIRTs and the EU Agencies, demonstrated by successful initiatives.
11	8	Support the preparation and promotion of cybersecurity certification schemes	Cybersecurity certification related activities	Promulgation of cybersecurity certification schemes, Support for ECCG and SCCG, Implementation of website and events	P, E, S	Art 8 (1) (b), Art 8 (1) (e), Art 8 (2), Art 50	(a) Agreed Rolling Work programme (b) Schemes delivered on time and in budget (c) Schemes meet defined success critieria	(a) Agreed multi-annual planning for schemes (RWP) (b) Evidence of stakeholder take-up (by a survey)
12	8	Perform market analysis in the area of cybersecurity and cybersecurity certification	Cybersecurity certification support activities	Analysis of Market aspects of cybersecurity certification, Evaluation of adopted schemes, Capacity building measures and support for peer reviews.	P, S	Art 8 (1) (b), Art 8 (1) (c), Art 8 (1) (d), Art 8 (4)	(a) Methodology defined for carrying out market analysis within the CSA (b) Methodology applied to the case of Cloud Certification	(a) Market analysis is an integrated component of the approach to defining schemes and results in decisions based on the analysis.

Output No.	Art. in CSA	Multiannual Objective	Name of Output	Deliverables	Type	Link to CSA	KPI 2021	Multi-Annual Goal (3 Years)
13	8	Perform market analysis in the area of cybersecurity and cybersecurity certification	Monitoring developments in standardisation	Liaising with SDOs, Report on standardisation landscape and gaps	P, S, E	Art 8 (1) (a), Art 12 (b)	(a) Working practices agreed with key SDOs (b) Report on landscape and drafts agreed with these SDOs	(a) SDOs fully integrated into the CSA certification approach (b) Documented approach to integrating standards development with the certification processes.
14	9	Perform analyses and develop good practices on emerging technologies	Securing Emerging Technologies	Monthly information notes, CTI maturity and best practice. Good practices and reports for the cybersecurity of emerging technologies. Report and workshop on future technology challenges	P, S, E	Art 5 (5) (b), Art 6 c), Art 7 (1), Art 7 (2), Art 9, Art 9c), Art 9 (e), Art 10 (a), Art 10 (b), Art 11	(a) Agreed challenges and high-level approach for securing AI (b) Vision of future challenges (crystal ball) endorsed by representative set of MS	(a) Key stakeholders endorsing and referencing ENISA's good practices for emerging technologies cybersecurity. (b) MS, academia and private sector use the 'crystal ball' approach as a reference (as evidenced by surveys and references)
15	10	Raise public awareness of cybersecurity risks, cyber-hygiene and cyber-literacy	Awareness raising activities	Support for European Cybersecurity Month, NIS Summer School and ECSC	P, E, S	Art.10	(a) Positive feedback from MS on the ECSM (using a survey) (b) Agreed planning for an international cybersecurity challenge (c) Positive feedback from NIS Summer School participants (evaluation forms)	(a) Stronger integration of the ECSM with national approaches for all MS (b) Global approach to cybersecurity challenges (c) Integration of the NIS Summer School in the global approach to awareness raising
16	10	Raise public awareness of cybersecurity risks, cyber-hygiene and cyber-literacy	Cybersecurity skills development	Support EU MS in cybersecurity skills development and provide technical training. Coordinate activities with ECSO WG5, JRC (on Atlas map activities), the 4 pilots projects, and, where possible, all EC Institutions active in cybersecurity skills (e.g. DG GROW).	P, S	Art 6, Art 7, Art 10, Art 11, Art 12	(a) Identified scope and approach clearly delimiting national and EU objectives (b) Mapping of synergies between involved communities	(a) ENISA functioning as part of a community approach to training, where the responsibilities of all actors are clearly defined and synergies are exploited as far as possible.
17	11	Assist MS and EC in identifying major R&D priorities	Supporting EU research & innovation	Supporting EU cybersecurity competency centres and future research & development programmes	S	Art 11	(a) ENISA's role in supporting the CCCs clearly defined and agreed.	(a) ENISA's role in supporting research activities across the EU defined – including the CCCs (b) ENISA providing guidance to publicly funded research initiatives in order to align with EU policy goals.
18	12	Assist MS and EC in international cooperation priorities of the Union	International cooperation	Support the European Commission on international cooperation.	S	Art 12	(a) Scope and responsibilities of ENISA agreed (b) Roadmap for agreeing working practices with relevant institutions (COM, EEAS, MS)	(a) ENISA acting with a well-defined scope and set of responsibilities to support the EU institutions in initiatives involving cybersecurity

Output 1. Providing assistance on policy development

This Output covers the following:

- ENISA will provide independent opinions and analysis to assist in the development and review of Union policy and law in the field of cybersecurity.
- Annual compilation of top 15 cyberthreats including interesting points, statistics, involved threat agents, mitigation and references to related sources providing detailed technical information per assessed threat.
- Threat analysis of assets of a particular sector/application area demonstrating their exposure to cyber threats based on known vulnerabilities.
- Contribute to the development and/or review of ongoing and prospective EU policies on cybersecurity of emerging technologies (including in the field of artificial intelligence) by providing evidence-based support building on ENISA's expertise and relevant studies.

Output 2. Supporting and learning from key implementation measures

This Output covers the following:

- The Agency will assist the MS in assessing the implementation of the Directive by supporting the Cooperation Group work programme activities
- Organise knowledge specific sessions for the Cooperation Group, assisting MS with the implementation of the NISD requirements for OES and DSP and build synergies with other CIIP initiatives.
- ENISA will support the Cooperation Group in updating already existing publications on the implementation of the requirements of the NISD
- Support and participate in sectorial Work Streams providing assistance and knowledge on the relevant outcomes. ENISA will further support the Commission with assessing the implementation and review of the Directive
- Support article 13a Group with incident notification requirements for telcos
- Organise three workshops for the Art.13a experts group in collaboration with relevant stakeholders
- Support article 19 Group with incident notification requirements for e-Trust services.
- Organise two workshops for the Art.19 experts group in collaboration with relevant stakeholders
- Support the NISD Cooperation Group with the incident notification requirements
- Policy recommendation for NIS sectoral incident response expertise
- A report elaborating on the new CSA tasks concerning electronic identity
- Examine and recommend technical guidelines implementing the eIDAS Regulation in the non-mandatory articles, for voluntary use of all stakeholders, including Trust Service Providers, Supervisory Bodies and Conformity Assessment Bodies
- Analysis and recommendations on Trust services in place
- Organize a workshop to engage stakeholders and validate ENISA's work in the area of eIDAS
- Analyse and provide recommendations on promote technical and cybersecurity aspects of personal data protection
- Support, upon request, the European Data Protection Board (EDPB) in cybersecurity aspects of privacy and data protection through technical independent expertise and opinions
- Analyse and provide support on practical implementation of technical and cybersecurity aspects relating to privacy
- Organize a workshop to engage stakeholders and validate ENISA's work in the areas of privacy and personal data protection
- Organize the Annual Privacy Forum (APF) to promote and enhance research and policy development in the areas of privacy and data protection

Output 3. Telecom Security and activities related to EECC/5G

This Output covers the following:

- Assist the NISD Cooperation Group with the implementation of the 5G Toolbox
- Develop good practices and recommendations required for the implementation of the Telecom Security policy

Output 4. Vulnerability disclosure policies

This Output covers the following:

- Support Member States and Union institutions, bodies, offices and agencies in developing and implementing guidelines regarding vulnerability disclosure policies on a voluntary basis.

Output 5. NISD Capacity Building

This Output covers the following:

- Maintain and update the online EU NCSS map
- Organise the 8th NCSS workshop
- Support MS in developing, implementing and evaluating their national cybersecurity strategy. ENISA in this way contributes in the capability maturity assessment of the EU MS.
- Assisting industry and MS in developing and implementing Union policies related to cybersecurity in critical sectors
- Assist the Commission and the MS in building synergies between the NIS Directive and other CIIP initiatives or policy implementation
- Enhance cybersecurity knowledge and expertise in critical sectors through conferences, workshops and dedicated trainings
- Organise sector specific knowledge building sessions, enhancing cybersecurity in the critical sectors
- Facilitate information sharing between operators of critical sectors and creation of collaboration platforms
- Cooperate with the EC in assisting the ISAC facilities manager in its tasks under the CEF project
- Organise conferences, workshops, meetings and knowledge building sessions dedicated to sectorial ISACs. Bring sectorial ISACs together and identify synergies.

Output 6. Capacity building and CSIRT related activities

This Output covers the following:

- Develop new training materials for sectors in the NISD with a focus on operational techniques. Deliver these trainings to MS and EU bodies to support there security capacities and preparedness for incidents.
- Develop and maintain a platform for hosting and delivering technical trainings with an operational focus. This allows MS and EU bodies to enhance their security capacities and capabilities.
- Tailor ENISA CSIRT maturity evaluation framework (including tool) for the NISD sectorial CSIRTs
- Continue activities and involvement in international CSIRT or taskforce initiatives in community fora like FIRST, TF-CSIRT-TI or GFCE.
- Support the offering of trainings regarding cybersecurity, where appropriate in cooperation with stakeholders such as TRANSITs or other organizations.
- Delivery of technical and operational trainings for MS and EU bodies, thus supporting them in developing their capabilities and knowledge.
- Report on capabilities and maturity for various types of CSIRTs, SOCs and PSIRTs

- Status report on incident landscape in NISD sectors. Incident response setup and current capabilities within various NISD sectors
- Report on CSIRTs and LE cooperation. A report on segregation of duties/competence mapping based on the 2019 Roadmap; training material
- Organise the annual ENISA/EC3 workshop for national and governmental CSIRTs and their LEA counterparts
- CSIRT LEA community building. Ad hoc and on demand interactions with MS and EU institutions
- Support for Council of Europe. Planned interactions

Output 7. Supporting and planning Cyber Exercises

This Output covers the following:

- Planning of Cyber Europe and CyberSOPEx. Develop and organize Cyber Europe, exploring new dimensions and formats with the aim of further preparing the Member States and Union institutions to cyber crises likely to occur in the future in the EU.
- Support CE related activities with platforms and tools. Moreover, upon request from external entities (e.g. EU Institutions and Agencies, National Authorities, other organisations) support the organisation of exercises.

Output 8. CSIRTs Network secretariat and tools

This Output covers the following:

- Ensuring the well-functioning of the CSIRTs Network IT infrastructure, tools and communication channels
- Supporting the operational cooperation as secretariat of the CSIRTs Network (as per NIS Directive provisions) and support the fulfilment of the CSIRTs Network Work Programme for 2017-2022

Output 9. Support activities for EU Cyber Crisis Cooperation Blueprint

This Output covers the following:

- Support activities for Cyber Crisis Management in the EU. Integrate existing and future EU-wide crisis management orientations, mechanisms, procedures and tools within the already existing crisis management framework of the EUIs;
- Contribute actively to the implementation of the blueprint by supporting MS in integrating into national crisis management frameworks EU-level orientations, mechanisms, procedures and tools.
- Develop, improve and build a community around the Open Cyber Situational Awareness Machine
- Develop an Operational Capacity for ENISA that will allow the continuous monitoring for cyber threats, the assessment, the estimation of risk and impact and the produce of mitigation measures and advise

Output 10. Support operational cooperation within CSIRTs Network and with LEA

This Output covers the following:

- Facilitate incident response coordination, operation and information exchange with the best tools and expertise
- Support the growth of the CSIRTs Network members by periodically assessing their maturity and provide dedicated tools and knowledge to advance their capabilities.
- Enable the highest level of incident response coordination and support to the incident data sharing among CSIRTs Network members by providing dedicated expertise and the best tools and support.

- Representation of the EU Decentralised Agencies on the Steering Board of CERT-EU. Cooperation with relevant EU Agencies on initiatives covering NIS dimension for example on capacity building support for trainings, awareness & education.

Output 11. Cybersecurity certification related activities

This Output covers the following:

- Prepare candidate European cybersecurity certification schemes
- Support the EC in carrying out formal roles
- Organise a conference to promote the deployment, uptake and further development of the framework
- Provide information on and publicising European cybersecurity certification schemes

Output 12. Cybersecurity certification support activities

This Output covers the following:

- Analyse main trends in the cybersecurity market on both the demand and supply sides
- Evaluate previously adopted schemes
- Guidelines for the uptake of certification schemes
- Support peer reviews of NCCAs on the basis of sound and transparent evaluation criteria and procedures

Output 13. Monitoring developments in standardisation

This Output covers the following:

- Ongoing and on demand requests (ETSI security week, coordination meetings etc.)
- A conference on standards and certification
- Follow up on strategy with ESO, SDO and private standardisation organisations
- A report on standardisation gaps in relation to certification

Output 14. Securing Emerging Technologies

This Output covers the following:

- Analyse and report on trends observed in threats, actors, tools, techniques and procedures used in major cybersecurity incidents.
- Support the community of cybersecurity experts in the development of good practices, tools and methodologies in cyber threat intelligence.
- Develop and when relevant update good practices and recommendations to promote the secure development and deployment of emerging technologies, e.g. Artificial Intelligence (AI), Connected and Automated Mobility (CAM) and Internet of Things (IoT).
- Mobilise the community of experts, practitioners and researchers to discuss developments in Cyber Threat Intelligence and learn about current CTI offerings, requirements, use cases, tools and practices.
- Support, upon request, MS in the update of relevant good practices and recommendations to promote the secure development and deployment of emerging technologies.
- Organise annual conference on cybersecurity of emerging technologies to promote awareness and support community engagement. Organise validation workshop for relevant ENISA studies with the involvement of subject matter experts.
- Biannual report on "Secure practices in using Cryptographic Algorithms and Protocols" including good practices and recommendations. e-learning module on an "Introduction to Cryptography".

- A report providing a multidimensional analysis over the trends and patterns with challenges and threats from the adoption of and adaptation to future emerging technologies.
- Mobilise experts in the field of technology, industry, economy, sociology and others to discuss future challenges in the Security of the Cyberspace.

Output 15. Awareness raising activities

This Output covers the following:

- Organization of annual workshop for the exchange of awareness raising best practices and to define and plan the campaign ahead
- Annual report that describes the planning, execution and evaluation of the campaign and provide recommendations
- Managing and executing the campaign. Coordinating outreach with MS to maximize effectiveness.
- A one-week training event with the main purpose of raising public awareness on cybersecurity risks, cyber-hygiene and cyber-literacy.
- European Cyber Security Challenges. Organize the European Cybersecurity Challenge (ECSC) with a view to making these events a venue for EU cybersecurity awareness raising"
- International Cyber Security Challenge. Organize the International Cybersecurity Challenge (ICSC) with a view to making these events a venue for EU cybersecurity awareness raising

Output 16. Cybersecurity skills development

This Output covers the following:

- Continue ENISA's support in raising awareness in NIS among youngsters and future cyber security experts in the EU MS by supporting the organisation of new national CTF competitions,
- Develop training material in Information security Management

Output 17. Supporting EU research & innovation

This Output covers the following:

- Support the CPP in developing common European Cybersecurity Research & Innovation Roadmap
- Support the creation of an European Cybersecurity Research and Competence Centre and engage the 4 pilots in order to find synergies with the activities done by ENISA or by other European stakeholders in the field of cybersecurity

Output 18. International cooperation

This Output covers the following:

- At the request from the European Commission, ENISA will contribute to Union effort to promote international cooperation on issues related to cybersecurity.

3.1.2. Allocation of financial and human resources for the core tasks

The tentative allocation of financial and human resources for the core tasks is presented in the table below.

Tentative allocation of resources per CSA core tasks, in the work programme 2021[6] (*)

Allocation of human and financial resources per CSA core tasks articles in WP21	Budget allocated (euro)	No. of posts allocated	% of budget /core tasks	% posts/ core tasks
Art 5	1.300.000,00	21,50	21%	27%
Art 6	1.290.000,00	18,75	21%	24%
Art 7	535.000,00	11,50	9%	15%
Art 8	1.381.471,40	12,75	23%	16%
Art 9	435.000,00	5,25	*7%*	*7%*
Art 10	905.000,00	5,75	*15%*	*7%*
Art 11	165.000,00	2,00	*3%*	*3%*
Art 12	100.000,00	1,00	*2%*	*1%*
Sub-total Art 9-12	1.605.000,00	14,00	26%	18%
Total	**6.111.471,40**	**78,50**	**100%**	**100%**

3.2. DELIVERING CROSS CUTTING ACTIVITIES

[As one of the first use of the strategy is to help to develop a new organisational structure, this section will be reviewed after the reorganisation is agreed and decided. As such, in below, limited reference is made to the agency's internal structure.]

This section refers to internal management cross-cutting issues, carried out to support operational activities and staff.

Multiannual planning 2021-2023, cross cutting activities. Tentative[7] (*) objectives, link to CSA article, expected results and indicators

Multi-Annual Objective	Indicators for 2021
Agile and knowledge base agency	• Absenteeism • Turn-over rate • % use of collaborative tools • Evaluation of internal/external deliverables/services • Staff survey (measurement of satisfaction) • New initiatives proposed/driven by staff • Mobility rate, secondments and agreed rotations • Training Hours/employee
Efficient and effective management of resources and assets	• FTE Actual vs planning • Budget vs planning (including reduction of budgetary transfers and Q4 de-commitments) • Progressive reduction of use paper/toners • Progressive reduction of travel carbon footprint • Staff survey • Benchmark with other agencies • Shared services with other EUIS
Respect of legal and financial framework. Compliance, risk management and quality	• Entries in the Register of Exceptions • Compliance with Internal Audit Recommendations • Observations from European Court of Auditors • [Quality control on delivery of core tasks KPIs] • Number of improvement identified ex-ante and ex post levels

[6] (*) The table lists the CSA articles. As the articles 9-12 in total share less resources, they are presented together, in one line.
[7] (*) the multiannual objectives, expected results and KPIs will be updated and re-structured in accordance with the future ENISA strategy as already explained in the 'About this version' Section at the beginning of this file.

3.2.1. Activities carried out to address the cross-cutting objectives

3.2.1.1. Management

The Executive Director is responsible for the overall management of the Agency.

In 2021, the Management Board Secretariat will continue to support the Management Board and the Executive Board in their functions by providing secretariat assistance. It includes, but is not limited to the support for meetings and correspondence that takes place between meetings, the management of annual declarations of interest and of commitment and other requirements.

In relation to the MB, two ordinary meetings will be organised during 2021 and informal meetings will be held as necessary. The MB Portal will be supported for the MB. In relation to the Executive Board, one formal meeting will be organised per quarter and informal meetings, when necessary.

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

Furthermore the Agency engages and further develops strategic relationships with e.g. specific industry sectors at decision making level, and identifies the strategic issues on cybersecurity. The Agency will also be in a position to support various institutions and bodies in respect of policy initiatives related to cybersecurity.

Planning activities of the Agency, including Single Programming Document preparation and Work Programme coordination are part of the cross cutting tasks.

The Public Affairs activities are carried out, including coordinating all communication activities, media and press activities, such as press releases, news items and interviews to enhance the reputation, visibility and image of the Agency. It supports the entire Agency with regards to publications, social media promotion, website management, public affairs activities and awareness campaigns.

3.2.1.2. Internal control

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

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

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

3.2.1.3. IT activities

Provided Athens building readiness, by the end of 2021 it is expected that the Agency has two new fully operating datacentres, one in Heraklion Crete and its highly available equivalent in Athens, prepared with cutting-edge hyper convergence technology. The Agency will also establish a Disaster Recovery site, in partnership with another EU Agency. This will enhance IT service availability in case of Disaster; rendering the Agency prepared for any challenges that may arise.

IT will reinforce the Agency's infrastructure in three pillars, namely in network, system and application readiness. It will proceed to major upgrades of all core IT platforms like Exchange 2016 and SharePoint 2019 and will provide a solution for skype for business, which is reaching end of support.

It will enhance the monitoring and performance capacity of the Agency's infrastructure by establishing system monitoring and network monitoring with thresholds and indicators for prompt detection and remediation of any related problems. This includes a monitoring capacity for the actual environmental conditions of the datacentres.

Following up the assessment of information security risks and IT operational procedures, ENISA will be putting in place and updating policies and procedures to mitigate any risks identified. Among the scope is end user computing, IT assets lifecycle, SharePoint governance and change management.

For 2021 and following up on the actions of 2020, the Agency will be investing heavily in the strengthening of its capabilities in the areas so information security and cybersecurity to continue its policy of having the best security posture possible. For the purpose, a plan of perfective maintenance will be undertaken for the on premise IT platforms in cooperation with the ISO.

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

MeliCERTes. In 2021 ENISA will continue running the central node of MeliCERTes and its local debug instance. MeliCERTes will be the primary collaboration platform between participating Member States CSIRTs facilitating improvement of EU MS preparedness, cooperation and coordination, in order to better respond to emerging cyber threats as well as to cross-border incidents.

The MeliCERTes project will run in close cooperation with the EC and the MS. The EC will have a new contract for several of the areas encompassed in the project for the short term future. The long term sustainability and development of this project will need to be analysed in collaboration is all stakeholders involved.

ENISA will investigate the technical landscape for the PKI services, currently provided by DFN CERT and the onboarding and sustainability of Member States in the platform along with change management requests that fall within the remit of Central Node or Helpdesk; like capacity augmentation in the case of extra CEF end nodes.

3.2.1.4. Finance and Procurement

The Agency plans to upgrade its internally developed electronic tools used for Procurement in order to simplify and further automate its tasks related to tendering and contracting. This is deemed necessary due to the expected increase in the volume of work based on a significantly increased operational budget.

It is anticipated that further development of the in-house systems should be outsourced. The aim is to optimize 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 training to assure 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 the best practices in the EU agencies in this regard).

3.2.1.5. Human Resources

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

deliver a successful day-to-day management of ENISA statutory staff and external staff (e.g. trainees) in compliance with the Staff Regulations/CEOS. Additionally, investment and efforts are focusing on several projects such as the acquisition of an E-Recruitment tool, the development in closed collaboration with the European Commission's services of SYSPER, adoption of Missions electronic tool used by the EC (MIPS).

3.2.1.6. Legal Affairs

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

3.2.1.7. Data Protection Compliance tasks and Data protection Office

The main tasks of the Data Protection Officer (DPO) are defined in Regulation (EU) 2018/1725, and include the following:

- Inform and advise ENISA pursuant to Regulation (EU) 2018/1725 and to other Union data protection provisions;
- Ensure in an independent manner the internal application of Regulation (EU) 2018/1725; monitor compliance with this Regulation, with other applicable Union law containing data protection provisions and with the policies of ENISA in relation to the protection of personal data, including the assignment of responsibilities, the raising of awareness and training of staff involved in processing operations, and the related audits;
- Ensure that data subjects are informed of their rights and obligations pursuant to Regulation (EU) 2018/1725;
- Provide advice where requested as regards the necessity for a notification or a communication of a personal data breach pursuant to Articles 34 and 35 Regulation (EU) 2018/1725;
- Provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 39 Regulation (EU) 2018/1725 and consult the European Data Protection Supervisor in case of doubt as to the need for a data protection impact assessment;
- Provide advice where requested as regards the need for prior consultation of the European Data Protection Supervisor pursuant to Article 40 Regulation (EU) 2018/1725; consult the European Data Protection Supervisor in case of doubt as to the need for a prior consultation;
- Respond to requests from the European Data Protection Supervisor; within the sphere of his or her competence, cooperate and consult with the European Data Protection Supervisor at the latter's request or on his or her own initiative;
- Ensure that the rights and freedoms of data subjects are not adversely affected by processing operations.

ENISA MB Decision 2019-2 provides further implementing rules regarding the tasks, duties and powers of the DPO in accordance with Articles 43, 44 and 45 of Regulation (EU) 2018/1725.

The DPO refers directly to the ENISA Executive Director.

3.2.1.8. Information Security coordination

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

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

3.2.1.9. Stakeholders communication and dissemination activities

In 2021, ENISA will continue its efforts to improve its focus on key activities and engage the higher possible number of stakeholders. This includes the statutory stakeholders and the various groups of stakeholders that count with institutional, academia, industry, citizens, media, etc. The Public Affairs team will play a major role in bringing visibility to events attended by ENISA management team and staff members, inter alia in its engagement with the stakeholders, the Agency is guided by principles as balanced representation, openness, trust, transparency, and inclusiveness.

ENISA Public Affairs Team will use the following KPIs to measure the success of its traditional communication with stakeholders:

3.2.1.10. Dissemination and Outreach

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

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

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

3.2.1.11. Internal communications

Internal communications strategy and activities are of utmost importance in order to:

- To ensure that everyone in the Agency is well-informed and engaged (to stay connected)
- To increase the cohesive functioning of the organisation (to bring in unison)
- To voice opinions (two-way dialogue), to collaborate for idea generation and problem solving, to share knowledge and best practices
- To support organisational changes and to shape ENISA working culture
- To understand better the Agency's vision, values, goals and achievements

3.2.1.12. ENISA Advisory Group

In 2021, ENISA will continue to support the ENISA Advisory Group and will aim to support the contribution of the group to the ENISA Work Programme.

The Advisory Group is composed of recognised experts representing relevant stakeholders, such as the ICT industry, consumer groups, academic experts in the field of cybersecurity, representatives of competent authorities notified in accordance with Directive (EU) 2018/1972 (European Electronic Communications Code) i.e. BEREC, as well as representatives of European standardisation organisations, 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 term of office of 2.5 years.

The Role of the Advisory Group is to advise ENISA in respect of the performance of ENISA's tasks, excluding Title III of the Cybersecurity Act, which concerns the Cybersecurity Certification Framework. It shall advise the Executive Director on the drawing up 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.

3.2.1.13. National Liaison Officer Network

Pursuant to Article 23 of the Cybersecurity Act, the National Liaison Officers Network (NLO) facilitate cooperation between ENISA and national experts in the context of the implementation of ENISA's annual work programme. For this purpose, two NLO meetings will be organised by ENISA, in Q1 2021 and Q3 2021.

In 2021, the NLO network will continue to receive information about upcoming ENISA project related tenders, news, vacancy notices, and events organised by ENISA or where the Agency contributes to (for example as a co-organiser, etc.) as well as time-critical information.

Annexes

A.1. ANNEX I: RESOURCE ALLOCATION PER ACTIVITY 2020 – 2023

Next sections of this Annex presents the evolution of past and current situation, as well as the distribution of resources and budget for the activities of the WP2021.

Resource programming for the years 2021-2023

The distribution of the total 2021 budget and resources following the core tasks as described in section 3.1.3 and the cross cutting activities as described in section 3.2. are presented in the table below:

Allocation of human and financial resources	Full budget allocation (in EUR)	Full FTE allocation
Article 5 - Policy/law development & implementation	4.865.489,00	24,55
Article 6 - Capacity-building	4.412.254,72	21,46
Article 7 - Operational cooperation	2.428.971,61	13,08
Article 8 - Market, certification	3.545.960,55	14,74
Articles 9 - Knowledge & information, 10 - Awareness-raising & education, 11 - Research & innovation, and 12 - International cooperation	3.988.918,35	16,22
Cross cutting activities	4.191.481,77	27,95
TOTAL	**23.433.076,00**	**118,00**

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 agency’s reorganisation in 2020 should ensure not only a gradual increase of the share of staff allocated for operational functions, but also a clear match btw the function and structures (eg staff performing administrative functions should not be allocated into structural units dedicated to the delivery of operational tasks) The table below reflects the situation at ENISA:

Type	2016	2017	2018	2019	2020	2021	2022
Total Administrative support and Coordination	**19,04%**	**19,27%**	**22,89%**	**18,37%**	**17,54%**	**17,54%**	**17,54%**
Administrative Support	15,47%	15,66%	19,28%	15,30%	14,91%	14,91%	14,91%
Coordination	3,57%	3,61%	3,61%	3,07%	2,63%	2,63%	2,63%
Total Operational	**66,66%**	**66,27%**	**62,65%**	**69,39%**	**69,30%**	**69,30%**	**69,30%**
Top Operational Coordination	7,14%	7,23%	7,23%	5,10%	4,39%	4,39%	4,39%
General Operational	59,52%	59,04%	55,42%	64,29%	64,91%	64,91%	64,91%
Total Neutral	**14,29%**	**14,46%**	**14,46%**	**12,24%**	**13,16%**	**13,16%**	**13,16%**
Finance and Control	14,29%	14,46%	14,46%	12,24%	13,16%	13,16%	13,16%

A.2. ANNEX II: HUMAN AND FINANCIAL RESOURCES 2021-2023

Table 1. Expenditure overview, in EUR

EXPENDITURE	2020		2021	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1	12.041.486	12.041.486	12.655.000	12.655.000
Title 2	2.986.000	2.986.000	3.374.971	3.374.971
Title 3	6.761.633	6.761.633	7.403.105	7.403.105
Total expenditure	**21.789.120**	**21.789.120**	**23.433.076**	**23.433.076**

Commitment and payment appropriations, in EUR

EXPENDITURE	Executed budget 2019	Budget 2020	Draft Budget 2021 Agency request	VAR 2021 / 2020	Envisaged in 2022	Envisaged in 2023
Title 1. Staff Expenditure	**7.458.310**	**12.041.486**	**12.655.000**	**5%**	**13.833.952**	**13.833.952**
11 Staff in active employment	5.627.276	10.181.000	8.684.182	-15%	10.730.045	10.730.045
12 Recruitment expenditure	254.762	445.000	407.952	-8%	252.676	252.676
13 Socio-medical services and training	222.200	250.000	1.023.944	310%	1.021.648	1.021.648
14 Temporary assistance	1.354.073	1.165.486	1.338.922	15%	611.165	611.165
15 Missions	0	0	1.200.000		1.218.418	1.218.418
Title 2. Building, equipment and miscellaneous expenditure	**4.346.742**	**2.986.000**	**3.374.971**	**13%**	**3.306.324**	**3.306.324**
20 Building and associated costs	783.366	1.180.000	2.056.500	74%	1.234.000	1.234.000
21 Movable property and associated costs	45.391	99.000	147.000	48%	99.000	99.000
22 Current administrative expenditure	81.829	176.000	175.000	-1%	302.324	302.324
23 ICT	3.436.156	1.531.000	996.471	-35%	1.671.000	1.671.000
Title 3. Operational expenditure	**4.402.318**	**6.761.633**	**7.403.105**	**9%**	**7.086.788**	**7.086.788**
30 Activities related to meetings and missions	910.929	1.410.000	440.000	-69%	548.509	548.509
32 Horizontal operational activities	524.689	1.001.633	851.633	-15%	1.023.053	1.023.053
36/37 Core operational activities	2.966.700	4.350.000	6.111.471	40%	5.515.226	5.515.226
TOTAL EXPENDITURE	**16.207.370**	**21.789.120**	**23.433.076**	**0**	**24.227.064**	**24.227.064**

Table 2 – Revenue Overview

Revenues	2020	2021	2022	2023
	Revenues estimated by the agency	Revenues estimated by the agency	Revenues estimated by the agency	Revenues estimated by the agency
EU contribution	20.646.000	22.248.000	23.023.000	23.023.000
Other revenue	1.143.120	1.185.076	1.204.064	1.204.064
Total revenues	**21.789.120**	**23.433.076**	**24.227.064**	**24.227.064**

REVENUES	2019 Executed Budget	2020 Revenue estimated by the agency	2021 As requested by the agency	VAR 2021 / 2020	Envisaged 2022	Envisaged 2023
1 REVENUE FROM FEES AND CHARGES						
2. EU CONTRIBUTION	15.400.829	20.646.000	22.248.000	8%	23.023.000	23.023.000
3 THIRD COUNTRIES CONTRIBUTION (incl. EFTA and candidate countries)	370.696	503.120	545.076	8%	564.064	564.064
of which EFTA	370.696	503.120	545.076	8%	564.064	564.064
of which Candidate Countries						
4 OTHER CONTRIBUTIONS	435.844	640.000	640.000	0%	640.000	640.000
of which delegation agreement, ad hoc grants						
5 ADMINISTRATIVE OPERATIONS						
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT						
7 CORRECTION OF BUDGETARY IMBALANCES						
TOTAL REVENUES	**16.207.370**	**21.789.120**	**23.433.076**	**8%**	**24.227.064**	**24.227.064**

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

Budget outturn	2017	2018	2019 (draft)
Revenue actually received (+)	11.223.387	11.572.995	16.740.086
Payments made (-)	-9.901.545	-10.345.736	-11.980.352
Carry-over of appropriations (-)	-1.376.730	-1.348.657	-4.357.734
Cancellation of appropriations carried over (+)	90.916	108.302	62.522
Adjustment for carry over of assigned revenue appropriations carried over (+)	49.519	124.290	116.393
Exchange rage difference (+/-)	-12	-689	-1.802
Adjustment for negative balance from previous year (-)	-		
Total	**85.535**	**110.505**	**579.113**

Cancellation of appropriations (information will be updated after 2019 annual accounts are produced)

- 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 year-end (31/12). The consumption of the 2018 budget at year-end 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 total C1 appropriations 2018.

- Cancellation of Payment Appropriations for the year

No payment appropriations were cancelled during 2018.

- 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 forward, the amount of EUR 108 302,57 was cancelled, due to the fact that the estimated expenditure deviated from the actual paid amount. This cancellation represents 1 % of the total budget.

A.3. ANNEX III: HUMAN RESOURCES – QUANTITATIVE

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

Staff population		Authorised under EU budget for year 2018	Actually filled as of 31.12.2018	Authorised under EUbudget for year 2019	Actually filled as of 31.12.2019	Envisaged in 2020	Envisaged in 2021	Envisaged in 2022	Envisaged in 2023
Officials	AD								
	AST								
	AST/SC								
TA	AD	34	32	43	37	51	57	60	60
	AST	13	12	16	14	18	19	19	19
	AST/SC								
TOTAL		**47**	**43**	**59**	**51**[8]	**69**	**76**	**79**	**79**
CA GFIV		28	16	28	17	28	28	28	28
CA GF III		5	10	2	8	2	2	2	2
CA GF II		0	0	0	0	0	0	0	0
CA GFI		0	1	0	1	0	0	0	0
Total CA		**33**	**27**	**30**	**26**	**30**[9]	**30**	**30**	**30**
SNE		**3**	**3**	**9**	**4**[10]	**12**	**12**	**12**	**12**
Structural service providers									
TOTAL		**83**	**73**	**98**	**81**	**111**	**118**	**121**	**121**
External staff for occasional replacement				5	5	5	5	5	5

8 51 TAs (47 TAs in-house and 4TAs procedures concluded)

9 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.

10 4 SNEs (2 in-house and 2 SNE procedures concluded)

Table 2 – Multi-annual staff policy plan year 2021 – 2023

Category and grade	Establishment plan in voted EU Budget 2019		Modifications in year 2019 in application of flexibility rule		Filled as of 31/12/2019		Establishment plan 2020		Establishment plan 2021		Establishment plan 2022		Establishment plan 2023	
	Off.	TA	Off.	TA	Off.	TA	Off.	TA	Off.	TA	Off.	TA	Off	TA
AD 16														
AD 15		1		1				1				1		1
AD 14						1				1				
AD 13				2						1		2		2
AD 12		6		4		6		6		5		4		4
AD 11				2						2		2		2
AD 10		5		4		3		5		3		4		4
AD 9		12		6		4		12		12		11		11
AD 8		19		10		10		21		22		22		22
AD 7				14		6		3		8		8		8
AD 6				0		6		3		3		6		6
AD 5						1								
Total AD		**43**		**43**		**37**		**51**		**57**		**60**		**60**
AST 11														
AST 10														
AST 9														
AST 8				2						1		2		2
AST 7		3		2		2		4		4		3		3
AST 6		7		4		2		8		8		8		8
AST 5		5		5		4		5		5		5		5
AST 4		1		3		4		1		1		1		1
AST 3						1								
AST 2						1								
AST 1														
Total AST		**16**		**16**		**14**		**18**		**19**		**19**		**19**
AST/SC6														
AST/SC5														
AST/SC4														
AST/SC3														
AST/SC2														
AST/SC1														
Total AST/SC														
TOTAL		**59**		**59**		**51**		**69**		**76**		**79**		**79**

A.4. Annex IV: Human Resources - Qualitative

A. Recruitment policy

Statutory Staff

The Agency, in line with its recruitment approach 2020-2023 "Delivering ENISA Mandate trough people", is considering recruitment in an organisational/transversal way by:

- Eliminating the fragmentation of calls by publishing the vacancies not based anymore on individual competencies needs in a specific "unit", but on the basis of a set of generic competencies per job role and family (operational staff) and expertise,
- Linking the level of competencies and expertise to the use of type of contract by exploiting at best ENISA staffing / Establishment Plan (TAs) capacity,
- Establishing meaningful and wider Reserve Lists (the size of the reserve list should = n x 4, where n is the number of unfilled TA post in the agency + the new post foreseen in the establishment plan of 2020 + 2021 combined, times a multiplication factor of 4 (statistically every 4th candidate in the reserve-list takes up the post), with a longer initial duration (2 years) that can be used transversally (not linked anymore to a post vacancy) for quick replacement/hiring,
- Considering the external demand/supply factors and redeployment,
- Simplifying the application modalities for candidates while a proper new e-recruitment tool is being implemented (SYSTAL or GSA recruitment tool).
- Developing ENISA as Employer of choice by pushing for an EVP (Employee Value Proposition), nurturing relationships networks and making current staff as ENISA Ambassadors.

To achieve this a Task Force was established in December 2019 to define the general competences which potential staff members should have (such as analytical capacity, capacity to lead and coordinate projects etc) and refine the terms of the call The new combined call will be launched in February 2020. The candidates will have 2 months to fill their applications during which time the agency will also embark on a wide campaign in all EU Member States to ensure that it captures a wide pool of diverse talent and a geographically balanced spread of potential candidates The candidates will be required to present information about their background and expertise in a simple EuroPass CV format, fulfil a talent-screener and attend an interview to test their competences. The assessment of candidates will focus on their competences and will be largely carried out by an external contractor (a framework contract which is already in development together with EFSA) under the supervision and guidance of a single pre-selection board, which will finish its job within 3 months, allowing the agency to draw up a reserve-list in late summer 2020. Provided that the call has been successful, the agency could them proceed swiftly to recruit new staff from the established reserve list for all vacant post, but also proceed to make offers for new posts in 2021 establishment plan, potentially ensuring that those will be filled already starting from 01.01.2021 thus ensuring the 100% rate of the 2021 establishment plan already in the beginning of the year.

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

Assistant Job Family:

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

Operational Job Family:

- Junior Officer/Administrator Job Category (staff providing junior expertise in a specific field of knowledge): typically, these posts are filled by grades AD5, FG IV 13
- Officer/Administrator Job Category (staff providing officer expertise in a specific field of knowledge): typically, these posts are filled by grades AD6-AD7, FG IV 14-18

- Lead Officer/Administrator (staff providing top level expertise in a specific field of knowledge): typically, these posts are filled by grades AD8-AD9
- Team Leader Job Category (staff providing operational excellence with some managerial responsibilities): typically, these posts are filed by grades AD7-AD10, FG IV 14-18
- 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 position (filled by grades AD11-AD13)
- Executive Director (filled by grades AD14-15)

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 the Article 3 of the MB Decision/12 of the European Union Agency for Network and Information Security on the general implementing 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 with all due care the available options as not to 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 one solution to attract the right profile(s) and to ensure nationality balanced (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 affect negatively 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 Temporary Agents contract was amended[11] in order to improve the attractiveness and retention. Hence, the typical duration for newly recruited Temporary Agents is an initial 5 years contract with the possibility to be renewed for an indefinite period. However, all contracts 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. ENISA used in the past 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 use again this possibility.

Non-Statutory Staff

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

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

[11] ED Decision 16/2019 of 20 February 2019

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.

Table 1 - Reclassification of temporary staff/promotion of officials

Category and grade	Staff in activity at 1.01.2018		How many staff members were reclassified in Year 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		1	2,16
AD 7		3			
AD 6		7		3	3,47
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**			

Table 2 - Reclassification of contract staff

Function Group	Grade	Staff in activity at 1.01.Year 2018	How many staff members were reclassified in Year 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		
	9	7	3	5,77
	8	2	1	4,8
CA II				
CA I	3	1		
Total		29		

C. Mobility policy

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

a. Mobility within agency: since January 2019, 13 staff members where moved under Article 7 of Staff Regulations.
b. Mobility among agencies: in 2019, 1 staff member was recruited under Inter-Agency Mobility Call.
c. Mobility between agency and Institutions: in 2019, 3 former ENISA staff moved to EU Agencies and 1 former staff moved to EU Institution.

D. Learning and Development

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

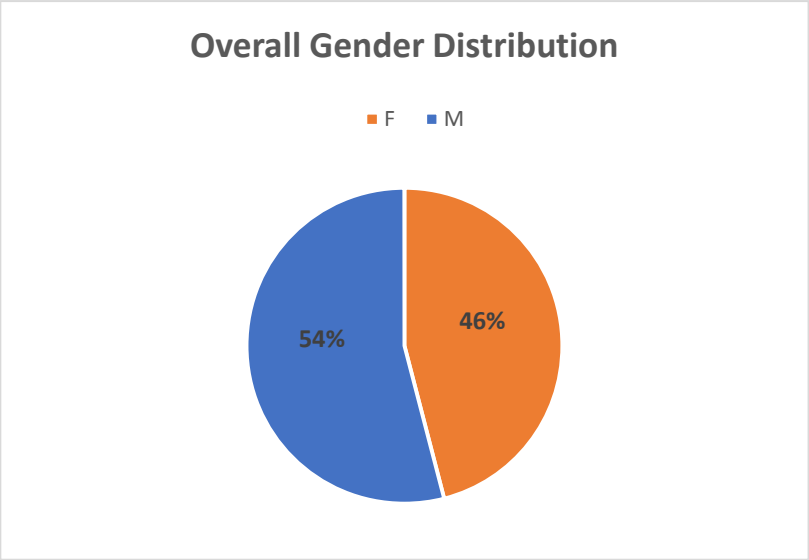
E. Gender and geographical balance

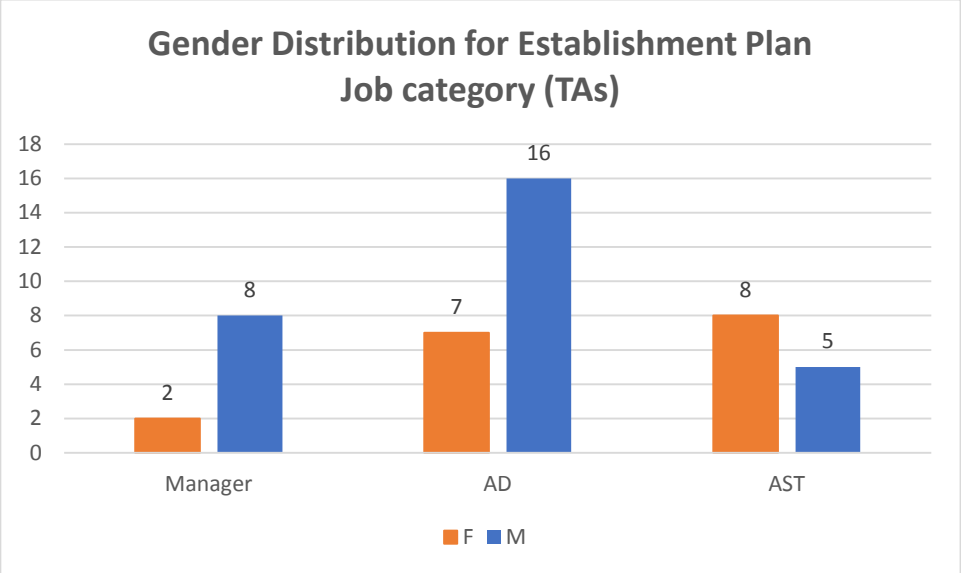
The overall gender balance among ENISA staff shows a slight male prevalence that is understandable given the scope of the Agency's work. As a measure to promote equal opportunities, the terms of published vacancy notices prevent any kind of discrimination and the Selection Board's composition is balanced in term of gender and nationality as far as possible. In 2019, the Agency has 2 women HoUs (Head of HR unit and Head of Finances and Procurement unit) and 5 women coordinating teams.

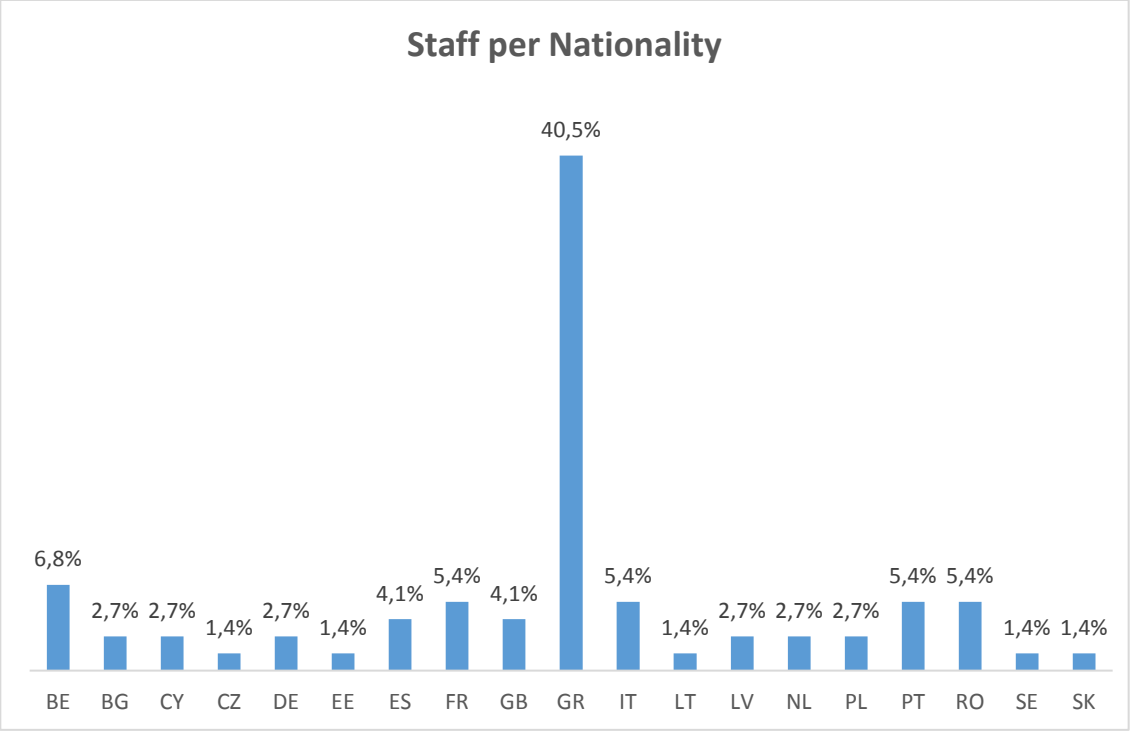
With regard to the geographical balance, while there is no quota system in operation, the Staff Regulations require when recruiting to strive for a broad balance among nationalities and to adopt measures if there is imbalance between nationalities among staff. ENISA is paying great attention to this requirement. However ENISA is facing the same challenges (as reported by the European Commission for the European Civil Service and as some other EU Agencies with low coefficient correcteur) in attracting and retaining some nationalities. Mainly, due to the specific labour market where ENISA operates and high salaries in the private sector where ENISA is not able to compete due to low corrector

coefficient, shows a shortfall of qualified professionals from different nationalities, hence, ENISA is facing challenges in increasing it 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 due to the lack of possibility for the staff members partner to find jobs, puts ENISA in the difficult position to attract staff from some nationalities. ENISA is committed to ensure a diverse workforce representation, however strives to retain staff from some nationailities on the abovementioned consideration.

Below the graphics for 31.12.2019:







F. Schooling

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

2019-2020 school year	CRECHES	SCHOOLS
ATHENS	14	33
HERAKLION	0	5

A.5. ANNEX V: BUILDINGS

As per the current Seat Agreement between ENISA and the Hellenic Authorities entered into force on the 04/10/2019, 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 were the majority of its staff is based.

At the time of this document the premises of ENISA in Athens are privately owned and rented by the Agency, and in Heraklion the premises 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 make available the amount of up to 640K 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 possible extension.

ENISA is in constant contact with the Hellenic Authorities to find suitable premises to accommodate all staff in the near future. It is expected that suitable options offered by the Hellenic Authorities are presented in early 2020.

A.6. ANNEX VI: PRIVILEGES AND IMMUNITIES

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

A.7 ANNEX VII. EVALUATIONS

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

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

A.8 ANNEX VIII: RISKS 2021

The Self Risk Assessment was performed by the Internal Audit Service in 2016. Three areas were proposed for the three next years: Stakeholders' Involvement in the Production of Deliverables in ENISA (done in 2017), Human Resources (done in 2019), Information and Communication Technology (forecasted in 2020).

The exercise peer-to-peer review with other Agencies was launched in 2019 and will be follow up every year. As recommended by the Commission, the PDN established clusters of Agencies to conduct the exercise.

Six clusters were defined: Supervision of financial Systems; Social and employment; Environment and health; Justice and Home affairs; Transport and energy; Support business and innovation.

The Agency was part of last cluster and three main risks identified:

Uncertainty associated with the Brexit process. The Brexit implies significant challenges that will have an impact on a number of areas: Changes in user behaviour; Financial impact on users; Status of UK-based representatives; Agencies staff with UK nationality; Changes in the Agencies' governing bodies; Cooperation projects where the UK is participating.

Cyber-attacks to access restricted information or to disrupt Agencies' services. The general increase in the Agencies' digital footprint (e.g. progressive transfer and management of information in the Cloud), coupled with an increase in "cyber-attacks" worldwide, are raising the

possibility of suffering "cyber-attacks" trying to gain access to Agencies' restricted/sensitive information.

In addition, the possible lack of Business Continuity Management bears the risk of not being able to provide an organizational, functional and operational framework to guarantee and ensure the continuity of Agencies' critical business functions in case of cyber-attacks.

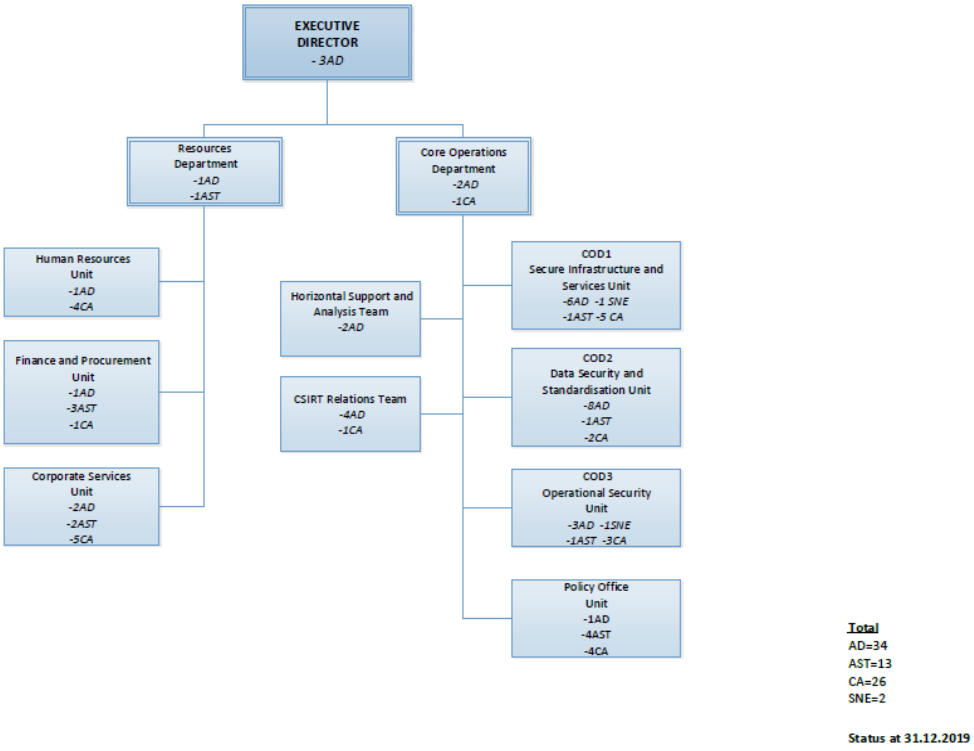
Reputation risk linked to misinformation from external media. It has been noticed that misleading information related to the activities and/or studies/reports of some EU Agencies is passed to, and consequently published by, external media (e.g. generalist press). This situation can put at risk the Agencies' credibility and reputation.

A.9 ANNEX IX: PROCUREMENT PLANNING 2021

[The procurement planning Annex will be updated in a later version of the document.]

A.10 ANNEX X: ENISA ORGANISATION

ENISA organisation as 31.12.2019.



A.11 ANNEX XI. STRATEGIES REQUIRED BY THE FRAMEWORK FINANCIAL REGULATION

The new framework financial regulation (Commission delegated regulation (EU) 2019/715 of 18 December 2018), specifies in Article 32, several requirements for the draft single programming document. Some are already covered in the previous annexes and in the text of the document.

This section provided update for the following requirements:

“(f) strategy for cooperation with third countries and/or international organisations;
(g) strategy for achieving efficiency gains and synergies;

(h) strategy for the organisational management and internal control systems including their anti-fraud strategy as last updated and an indication of measures to prevent recurrence of cases of conflict of interest, irregularities and fraud, in particular where weaknesses, reported under Article 48 or paragraph 6 of Article 78, have led to critical recommendations."

Strategy for cooperation with third countries and/or international organisations

While the agency has MB guidelines for this purpose the CSA also provides in article 12 tasks regarding international cooperation. Outputs linked to article 12 covers activities proposed by the agency and agreed with the MB. 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, within its mandate and the institutional framework.

Strategy for achieving efficiency gains and synergies

The new strategy of the agency will serve as basis which will be taken into account in the agency's reorganisation in 2020, which will in effect implement and outline steps to develop efficiency gains and synergies. ENISA is continuously working to improve its functioning, with the aim to allow the reallocation of its resources to the most efficient and economic actions for the set objectives. ENISA will update this section, after the document is revised in line with the future ENISA strategy, with example(s) as regards possible/expected efficiency gains and budget savings (both quantitative and qualitative) that could be achieved in the agency including by:

- Identifying the tasks considered for downsizing /discontinuation as well as tasks that are no longer a priority (if applicable),
- Reflecting on reprioritisation of its actions and to envisage possible redeployment of resources,
- Sharing services and IT development projects among agencies (and Joint Undertakings) operating in the same Member States or policy areas and between the agencies and the Commission,
- Increasing the automation/streamlining of work processes, moving to e-administration and e-training
- Reviewing IT infrastructure to make it more efficient and reduce duplication of IT systems within and cross agencies,
- If applicable, reviewing the network of local offices based on the principle of sound financial management, avoiding unnecessary costs and duplication of administrative functions.

Given that several internal action are ongoing on this respect, the above points will be revised in the next version. While associated projects of the above initiative(s) may need several years to be fully implemented, the progress will be presented in this section until the goals are achieved.

Strategy for the organisational management and internal control systems including anti-fraud strategy

In November 2019 the ED set up a Task Force to review the internal control systems of the agency and make recommendations as regards to the steps that should be taken in order to foster the organisational management and internal control systems. The Task Force delivered its preliminary report on 15.01.2020. Its recommendations will in effect be regarded as the strategic framework, and once elaborated, an implementation plan will be drawn up together with the reorganisation of the agency, in 2020, which will serve as a roadmap to implement the recommendations of the Task Force. Additionally, the MB of the agency is due to adopt a renewed anti-fraud strategy in Q1 2020, which will also be taken into account in the aforementioned roadmap. [to be added based on the agency's reorganisation].

ANNEX B. ACRONYMS

CSA – Cybersecurity Act
EECC – European Electronic Communication Code
GDPR – General Data Protection Regulation
NISD – NIS Directive
NISCG – NIS directive Cooperation Group
NCSS – National Cybersecurity Strategies

// MAKE SURE THAT THE OUTSIDE BACK COVER WILL BE A LEFT HAND PAGE. INSERT A BLANK RIGHT HAND PAGE IF NECESSARY.

XX-00-00-000-XX-X

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. 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

ISBN 000-00-0000-000-0
doi: 0000.0000/000000

Draft Statement of Estimates 2021 (Budget 2021)

European Union Agency for Cybersecurity

CONTENTS

1. GENERAL INTRODUCTION

Explanatory statement

Legal Basis:

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) 526/2013.

Reference acts

1. Impact assesment submitted by the Commission on 13 September 2017, on ENISA, the 'EU Cybersecurity Agency', aas part of the draft 'Cybersecurity Act' (COM(2017) 477 final)

2. ENISA Financial Rules adopted by the Management Board on 15 October 2019.

2. JUSTIFICATION OF MAIN HEADINGS

2.1 Revenue in 2021

The 2021 total revenue amounts to € 23433076 and consists of a subsidy of € 22248000 from the General Budget of the European Union, EFTA countries' contributions, € 545076 a subsidy from the Greek Government for the rent of the offices of ENISA in Greece €640000 and the interest on cash deposits.

2.2 Expenditure in 2021

The total forecasted expenditure is in balance with the total forecasted revenue.

Title 1 - Staff

The estimate of Title 1 costs is based on the Establishment Plan for 2021, which contains 76 Temporary Agent posts.

Total expenditure under Title 1 amounts to **€12.655.000,00**

Title 2 - Buildings, equipment and miscellaneous operating expenditure

Total expenditure under Title 2 amounts to **€3.374.971,40**

(including € 640.000,00 for the rent of two offices in Greece, subsidised by the Greek Government)

Title 3 - Operational expenditure

Operational expenditure is mainly related to the implementation of Work Programme 2021 and amounts to **€7.403.104,60**

3. STATEMENT OF REVENUE 2021

Title	Heading	Voted Appropriations 2018 in €	Voted Appropriations 2019 in €	Voted Appropriations 2020 in €	Draft Proposed Appropriations 2021 €	Remarks - budget 2021
1	EUROPEAN COMMUNITIES SUBSIDY	10.529.000	15.910.000	20.646.000	22.248.000	Total subsidy of the European Communities
2	THIRD COUNTRIES CONTRIBUTION	248.626	382.952	503.120	545.076	Contributions from Third Countries.
3	OTHER CONTRIBUTIONS	640.000	640.000	640.000	640.000	Subsidy from the Government of Greece
4	ADMINISTRATIVE OPERATIONS	10.500	0	0	0	Other expected income.
	GRAND TOTAL	**11.428.126**	**16.932.952**	**21.789.120**	**23.433.076**	

Article Item	Heading	Voted Appropriations 2018 in €	Voted Appropriations 2019 in €	Voted Appropriations 2020 in €	Draft Proposed Appropriations 2021 €	Remarks - budget 2021
1	EUROPEAN COMMUNITIES SUBSIDY					
10	EUROPEAN COMMUNITIES SUBSIDY					
100	*European Communities subsidy*	10.529.000	15.910.000	20.646.000	22.248.000	Regulation (EU) N° 526/2013 establishing an European Union Agency for Network and Information Security.
	CHAPTER 10	10.529.000	15.910.000	20.646.000	22.248.000	
	TITLE 1	**10.529.000**	**15.910.000**	**20.646.000**	**22.248.000**	
2	THIRD COUNTRIES CONTRIBUTION					
20	THIRD COUNTRIES CONTRIBUTION					
200	*Third Countries contribution*	248.626	382.952	503.120	545.076	Contributions from Associated Countries.
	CHAPTER 2 0	248.626	382.952	503.120	545.076	
	TITLE 2	**248.626**	**382.952**	**503.120**	**545.076**	
3	OTHER CONTRIBUTIONS					
30	OTHER CONTRIBUTIONS					
300	*Subsidy from the Ministry of Transports of Greece*	640.000	640.000	640.000	640.000	Subsidy from the Government of Greece.
	CHAPTER 30	640.000	640.000	640.000	640.000	
	TITLE 3	**640.000**	**640.000**	**640.000**	**640.000**	
4	ADMINISTRATIVE OPERATIONS					
40	ADMINISTRATIVE OPERATIONS					
400	*Administrative Operations*	10.500	0	0	0	Revenue from administrative operations.
	CHAPTER 40	10.500	0	0	0	
	TITLE 4	**10.500**	**0**	**0**	**0**	
	GRAND TOTAL	**11.428.126**	**16.932.952**	**21.789.120**	**23.433.076**	

4. STATEMENT OF EXPENDITURE 2021

Title	Heading	Voted Appropriations 2018 in €	Voted Appropriations 2019 in €	Voted Appropriations 2020 in €	Draft Proposed Appropriations 2021 €	Remarks - budget 2021
1	STAFF	6.386.500	9.387.948	12.041.486	12.655.000	Total funding for covering personnel costs.
2	BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE	1.687.500	2.677.000	2.986.000	3.374.971	Total funding for covering general administrative costs.
3	OPERATIONAL EXPENDITURE	3.354.126	4.868.004	6.761.633	7.403.105	Total funding for operational expenditures.
	GRAND TOTAL	**11.428.126**	**16.932.952**	**21.789.120**	**23.433.076**	
1	STAFF					
11	STAFF IN ACTIVE EMPLOYMENT					
110	*Staff holding a post provided for in the establishment plan*					
1100	Basic salaries	3.779.100	5.000.000	7.693.000	6.452.977	Staff Regulations applicable to officials of the European Communities, and in particular Articles 62 and 66 thereof. This appropriation is intended to cover salaries, allowances, and employee contributions on salaries of permanent officials and Temporary Agents (TA).
	Article 1 1 0	3.779.100	5.000.000	7.693.000	6.452.977	

111	***Other staff***					
1110	Contract Agents	1.168.300	1.650.000	2.041.000	2.106.500	Conditions of employment of other servants of the European Communities, and in particular Article 3 and Title III thereof. This appropriation is intended to cover salaries, allowances, and employee contributions on salaries of Contract Agents (CA).
1113	Seconded National Experts (SNEs)	239.000	144.000	447.000	124.705	This appropriation is intended to cover basic salaries and all benefits of SNEs.
	Article 111	1.407.300	1.794.000	2.488.000	2.231.205	
119	***Salary Weightings***					
1190	Salary Weightings	p.m.	p.m.	p.m.	p.m.	Staff Regulations applicable to officials of the European Communities, and in particular Articles 64 and 65 thereof. This appropriation is intended to cover the impact of salary weightings applicable to the remuneration of officials and temporary staff.
	Article 1 1 9	p.m.	p.m.	p.m.	p.m.	
	CHAPTER 11	**5.186.400**	**6.794.000**	**10.181.000**	**8.684.182**	
12	**RECRUITMENT EXPENDITURE**					
120	***Travel Expenses in interviewing candidates***					
1200	Travel Expenses in interviewing candidates	19.000	97.000	80.000	80.000	This appropriation is intended to cover travel expenditure incurred for interviewing candidates.
1201	Miscellaneous expenditure related to recruitment	n/a	n/a	n/a	39.087	This appropriation is intended to cover other expenditure related to recruitment, e.g. vacancy notices publication.
	Article 1 2 0	19.000	97.000	80.000	119.087	
121	***Expenditure on entering/leaving and transfer***					
1210	Expenses on Taking Up Duty and on End of Contract	9.600	40.000	10.000	20.536	Staff Regulations applicable to officials of the European Communities, and in particular Articles 20 and 71 thereof and Article 7 of Annex VII thereto. This appropriation is intended to cover the travel expenses of staff (including members of their families).
1211	Installation, Resettlement and Transfer Allowance	68.000	356.042	125.000	113.482	Staff Regulations applicable to officials of the European Communities, and in particular Articles 5 and 6 of Annex VII thereto. This appropriation is intended to cover the installation allowances for staff obliged to change residence after taking up their duty.
1212	Removal Expenses	68.000	247.000	100.000	59.400	Staff Regulations applicable to officials of the European Communities, and in particular Articles 20 and 71 thereof and Article 9 of Annex VII thereto. This appropriation is intended to cover the removal costs of staff obliged to change residence after taking up duty.
1213	Daily Subsistence Allowance	96.500	228.906	130.000	95.446	Staff Regulations applicable to officials of the European Communities, and in particular Articles 20 and 71 thereof and Article 10 of Annex VII thereto, as well as Articles 25 and 67 of the Conditions of Employment of other Servants. This appropriation is to cover the costs of daily subsistance allowances.
	Article 1 2 1	242.100	871.948	365.000	288.865	
	CHAPTER 1 2	**261.100**	**968.948**	**445.000**	**407.952**	

13	**SOCIO-MEDICAL SERVICES AND TRAINING**					
131	***Medical Service***					
1310	Medical Service	35.000	75.000	75.000	53.882	This appropriation is intended to cover the costs of annual medical visits and inspections, occupational doctor services as well as pre-recruitment medical costs and other costs related to medical services.
	Aticle 1 3 1	35.000	75.000	75.000	53.882	
132	***Training***					
1320	Language Courses and Other Training	155.000	250.000	175.000	280.182	This appropriation is intended to cover the costs of language and other training needs as well as teambuilding activities.
	Article 1 3 2	155.000	250.000	175.000	280.182	
133	***Social welfare***					
1330	Other welfare expenditure	n/a	n/a	n/a	211.133	This appropriation is intended to cover other welfare expenditure such as health related activities to promote well-being of staff, other activities related to internal events, other welfare measures.
1331	Schooling & Education expenditure	n/a	n/a	n/a	478.747	This appropriation is intended to cover the subsidy for the functioning of the School of European Education of Heraklion, and other expenditure relevant to schooling & education of children of the Agency staff.
	Article 1 3 3	0	0	0	689.880	
	CHAPTER 1 3	**190.000**	**325.000**	**250.000**	**1.023.944**	
14	**TEMPORARY ASSISTANCE**					
140	***European Commission Management Costs***					
1400	EC Management Costs	54.000	58.000	60.000	70.939	This appropriation is intended to cover the EC management costs.
	Article 1 4 0	54.000	58.000	60.000	70.939	
141	***Social welfare***					
1410	Special Assistance Grants	0	0	0	p.m.	This appropriation is intended to cover special assistance grants.
1411	Other welfare expenditure	130.000	110.000	225.000	p.m.	This appropriation is intended to cover other welfare expenditure.
1412	Schooling & Education expenditure	300.000	420.000	420.000	p.m.	This appropriation is intended to cover the subsidy for the functioning of the School of European Education of Heraklion, and other expenditure relevant to schooling & education of children of the Agency staff.
	Article 1 4 1	430.000	530.000	645.000	0	
142	***Temporary Assistance***					
1420	Interim Service	155.000	572.000	250.000	1.165.287	This appropriation is intended to cover the costs of temporary assistance (trainees and interim services).
1421	HR consultancy services	95.000	115.000	165.486	102.696	This appropriation is intended to cover expenditure of contracting consultants and other costs of HR related services provided by external contractors, e.g. internal communication, staff survey or other similar services.
1422	Internal Control and Audit	15.000	25.000	45.000	p.m.	This appropriation is intended to cover expenditure related to the development and functioning of Internal Control Coordination functions.
	Article 1 4 2	265.000	712.000	460.486	1.267.983	
	CHAPTER 1 4	**749.000**	**1.300.000**	**1.165.486**	**1.338.922**	
15	**MISSIONS AND DUTY TRAVEL**					
150	***Missions expense, duty travel expense and ancillary expenditure***					
1500	Missions expense, duty travel expense and ancillary expenditure	n/a	n/a	n/a	1.200.000	This appropriation is intended to cover travel expenses, daily subsistence allowances and ancillary or exceptional expenditure incurred by staff and SNEs in connection with missions and duty travel. This appropriation is intended to cover travel agency fees and other costs related to missions.
	Article 1 5 0	n/a	n/a	n/a	**1.200.000**	
	Total Title 1	**6.386.500**	**9.387.948**	**12.041.486**	**12.655.000**	
2	**BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE**					
20	**BUILDINGS AND ASSOCIATED COSTS**					
200	**Buildings and associated costs**					
2000	Rent of buildings	640.000	640.000	640.000	640.000	This appropriation is intended to cover the payment of rents for buildings or parts of buildings occupied by the Agency and the hiring of parking spaces.
2002	Building Insurance	5.500	6.000	6.000	6.500	This appropriation is intended to cover the insurance costs of the premises of the Agency.
2003	Water, gas, electricity and heating	85.000	130.000	130.000	100.000	This appropriation is intended to cover the costs of utitlities for the premises of the Agency.
2004	Cleaning and maintenance	55.000	74.000	74.000	100.000	This appropriation is intended to cover the costs of cleaning and upkeeping of the premises used by the Agency.
2005	Fixtures and Fittings	15.000	25.000	25.000	50.000	This appropriation is intended to cover the fitting-out of the premises and repairs in the building.

2006	Security equipment		15.000	25.000	25.000	50.000	This appropriation is intended to cover purchases and maintenance cost of equipment related to security and safety of the building and the staff.
2007	Security Services		110.000	140.000	180.000	160.000	This appropriation is intended to cover expenditure on buildings connected with security and safety, in particular contracts governing building surveillance.
2008	Other expenditure on buildings		75.000	60.000	100.000	950.000	The appropriation is intended to cover expenditure on buildings not specially provided for in the articles in Chapter 20, for example market survey costs for rent of buildings, and costs of departmental removals and other handling costs.
		Article 2 0 0	1.000.500	1.100.000	1.180.000	2.056.500	
		CHAPTER 2 0	**1.000.500**	**1.100.000**	**1.180.000**	**2.056.500**	

21	**MOVABLE PROPERTY AND ASSOCIATED COSTS**						
210	***Technical Equipment and installations***						
2100	Technical Equipment and services		15.000	25.000	25.000	50.000	This appropriation is intended to cover expenditure of acquiring technical equipment, as well as maintenance and services related to it.
		Article 2 1 0	15.000	25.000	25.000	50.000	
211	***Furniture***						
2110	Furniture		30.000	15.000	50.000	75.000	This appropriation is intended to cover the costs of purchasing, leasing, and repairs of furniture.
		Article 2 1 1	30.000	15.000	50.000	75.000	
212	***Transport Equipment***						
2120	Transport Equipment		p.m.	p.m.	p.m.	p.m.	This appropriation is intended to cover the costs of purchasing and leasing of transport equipment.
2121	Maintenance and Repairs of transport equipment		10.000	12.000	12.000	12.000	This appropriation is intended to cover the costs of maintenance and repairs of transport equipment as well as insurance and fuel.
		Article 2 1 2	10.000	12.000	12.000	12.000	
213	***Library and Press***						
2130	Books, Newspapers and Periodicals		5.000	6.000	12.000	10.000	This appropriation is intended to cover the purchase of publications and subscriptions to information services necessary for the work of the Agency, including books and other publications, newspapers, periodicals, official journals and subscriptions.
		Article 2 1 3	5.000	6.000	12.000	10.000	
		CHAPTER 2 1	**60.000**	**58.000**	**99.000**	**147.000**	
22	**CURRENT ADMINISTRATIVE EXPENDITURE**						
220	***Stationery, postal and telecomunications***						
2200	Stationery		30.000	60.000	75.000	35.000	This appropriation is intended to cover the costs of office stationery.
2201	Postage and delivery charges		19.000	20.000	55.000	22.000	This appropriation is intented to cover post office and special courrier costs.
2203	Other Office Supplies		12.000	23.000	45.000	22.000	This appropriation is intended to cover the purchase of office kitchen consumables.
		Article 2 2 0	61.000	103.000	175.000	79.000	
221	***Financial charges***						
2210	Bank charges and interest paid		1.000	1.000	1.000	1.000	This appropriation is intended to cover bank charges, interest paid and other financial and banking costs.
		Article 2 2 1	1.000	1.000	1.000	1.000	
222	***Outsourced services***						
2220	Outsourced consultancy services		n/a	n/a	n/a	45.000	This appropriation is intended to cover outsourced expenditure linked to support services, e.g. for financial, accounting, internal controls, legal consultancy, advisory, audit and/or other administrative support services provided by third parties.
2221	Strategic consultancy		n/a	n/a	n/a	50.000	This appropriation is intended to cover the costs of consultancy services related to the strategy, planning and organisation of the Agency.
		Article 2 2 2	0	0	0	95.000	
223	***Damages***						
2230	Damages		p.m.	p.m.	p.m.	p.m.	This appropriation is intended to cover the costs of all kinds of damages incurred by the Agency.
		Article 2 2 3	p.m.	p.m.	p.m.	p.m.	
		CHAPTER 2 2	**62.000**	**104.000**	**176.000**	**175.000**	
23	**ICT**						
230	***ICT***						
2304	Service Transition		130.000	600.000	770.000	150.000	This appropriation is intended to cover the costs of purchasing hardware & software, as well as maintenance and consultancy services related to the transition to new ICT infrastructure and systems.
2305	Service Operations		95.000	220.000	250.000	196.471	This appropriation is intended to cover the costs of purchasing hardware & software, as well as maintenance and consultancy services related to existing ICT infrastructure and systems.
2307	Service External		340.000	595.000	511.000	650.000	This appropriation is intended to cover the costs of IT related outsourced services, including hosting, telecommunications, ISP, subscriptions and other.
		Article 2 3 0	565.000	1.415.000	1.531.000	996.471	
		CHAPTER 2 3	**565.000**	**1.415.000**	**1.531.000**	**996.471**	
		Total Title 2	**1.687.500**	**2.677.000**	**2.986.000**	**3.374.971**	

3	**OPERATIONAL EXPENDITURE**					
30	**ACTIVITIES RELATED TO MEETINGS AND MISSIONS**					
300	***Meetings of the Bodies of the Agency***					
3001	Management Board meetings	120.000	120.000	170.000	200.000	This appropriation is intended to cover the costs of Management Board and Executive Board meetings of the Agency, i.e. meetings, travel costs of experts participating.
3002	Meetings of other ENISA bodies	n/a	n/a	n/a	200.000	This appropriation is intended to cover the costs of meetings of other ENISA bodies including the costs of Advisory Group (AG) and National Liaison officers (NLO) network meetings and relevant travel costs.
	Article 3 0 0	120.000	120.000	170.000	400.000	
301	***Mission and Representation Costs***					
3011	Entertainment and Representation expenses	2.500	15.394	20.000	20.000	This appropriation is intended to cover the costs of entertainment and representation expenses.
3016	Missions	590.000	897.930	1.200.000	p.m.	This appropriation is intended to cover all staff and SNE mission related costs.
	Article 3 0 1	592.500	913.324	1.220.000	20.000	
302	***Other meetings***					
3021	Other Operational meetings	2.500	10.000	20.000	20.000	This appropriation is intended to cover the costs of the various operational meetings.
	Article 3 0 2	2.500	10.000	20.000	20.000	
	CHAPTER 3 0	**715.000**	**1.043.324**	**1.410.000**	**440.000**	
32	**HORIZONTAL OPERATIONAL ACTIVITIES**					
320	***Conferences and Joint Events***					
3200	Horizontal Operational meetings	165.000	214.608	200.000	p.m.	This appropriation is intended to cover the costs of horizontal operational meetings, including the costs of Advisory Group (AG) and National Liaison officers network meetings and relevant travel costs.
	Article 3 2 0	165.000	214.608	200.000	0	
321	***Communication and Information dissemination***					
3210	Communication activities	80.000	150.000	175.000	175.000	This appropriation is intended to cover the costs of the corporate communication activities of the Agency.
3211	Internal Communication	20.000	0	65.000	65.000	This appropriation is intended to cover the costs of internal communication activities of the Agency.
3212	Stakeholders' communication	160.000	113.000	200.000	200.000	This appropriation is intended to cover the costs of activities related to communication with stakeholders of the Agency.
	Article 3 2 1	260.000	263.000	440.000	440.000	
323	***Translation and interpretation services***					
3230	Translations	15.000	30.072	71.633	71.633	This appropriation is intended to cover the costs of translations of documents for the Agency.
	Article 3 2 3	15.000	30.072	71.633	71.633	
325	***Operational Systems***					
3250	Operational Systems including website development	80.000	57.000	140.000	140.000	This appropriation is intended to cover the costs of development and hosting of external facing systems, e.g. ENISA website
	Article 3 2 5	80.000	57.000	140.000	140.000	
326	***Strategy and Evaluation***					
3260	*Strategic consultancy*	40.000	50.000	50.000	p.m.	This appropriation is intended to cover the costs of consultancy services related to the strategy of the Agency.
3261	*External Evaluations*	100.000	0	100.000	200.000	This appropriation is intended to cover the costs of external evaluations geared towards the Agency operations.
	Article 3 2 6	140.000	50.000	150.000	200.000	
	CHAPTER 3 2	**660.000**	**614.680**	**1.001.633**	**851.633**	

36	**CORE OPERATIONAL ACTIVITIES**						
363	***Activity: Expertise***						
3630	Activity: Expertise		536.626	875.000	1.030.000	p.m.	This appropriation is intended to cover the costs of Activity 1 – Expertise. Anticipate and support Europe in facing emerging network and information security challenges
		Article 3 6 3	536.626	875.000	1.030.000	0	
364	***Activity: Policy***						
3640	Activity: Policy		646.500	1.150.000	1.530.000	p.m.	This appropriation is intended to cover the costs of Activity 2 – Policy and the costs of Activity 5 - Certification.
		Article 3 6 4	646.500	1.150.000	1.530.000	0	
365	***Activity: Capacity***						
3650	Activity: Capacity		300.000	535.000	940.000	p.m.	This appropriation is intended to cover the costs of Activity 3 – Capacity. Support Europe in setting up state-of-the-art network and information security capacities
		Article 3 6 5	300.000	535.000	940.000	0	
366	***Activity: Community***						
3660	Activity: Community		496.000	650.000	850.000	p.m.	This appropriation is intended to cover the costs of Activity 4 – Community. Make the European network and information security community a reality
		Article 3 6 6	496.000	650.000	850.000	0	
		CHAPTER 3 6	**1.979.126**	**3.210.000**	**4.350.000**	**0**	
37	**CORE OPERATIONAL ACTIVITIES**						
371	***Article 5***						
3710	Article 5 - Policy/law development & implementation		n/a	n/a	n/a	1.300.000	This appropriation is intended to cover the costs of activities related to implementation of Article 5 - Policy/law development & implementation.
		Article 3 7 1	n/a	n/a	n/a	1.300.000	
372	***Article 6***						
3720	Article 6 - Capacity-building		n/a	n/a	n/a	1.290.000	This appropriation is intended to cover the costs of activities related to implementation of Article 6 - Capacity-building.
		Article 3 7 2	n/a	n/a	n/a	1.290.000	
373	***Article 7***						
3730	Article 7 - Operational cooperation		n/a	n/a	n/a	535.000	This appropriation is intended to cover the costs of activities related to implementation of Article 7 - Operational cooperation.
		Article 3 7 3	n/a	n/a	n/a	535.000	
374	***Article 8***						
3740	Article 8 - Market, certification		n/a	n/a	n/a	1.381.471	This appropriation is intended to cover the costs of activities related to implementation of Article 8 - Market, certification.
		Article 3 7 4	n/a	n/a	n/a	1.381.471	
375	***Article 9-12***						
3750	Articles 9 - Knowledge & information, 10 - Awareness-raising & education, 11 - Research & innovation, and 12 - International cooperation		n/a	n/a	n/a	1.605.000	This appropriation is intended to cover the costs of activities related to implementation of Articles 9 - Knowledge & information, 10 - Awareness-raising & education, 11 - Research & innovation, and 12 - International cooperation.
		Article 3 7 5	n/a	n/a	n/a	1.605.000	
		CHAPTER 3 7	**0**	**0**	**0**	**6.111.471**	
		TITLE 3	**3.354.126**	**4.868.004**	**6.761.633**	**7.403.105**	
		GRAND TOTAL	**11.428.126**	**16.932.952**	**21.789.120**	**23.433.076**	

European Union Agency
for Cybersecurity

Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

Draft Establishment plan 2021

Category and grade	Establishment plan 2020		Establishment plan 2021
	Off.	TA	TA
AD 16			
AD 15		1	
AD 14			1
AD 13			1
AD 12		6	5
AD 11			2
AD 10		5	3
AD 9		12	12
AD 8		21	22
AD 7		3	8
AD 6		3	3
AD 5			
Total AD		**51**	**57**
AST 11			
AST 10			
AST 9			
AST 8			1
AST 7		4	4
AST 6		8	8
AST 5		5	5
AST 4		1	1
AST 3			
AST 2			
AST 1			
Total AST		**18**	**19**
AST/SC6			
AST/SC5			
AST/SC4			
AST/SC3			
AST/SC2			
AST/SC1			
Total AST/SC			
TOTAL		**69**	**76**