European Union Agency for Cybersecurity

DECISION No MB/2021/1 of the Management Board of the European Union Agency for Cybersecurity (ENISA) endorsing the draft Programming Document 2022-2024, the draft Statement of estimates 2022 and the draft Establishment plan 2022

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(2020) 2297 final of 20 April 2020 on the guidelines for single programming document for decentralised agencies and the template for the Consolidated Annual Activity Report for decentralised agencies.

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 2021;

(2) The Management Board should endorse the draft programming document by 31 January 2021;

(3) The Executive Board has endorsed the draft single programming document 2022-2024 at its meeting held on 21-22 January 2021.

(4) The Agency should send the draft programming document to the Commission, the European Parliament and the Council no later than 31 January 2021;

[1] *OJ L 151, 7.6.2019, p. 15–69*

HAS DECIDED TO ADOPT THE FOLLOWING DECISION:

Article 1

The Programming Document 2022-2024 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 2022 and the Establishment plan 2022 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 of its adoption. It will be published on the Agency website.

Done by written procedure on 1 February 2021.

On behalf of the Management Board,

[signed]

Jean-Baptiste Demaison

Chair of the Management Board of ENISA

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA SINGLE PROGRAMMING DOCUMENT 2022-2024

Including Multiannual planning,
Work programme 2022 and
Multiannual staff planning

VERSION: DRAFT V.1

DOCUMENT HISTORY

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

Date	Version	Modification	Author
December 2020	V.01	MB for consultation	ENISA
January 2021	V.1	For adoption by MB	ENISA

TABLE OF CONTENTS

LIST OF ACRONYMS

ABAC	Accrual-based accounting
AD	Administrator
AST	Assistant
BEREC	Body of European Regulators for Electronic Communications
Cedefop	European Centre for the Development of Vocational Training
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERT-EU	Computer Emergency Response Team for the EU
COVID-19	Coronavirus disease 2019
CSA	Cybersecurity Act
CSIRT	Computer security incidence response team
ECoA	European Court of Auditors
EC3	European Cybercrime Centre
ECCG	European Cybersecurity Certification Group
EDA	European Defence Agency
EEAS	European External Action Service
EECC	European Electronic Communications Code
EFTA	European Free Trade Association
eID	Electronic identification
ENISA	European Union Agency for Cybersecurity
EU-LISA	European Union Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice
Europol	European Union Agency for Law Enforcement Cooperation
FTE	Full-time equivalent
ICT	Information and communication technology
IPR	Intellectual property rights
ISAC	Information Sharing and Analysis Centre
IT	Information technology
MoU	Memorandum of understanding
NIS	Networks and information systems
NIS CG	NIS Cooperation Group
NLO	National Liaison Officers
SC	Secretary
SCCG	Stakeholder Cybersecurity Certification Group
SLA	Service-level agreement
SMEs	Small and medium-sized enterprises
SOP	Standardised operating procedure
SPD	*Single Programming Document*

INTRODUCTION

FOREWORD[1]

Europe's *digital decade* has started off with a wide range of key, ambitious and pioneering EU policy initiatives which will already lead to a changed digital landscape by the time we implement this ENISA 2022-2024 Single Programming Document.

A great many of these initiatives either directly or indirectly integrate cybersecurity concerns, challenges and solutions and they have been crowned in December 2020 by the EU's new Cybersecurity Strategy. ENISA is ready and indeed very proud to contribute to making these initiatives and their implementation a success, whether this be promoting the uptake of the EU's first cybersecurity certification schemes, revising the NIS Directive or supporting the full implementation of the EU's 5G cybersecurity Toolbox. It will use its new mandate, the expanded tasks and the fresh resources given to it by the Cybersecurity Act in 2019 to make sure that ENISA remains a key and reliable player and partner within the EU's cybersecurity ecosystem, able to tackle the ever-moving target of cybersecurity.

In this first year and a half of my tenure, I have been inspired in my work by the motivation and drive of the EU cybersecurity community - from my ENISA staff colleagues in their daily work to the political figureheads and the European stakeholder community in and across the EU and in the national institutions in their united vision and support. There is a real common determination and a *let's-do-it* approach to make Europe more cybersecure. We will need to maintain that momentum to tackle the ever-growing sophistication of cyber-attackers and cyber challenges. Only in this way we will be able to establish a European technological autonomy in the area of cybersecurity.

I am also particularly proud that - together with the Agency's staff and its Management Board - we have laid solid foundations to make ENISA more agile, more connected and more performance orientated in the way it works. This has been enshrined in the 2020 ENISA-specific Strategy for a Trusted and Cyber Secure Europe. And the effects are showing… we are increasingly able to attract cybersecurity talent from all over the EU to help us make a difference. And with the generous support of our Greek host authorities, we are planning to move to larger premises in Athens, and are expanding our networks throughout the EU.

The full positive effects of these investments will only be truly felt once we have overcome the current pandemic, but I am convinced that we will come out of this stronger, more united and better prepared to embark on this European digital decade project.

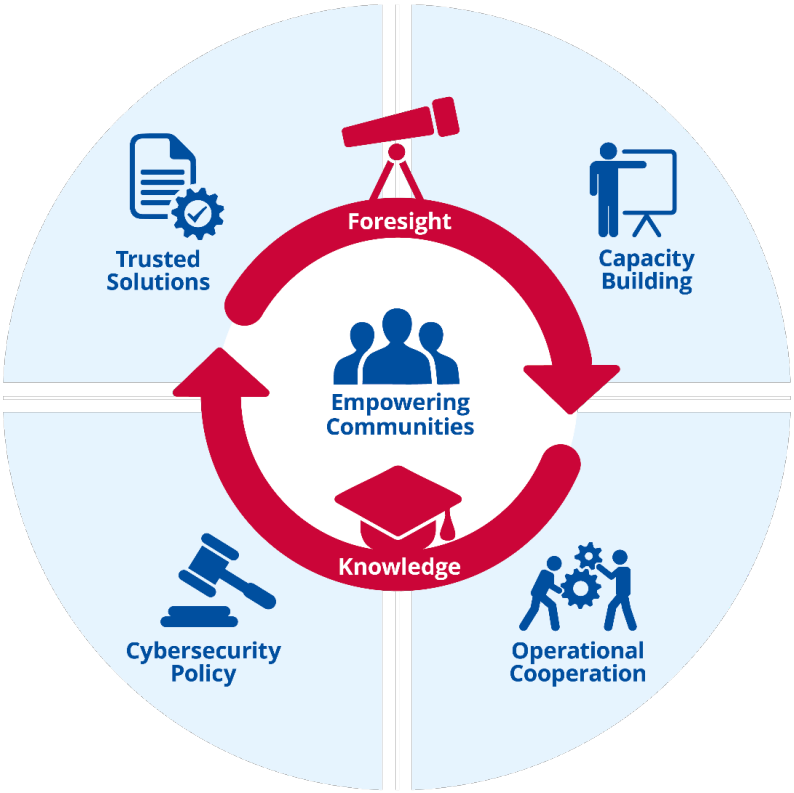
Juhan Lepassaar

[1] Status as of 31st January 2021 to be updated

MISSION STATEMENT

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union in cooperation with the wider community. It does this through acting as a centre of expertise on cybersecurity, collecting and providing independent, high quality technical advice and assistance to Member States and EU bodies on cybersecurity. It contributes to developing and implementing the Union's cybersecurity policies.

Our aim is to strengthen trust in the connected economy, boost resilience and trust of the Union's infrastructure and services and keep our society and citizens digitally secure. We aspire to be an agile, environmentally and socially responsible organisation focused on people.



STRATEGY

EMPOWERING COMMUNITIES

Cybersecurity is a shared responsibility. Europe strives for a cross sectoral, all-inclusive cooperation framework. ENISA plays a key role in stimulating active cooperation between the cybersecurity stakeholders in Member States and the EU institutions and agencies. It strives to ensure complementarity of common efforts, by adding value to the stakeholders, exploring synergies and effectively using limited cybersecurity expertise and resources. Communities should be empowered to scale up the cybersecurity model.

CYBERSECURITY POLICY

Cybersecurity is the cornerstone of digital transformation and the need for it permeates all sectors, therefore it needs to be considered across a broad range of policy fields and initiatives. Cybersecurity must not be restricted to a specialist community of technical cybersecurity experts. Cybersecurity must therefore be embedded across all domains of EU policies. Avoiding fragmentation and the need for a coherent approach while taking into account the specificities of each sector is essential.

OPERATIONAL COOPERATION

The benefits of the European digital economy and society can only be fully attained under the premise of cybersecurity. Cyber-attacks know no borders. All layers of society can be impacted and the Union needs to be ready to respond to massive (large-scale and cross-border) cyber-attacks and cyber crisis. Cross-border interdependencies have highlighted the need for effective cooperation between Member States and the EU institutions for faster response and proper coordination of efforts at all levels (strategic, operational, technical and communications).

CAPACITY BUILDING

The frequency and sophistication of cyberattacks is rising speedily, while at the same time the use of ICT infrastructures and technologies by individuals, organisations, and industries is increasing rapidly. The needs for cybersecurity knowledge and competences exceeds the supply. The EU has to invest in building competences and talents in cybersecurity at all levels, from the non-expert to the highly skilled professional. The investments should focus not only on increasing the cybersecurity skillset in the Member States but also on making sure that the different operational communities possess the appropriate capacity to deal with the cyber threat landscape.

TRUSTED SOLUTION

Digital products and services bring about benefits that need to be leveraged as well as risks that need to be mitigated. While evaluating the security of digital solutions and ensuring their trustfulness, it is essential to adopt a common approach, with the goal to strike a balance across societal, market, economic and cybersecurity needs. Innovative solutions are explored, much as repurposing standardised ones is. A dedicated entity acting in a cohesive manner is likely to increase stakeholders' trust on digital solutions and the broader digital environment in the internal market.

FORESIGHT

Numerous new technologies, still in their infancy or close to mainstream adoption, would benefit from the use of foresight methods. Through a structured process enabling dialogue among stakeholders, decision- and policy-makers would be able to define early mitigation strategies that improve the EU resilience to cybersecurity threats and find solutions to address emerging challenges.

KNOWLEDGE

The energy that fuels the mill of cybersecurity is information and knowledge. For cybersecurity professionals to be efficient at tackling our objectives, to work in a constantly moving environment – in terms of digital developments as well as with regard to actors – to face the challenges of our time, a continuous process of collecting, organising, summarising, analysing, communicating, and maintaining cybersecurity information and knowledge is clearly needed. All phases are essential to ensure that information and knowledge is shared and expanded within the EU cybersecurity ecosystem.

SECTION I. GENERAL CONTEXT

2020 was characterised by the increased prioritisation of EU digital policies ranging from initiatives such as the Digital Services Act (DSA) to the cybersecurity-specific revision proposals of the NIS Directive – with many additional digital initiatives in between. The EU's ambitions were coined by the phrase "making 2020-2030 'Europe's Digital Decade'" by Commission President Van der Leyen in her State of Union speech[2] in September 2020. Where cybersecurity is concerned, these ambitions were made more concrete in the EU's Cybersecurity Strategy[3] for the Digital Decade, released in December 2020 and also in the context of ensuring the EU's technological autonomy.

ENISA welcomes the EU's new Cybersecurity Strategy. The strategy proposes amongst many things, the review of the Network and Information Services (NIS) Directive, a new Critical Entities Resilience (CER) Directive, a network of Security Operations Centres (SOCs), new measures to strengthen the EU Cyber Diplomacy Toolbox and the further implementation of its 5G cybersecurity Toolbox. The Agency is ready to utilise fully its mandate and tasks to act in the areas outlined by the strategy over the period of the SPD for 2022-2024.

The Covid-19 pandemic has not only brought healthcare challenges, it has also impacted the process of digitalization in Europe, worldwide and across sectors, has increased technological complexities and exposed the need to boost technology skill sets. These effects in turn have also accelerated the exposure to a wide range of cybersecurity threats and threat actors as documented by ENISA in 2020 on the one hand, while increasing the need for cybersecurity knowledge, awareness, resilience, cooperation and solutions on the other. This affects all aspects of the work of ENISA and the cybersecurity ecosystem that the EU is building up.

ENISA's 8th edition of its annual Threat Landscape Report[4] confirmed current and future trends that cyberattacks are becoming ever more sophisticated, targeted, widespread and undetected. Malware was voted again as the EU's number one cyber threat by a poll of intelligence experts, and changes were observed for phishing, identity theft and ransomware moving to higher-ranking positions. Monetisation remains cybercriminals' top motivation, and the COVID-19 environment has fuelled attacks on homes, businesses, governments and critical infrastructure in 2020. Industries and governments alike continue to be hit by cyberespionage attacks. The number of data breach incidents continues to be very high, and the amount of stolen financial information and user credentials is growing. Unfortunately, we are getting used to hearing terms like *badrabbit ransomware, winnti, magecart* or *watering hole attacks*. In December 2020, the European Medicines Agency (EMA) was a victim of a cyberattack resulting in the leak of documents relating to the evaluation processes for COVID-19 vaccines. In the same month, another cyberattack to the software company SolarWinds through its supply chain resulted in a backdoor infiltration into its commercial software application. The current escalation and the threat landscape status require ever new methods and a different approaches for Europe to become cyber secure.

The adoption and implementation of policy frameworks is one key area where the EU is making a difference. Indeed, the policies and initiatives being put in place in the coming years will determine how the EU faces the cybersecurity challenges of today and tomorrow. Within this picture, ENISA will determine and adapt its support in particular in the following areas:

Operational cooperation - NIS2 & Joint Cyber Unit

[2] https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655
[3] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391
[4] https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

Improving cyber resilience, particularly for those who operate essential services such as healthcare and energy or for those who provide online marketplace services has been the main focus of the current NIS Directive since 2016. The proposed expansion of scope under the new NIS2 Directive foresees far more entities obliged to take measures to increase the level of cybersecurity in Europe.

A 2020 ENISA study on NIS Investments[5] showed that for organisations implementing the NIS Directive "Unclear expectations" (35%) and "Limited support from the national authority" (22%) were among the challenges faced. The NIS2 proposal addresses these areas, aiming to provide more clarity towards what is expected from the national authorities, computer security incident response team (CSIRTs) and essential and important entities in terms of reporting, crisis management framework and information sharing.

ENISA is already invested in the above resilience, cooperation and capacity-building work, and will be building up its own capacities to support the outcome of the proposal in the coming years. Pending a decision, this would also apply to increased cooperation under a potential future Joint Cyber Unit umbrella.

Implementation of the EU cybersecurity certification framework
2021 will see Europe's first Union Rolling Work Programme (URWP) outlining the cybersecurity certification priority areas launched by the European Commission. ENISA is playing a central role in supporting the implementation of the European cybersecurity certification framework of 2019 by preparing and maintaining the candidate schemes with the support of area experts and in collaboration with public authorities in the MS. It is expected that the draft candidate cybersecurity certifications schemes proposed by ENISA will be adopted as Commission implementing Regulations. The adopted schemes will allow a conformity assessment of digital products, services and processes that are produced and consumed in the Digital Single Market under those schemes, therefore increasing their cybersecurity. Finalizing the candidate schemes for the more specialized product categories under the EUCC (EU Common Criteria) scheme and for cloud services is just the first step and should start bringing first benefits in terms of EU-wide certification processes and higher consumer and user trust during the time period 2022-2024.

Research & Innovation
The EU is extending its support and investments in the wealth of expertise and experience in cybersecurity research, technological and industrial development that exists in the Union also by prioritising cybersecurity in its research and innovation support efforts, and in particular through its Horizon Europe and Digital Europe programmes. It is also pooling resources and expertise by setting up the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. ENISA is ready to contribute to this essential area in the coming years within the role which will be given to it by the Regulation and by the mandate of the Cybersecurity Act. Some of this work can already be anticipated for the 2022-2024 period, and will be made more concrete as the Competence Centre is rolled out.

Artificial Intelligence (AI)
With the EU's AI agenda advancing rapidly following the initial 2020 White Paper and Impact Assessment, the EU is addressing the major technological, ethical, legal and socio-economic challenges to put AI at the service of European citizens and the economy, for instance by considering linking high-risk AI systems to mandatory trustworthiness requirements. One of these challenges is understanding the interplay between cybersecurity and AI and how this can affect availability, safety or resilience of

[5] https://www.enisa.europa.eu/publications/nis-investments

future AI services and applications.
Building on ENISA's AI Threat Landscape Report[6] of December 2020, the Agency can continue its open dialogue with EU institutions in support of the legislative initiatives reaching into 2022-2024. Here ENISA could provide good security requirement practices and guidelines, therefore assisting the Commission and Member States in the possible development of an AI Cyber Security Toolbox or integrate new threat attack scenarios or new emerging technologies into its threat landscape assessment.

Digital identities & eIDAS
The EU's eIDAS regulation provides a framework for interoperability of national e-ID schemes and sets up an EU-wide market of (electronic) trust services. Electronic identity schemes and trust services are crucial for the EU digital market, because they allow citizens and businesses to carry out transactions online in a safe and trusted way. In 2020 the Commission reviewed the eIDAS Regulation and identified several gaps. At the start of 2021 the Commission made proposals for an improved eIDAS Regulation, aiming to enable a European digital identity, that can be used by all EU citizens and by EU businesses when carrying out online transactions. In the 2022-2024 period ENISA will support Member States and the Commission with the discussions about these new proposals as well as with the implementation.

[6] https://www.enisa.europa.eu/news/enisa-news/enisa-ai-threat-landscape-report-unveils-major-cybersecurity-challenges

SECTION II. MULTI-ANNUAL PROGRAMMING 2022 – 2024

Europe has for decades taken steps to improve digital security and trust through policies and initiatives. The Management Board of ENISA adopted a new strategy for the Agency in June 2020, which builds on the Cybersecurity Act (CSA), and outlines how the Agency will strive to meet the expectation of the cybersecurity ecosystem in a long-term perspective, in a manner that is open, innovative, agile as well as being socially and environmentally responsible. The strategy sets out a vision of “A trusted and cyber secure Europe” in which all citizens and organisations of Europe not only benefit but are also key components in the effort to secure Europe. Most importantly, the new ENISA strategy outlines seven strategic objectives which are derived from the CSA and set the expected long-term goals for the Agency.

The following table maps the strategic objectives against the CSA Articles and the activities of the Work Programme.

STRATEGIC OBJECTIVE	ACTIONS TO ACHIEVE OBJECTIVE	ARTICLE OF THE CSA	EXPECTED RESULTS	KPI	METRICS
SO1 **Empowered and engaged communities across the cybersecurity ecosystem**	Activities 1 to 9	Art.5 to Art.12	Empowered ecosystem encompassing Member States authorities, EU institutions, agencies and bodies, associations, research centres and universities, industry, private actors and citizens, who all play their role in making Europe cyber secure	Community-building across the cybersecurity ecosystem	Additional quantitative measures stemming from the stakeholder strategy that will be developed in 2021 Stakeholder satisfaction of ENISA's role as facilitator of community-building and collaboration across the cybersecurity ecosystem
SO2 **Cybersecurity as an integral part of EU policies**	Activities 1 & 2	Art.5	Cybersecurity aspects are considered and embedded across EU and national policies	ENISA's added value to EU institutions, bodies and Member States in providing support to policy-making (ex-ante)	1. Number of relevant contributions to EU and national policies and legislative initiatives 2. Number of references to ENISA reports, analysis and/or studies in EU and national policy documents 3. Satisfaction with ENISA added-value and weight of contributions (survey)
			• Consistent implementation of Union policy and law in the area of cybersecurity • EU cybersecurity policy implementation reflects sectorial specificities and needs • Wider adoption and implementation of good practices	Contribution to policy implementation and implementation monitoring at EU and national level (ex-post)	1. Number of EU policies and regulations implemented at national level supported by ENISA 2 Number of ENISA reports, analysis and/or studies referred to at the EU and national level (survey) 3 Satisfaction with ENISA added-value and weight of support (survey)
SO3 **Effective cooperation amongst operational actors within the Union in case of massive[7] cyber incidents**	Activities 4 & 5	Art.7	• All communities (EU Institutions and MS) use rationalised and coherent set of SOPs for cyber crises management • Efficient framework, tools and methodologies for effective cyber crisis management	Effective use of ENISA's tools, platforms and take up of SOPs in operational cooperation	1. Number of users both new and recurring and usage per platform/ tool/ SOPs provided by ENISA 2. Uptake of the platform/ tool/ SOPs during massive cyber incidents 3. Stakeholder satisfaction on the relevance and added value of the platforms/ tools/ SOPs provided by ENISA
			• Member States and institutions cooperating effectively during large scale cross border incidents or crises • Public informed on a regular basis of important cybersecurity developments • Stakeholders aware of current cybersecurity situation	ENISA ability to support response to massive cyber incidents	1. Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents ENISA contributes to mitigate 2. Stakeholders' satisfaction of ENISA's ability to provide operational support

[7] large scale and cross-border

SO4 **Cutting-edge competences and capabilities in cybersecurity across the Union**	Activities 3 & 9	Art.6 and Art.7(5)	• Enhanced capabilities across the community • Increased cooperation between communities	Increased resilience against cybersecurity risks and preparedness to respond to cyber incidents	1. Increase/decrease of maturity indicators 2. Outreach, uptake and application of lessons learnt from capability-building activities. 3. Number of cybersecurity programmes (courses) and participation rates 4. Stakeholder assessment on usefulness, added value an relevance of ENISA capacity building activities
		Art.10 & Art.12	• Greater understanding of cybersecurity risks and practices • Stronger European cybersecurity through higher global resilience.	Level of awareness on cybersecurity, cyber hygiene and cyber literacy across the EU	1. Number of activities and participation to awareness raising actions organised by ENISA on cybersecurity topics 3. Level of awareness, on cybersecurity across the EU/ general public (e.g. EU barometer)
SO5 **High level of trust in secure digital solutions**	Activities 6 & 7	Art.8	Candidate cybersecurity certification schemes under the European cybersecurity certification framework are adopted Successful transition to the EU cybersecurity certification framework Certified ICT products, services and processes are preferred by consumers and where relevant, Operators of Essential Services or Digital Service Providers	Uptake of the European cybersecurity certification framework and schemes as an enabler for secure digital solutions Effective preparation of candidate certification schemes prepared by ENISA	1. Number of stakeholders (governments or commercial solution providers) on the EU market using the cybersecurity certification framework for their digital solutions 2. Stakeholders trust in digital solutions of certification schemes (Citizens, public sector, businesses) 3. Satisfaction with ENISA's support in the preparation of candidate schemes (survey)
			• Where relevant, contribution towards a more competitive European cybersecurity industry, SMEs and start-ups	Recognition of ENISAs supporting role for participants in the European cybersecurity market	1. Number of market analysis, guidelines and good practices issued by ENISA 2. Uptake of lessons learnt / recommendations from ENISA reports 3. Stakeholder satisfaction with the added value and quality of ENISA's work
SO6 **Foresight on emerging and future cybersecurity challenges**	Activity 8	Art.11	• Decisions about cybersecurity are future proof and to take account the trends, developments and knowledge across the ecosystem • Stakeholders receive relevant and timely information for policy and decision making	ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge	1. Number of users and frequency of usage of dedicated portal (observatory) 2 Number of recommendations, analysis, challenges identified and analysed 3 Stakeholder satisfaction on the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity

					challenges & opportunities (incl in research)
SO7 **Efficient and effective cybersecurity information and knowledge management for Europe**	Activity 8	Art.9	• Research and innovation agenda tied to the cybersecurity needs and requirements	ENISA's ability to contribute to Europe's research and innovation agenda	1. Number of requests from Member States and EU research and innovation entities to contribute, provide advice or participate in activities. 2. Stakeholder satisfaction on the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges & opportunities (incl in research)

The strategy of ENISA also establishes a set of values which guide the execution of its mandate and its functioning, namely:

Community Mind-Set ENISA works with communities, respecting their competencies and expertise, and fosters synergies and trust to best achieve its mission.

Excellence ENISA aims for state-of-the-art expertise in its work, upholds the highest quality standards of operation and evaluates its performance to strive for continuous improvement through innovation and foresight.

Integrity/ethics ENISA upholds ethical principles and EU relevant rules and obligations in its services and working environment ensuring fairness and inclusiveness.

Respect ENISA respects fundamental European rights and values covering all its services and working environment, as well as the expectations of its stakeholders.

Responsibility ENISA assumes responsibility thus ensuring integration of the social and environmental dimensions into practices and procedures.

Transparency ENISA adopts procedures, structures and processes that are open, factual and independent, thus limiting bias, ambiguity, fraud and obscurity.

Those values are built on the ethos of the CSA, and in particular the objectives set out in Articles 3(4) and 4(1), and have been encapsulating into two corporate objectives, which form the baseline from which the multiannual activities of the SPD will be delivered.

The corporate objective of **sound resource and risk management** is derived from requirements in Art 4(1) of the CSA that sets an objective for the Agency to: "be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying

out its tasks". In addition, the inspiration for this corporate objective stems from the values of **Excellence** and **Transparency** derived from the ENISA strategy and the principle of **Efficiency** set out in MB decision 2020/5 on the principles to be applied for organising ENISA. This aims for ENISA to uphold the highest quality of standards, strive for continuous improvement and enhance the organisation's performance.

The corporate objective of **building an agile organisation focused on people** is derived from requirements in Art 3(4) of the CSA which obliges the Agency to: "develop its own resources, including /…/ human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation". In addition, the inspiration for this corporate objective stems from the values of **Responsibility** and **Respect** derived from the ENISA strategy and the principle of **Competences** set out in MB decision 2020/5 on the principles to be applied for organising ENISA. This aims for ENISA to respect fundamental European rights and values in its working environment, assume responsibility for social and environmental dimensions of its procedures and to develop its staff competences, expertise and talent.

CORPORATE OBJECTIVE	ACTIVITY TO ACHIEVE OBJECTIVE	ARTICLE OF THE CSA	EXPECTED RESULTS	KPI	METRICS
Sound resource and risk management	Activity 10	Art 4(1)	Maximize quality and value provided to stakeholders and citizens Building lasting credibility and trust	1.Organisational performance 2. Trust in ENISA brand	1. Proportion of KPI's reaching targets 2. Individual contribution to achieving the objectives of the agency via clear link to KPI's (CDR report) 3. Exceptions in Risk Register 4. Number of complaints filed against ENISA incl number of inquiries/ complaints of the EU Ombudsman 5. Results of annual risk assessment exercise 6. Observations from external audit bodies (e.g. ECoA) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings 7. Level of trust in ENISA increases (survey)
Build an agile organisation focused on people	Activity 11	Art 3(4)	ENISA as an employer of choice	Staff commitment, motivation and satisfaction	1. Staff satisfaction survey (incl attractiveness of ENISA as employer, staff empowerment, organisational culture, opportunities on internal mobility, work-space, -environment and -tools) 2. Quantity and quality of ENISA training and career development activities organised for staff 3.Reasons for staff departure (exit interviews) 4.Staff retention/turnover rates 5.Resilience and quality of ENISA IT systems and services (including ability to consistently increase satisfaction with IT services & tools)

2. HUMAN AND FINANCIAL RESOURCE - OUTLOOK FOR YEARS 2022 – 2024

2.1 OVERVIEW OF THE PAST AND CURRENT SITUATION

In 2020 the Agency embarked on a large-scale call for expression of interest for temporary agents (TA) and contract agents (CA) following a novel approach, with the aim of creating a sufficiently diverse and broad reserve shortlist of candidates with more transversal competences and skills that could be used to recruit staff thus fill the gaps in the current establishment plan, as well as serve as a pool of candidates for the establishment plan in 2021 and 2022 if necessary. The key challenge that he Agency had to overcome was threefold, on one hand it had to mitigate the delay in recruitment from past years and on the other hand it had to meet the goals of the establishment plan following the adoption of the Regulation and thirdly plan the reorganisation of the Agency in 2020. Clearly there was urgency involved that called for appropriate action. The situation was exacerbated by the onset of the pandemic that eliminated physical meetings and required the swift adaptation of the recruitment procedures. The call, which was accompanied by a widespread promotion campaign, attracted 1 173 candidates for TA posts and 590 for CA posts from across all Member States. This has already resulted in a reserve shortlist of 69 candidates for TA posts and for CA posts 15 in reserve shortlist. The table below represents the results of the recruitment exercise for both the temporary agent and contract agent call.

Category		Number of eligible applications			Number of candidates put on a reserve lists			Number of candidates recruited[8]		
Member State	Gender	TA call	CA call	Managers	TA call	CA call	Managers	TA call	CA call	Managers
Austria	Male	6		2						
	Female	1		1						
Belgium	Male	13	2	5	2		1			1
	Female	9	4	1						
Bulgaria	Male	11	6	2	1					
	Female	17	5		1					
Croatia	Male	4	3		1					
	Female	2	1	1						
Cyprus	Male	13	6	3						
	Female	7	5	4		1				
Czech	Male	6	5	1						
	Female	1		2						
Danish	Male	1								
	Female									
Dutch	Male	7	1	2	1			1		
	Female	2								
Estonian	Male	7	3							

[8] The numbers include the offers sent and accepted as of 14.12.2020

	Female	3								
Finland	Male	3	1	2						
	Female	6								
French	Male	25	8	8	1			1		
	Female	15	10	2	1			1		
Greece	Male	411	199	90	30	3		2		
	Female	254	182	42	9	4	1	2		1
Germany	Male	16	2	4	2	1	1	1		
	Female	5	1	1						
Hungary	Male	5	2	1						
	Female	3	2							
Ireland	Male	7	2							
	Female	2								
Italian	Male	79	35	18	2	3	2			
	Female	36	21	2	3	1				
Latvia	Male	5								
	Female	3	4	2			1			1
Lithuanian	Male	3								
	Female	3								
Luxembourg	Male	1	1							
	Female	1								
Maltese	Male	3	1	2						
	Female	1								
Polish	Male	15	9	2		1			1	
	Female	11	7	1	1	1		1		
Portuguese	Male	16	6	2	3		1			
	Female	7	1	1	1					
Romanian	Male	24	8	3	3			1		
	Female	24	12	2	1			1		
Spanish	Male	42	13	10	5		1			
	Female	19	12	1						
Slovakian	Male	2	2	1						
	Female	3	1							

Swedish	Male	5	2	2						
	Female	1		5						
Slovenian	Male	3	2	1						
	Female	4	3							

2.2 OUTLOOK FOR THE YEARS 2022 – 2024

2.3 RESOURCE PROGRAMMING FOR THE YEARS 2022 – 2024

2.3.1 Financial Resources

The evolution of the planned total EU contribution for 2021–2023, as well as for the full period of the new multiannual financial framework 2021–2027, is not yet available. As part of the CSA, the estimated impact on expenditure was indicated for the period 2019–2022, which is presented in the table 4 below. Average growth during 2019–2022 is expected to be 12 %. A similar growth trend is expected for 2023.

Table 1

	2019	2020	2021	2022
Total appropriations for ENISA ***(thousand EUR)***	16 550	21 683	23 433	24 227

95 % of ENISA's revenue in 2019 came from the EU contribution, 2 % was from the European Free Trade Association (EFTA) country contribution and 3 % was from other contributions (Table 6 in Annex III). A similar trend is expected for 2021–2023. The EU contribution for 2021 is estimated to be EUR 22.3 million, the EFTA contribution is estimated to be EUR 0.5 million and other contributions, mainly from the Hellenic Authorities, are expected to be EUR 0.6 million.

The general allocation of funds across titles is expected to remain at a similar level in 2021–2023 to that in 2019 (Table 8 in Annex III). Expenditure in 2020 is expected to be EUR 21.7 million, of which EUR 11.2 million in Title 1 covers all staff-related costs, EUR 3.2 million in Title 2 covers main items such as building rental and ICT expenses, and EUR 7.3 million in Title 3 covers all core operating expenditure.

Taking into account the implementation of its founding Regulation, the Agency does not expect to request an increase in financial resources in the said period. Any important increase in tasks, would need to be quantified and if occurring in this period it might give grounds to a request before the Budgetary Authority for an increase in allocated resources.

2.3.2 Human Resources

The Agency expects to dutifully implement the entire scope of it Regulation within the boundaries of resources currently allocated. There is scope for further consideration nevertheless as the Agency would perform optimally had

it benefited from the unequivocal support of competent public authorities in the Member States. As such increasing the overall number of Seconded National Experts emerges as a viable opportunity in 2022 onwards. At a time when cybersecurity policy matures further it is necessary to continue providing the Member States authorities with the opportunity to get a first-hand view on the way the Agency implements the provisions of the Regulation at the day to day level. As such the increased presence of Seconded National Experts is hereby proposed as a viable and cost effective instrument to increase the visibility and input of the public authorities to the execution of the day to day tasks in ENISA. A range of new tasks could benefit thereto, notably in the areas of operational cooperation, certification, etc.

2.4 STRATEGY FOR ACHIEVING EFFICIENCY GAINS

ENISA is committed to continuously implement measures to obtain efficiency gains in all activities. In 2021 the ENISA organisational structure is being implemented to follow the principles of sound budgetary management and build efficiencies in both executing its core mandate as well as in fulfilling its corporate functions. Also the Agency continues to implement its work programme by systematic use its statutory bodies (NLO Network, ENISA Advisory Group), as well as other statutory groups ENISA is involved in (SCCG as set out in CSA Art. 22, NISD Cooperation Group and its work-streams, expert groups created under the Union law) and its own ad hoc expert groups, where appropriate to peer-review the scope and direction of actions undertaken to implement outputs, as well as validate the results. This way the Agency will fulfil its obligation is outlined in Article 3(3) of the CSA, to avoid the duplication of Member State activities and taking into consideration existing Member State expertise. Hence, all activities enlisted under section 3.1. and 3.2. in this SPD contain an indication of how specific deliverables and other actions undertaken to fulfil the outputs will be validated and peer-reviewed or consulted as per legal framework in the area of certification.

In 2021 the framework for structured cooperation with CERT-EU to utilise synergies and avoid duplication of activities in executing its task in the field of operational cooperation (Art 7 of the CSA) is being implemented and a local office in Brussels established in 2021 should further enable the Agency to further create synergies with other EU Institutions, agencies and bodies within and beyond these activities. The Agency is also pursuing cooperation with relevant Union bodies (JRC) and will embark to create synergies with the Cybersecurity Competence Centre and Network once it is established to pursue synergies in fulfilling its tasks in the field of research and innovation (Article 11 of the CSA).

In its corporate functions, ENISA further seeks to rationalise its internal processes to improve its overall efficiency and to benchmark its activities with the best practices implemented by other EU Institutions and Agencies. The Agency is continuing and further expanding the sharing of services among other EU agencies. A number of collaborations and agreements are currently in place (EUIPO) and in 2021 the Agency signed a cooperation plan with EU-LISA.

Prompted by the COVID-19 crisis, the Agency established efficiency gains through digitalisation of its functions. It is already using the EU Tools such as ABAC; ABAC assets; Procurement; E-invoicing. Furthermore in 2020, the Agency deployed Sysper and in 2021 the migration of its services to other tools, such as MIPS and ARES are foreseen. Most of the administrative tasks are already supported by the application “Paperless” and others that are significant steps for the aimed 100% e-administration. E-trainings are also internally encouraged with the aim, among others, to reduce the associated costs from “class-room” training (traveling costs, etc…).

With the COVID-19 travel restrictions in place, in 2020 the Agency has established series of events and webinars to external parties and will upgrade its capabilities to use secure digital conferencing across the field, providing further opportunities in efficiency gains as well as expanding the scale and scope of its activities.

SECTION III. WORK PROGRAMME 2022

This is the main body of the Work Programme describing, per operational and corporate activity, what the agency aims to deliver in the respective year towards achieving its strategy and the expected results. In total 9 operational activities and 2 corporate activities have been identified to support the implementation of ENISA's mandate in 2022.

3.1 OPERATIONAL ACTIVITIES

Activity 1 Providing assistance on policy development

OVERVIEW OF ACTIVITY

The activity delivers assistance and advice to the EU and Member States in developing cybersecurity policy and sector-specific policy and law initiatives where matters related to cybersecurity are involved and on the basis of the new 2020 EU Cybersecurity Strategy.

The activity seeks to bolster policy initiatives on novel/emerging technology areas by providing technical, fact-driven and tailor-made cybersecurity advice and recommendations. In addition to support in emerging policy areas (such as AI, 5G, EU eID, quantum computing, blockchain, big data digital resilience and response to current and future crises), ENISA – in coordination with the EC and MSs - will also conduct policy scouting to support them in identifying potential areas in policy development, as well as develop monitoring capabilities and tools to regularly and consistently be able to give advice on the effectiveness of the existing Union policy and law in accordance with the EU's institutional competencies in this area.

The added value of this activity is to support the decision makers in a timely manner on developments at the technological, societal and economic market levels which might affect the cybersecurity policy framework (see also Activity 8). Given the cross-cutting nature of cybersecurity across the policy landscape, the activity will provide an up-to-date risked based analysis of cybersecurity not only in the areas of critical infrastructure and sectors, but also by providingadvice across the field in an integrated and holistic manner. The legal basis for this activity is Article 5 of the CSA.

OBJECTIVES

- Foster cybersecurity as an integral part of EU policy (existing and new)
- Ensure that EU policy makers are regularly informed about the effectiveness of existing cybersecurity policy frameworks
- Ensure that EU policy makers are regularly informed about the effectiveness of the existing framework EU policy makers and stakeholders are provided with timely and tailor-made policy recommendations on future cybersecurity challenges and opportunities

RESULTS	LINK TO STRATEGIC OBJECTIVE (ENISA STRATEGY)
Cybersecurity aspects are considered and embedded across EU and national policies	Cybersecurity as an integral part of EU policies
OUTPUTS	**KPI**
1.1 Issue reports, studies and analyses on the effectiveness of the current cybersecurity policy frameworks 1.2 Carry out preparatory work and provide the EC and MSs with tailor-made advice and recommendations on new policy initiatives in emerging technological, societal and economic trends, such as Artificial Intelligence, 5G, eID, digital operational resilience in the finance sector and cyber insurance and other potential initiatives (e.g. The Once Only Technical Solution) 1.3 Assist the Commission in reviewing existing policy initiatives	**Indicator:** ENISA's added value to EU institutions, bodies and Member States in providing support to policy-making (ex-ante) **Metric:** 1.1 Number of relevant contributions to EU and national policies and legislative initiatives 1.2 Number of references to ENISA reports, analysis and/or in EU and national policy documents 1.3 Satisfaction with ENISA added-value and weight of contributions (survey) **Frequency:** Annual (1.1 & 1.2), bi-annual (1.3)
VALIDATION	**TARGET GROUPS AND BENEFICIARIES**
• NIS Cooperation Group (NIS CG) and other formally established Groups (outputs 1.1 & 1.2) • ENISA ad hoc working groups[9] (output 1.2) • NLO Network and ENISA Advisory Group and other formally established expert group (when necessary)	EU and national policy making institutions; EU and national experts (NIS CG, relevant/competent EU or MS-organisations/bodies)

RESOURCES PLANNED

[9] created under Art 20(4) of CSA

Human Resources (FTE)[10]			Financial Resources [11]	EUR
Total	6		Total	316.023,93

Activity 2 Supporting implementation of Union policy and law

OVERVIEW OF ACTIVITY

The activity provides support to MS and EU Institutions in the implementation of European cybersecurity policy and legal framework and advice on specific cybersecurity aspects related to the 2020 EU's Cybersecurity Strategy, NIS Directive, telecom and electronic communications security, data protection, privacy, eID and trust services, incident notification and the general availability or integrity of the public core of the open internet.

It further supports initiatives related to implementation of policy frameworks on novel digital technologies such as 5G (e.g. 5G security toolbox) and assisting the work of the NIS Cooperation Group and its work streams.

An ENISA contribution towards the Commission's regular monitoring of the implementation of specific EU policies is envisaged, which considers relevant indicators and could contribute to possible indices which could capture the maturity of relevant cybersecurity policies, and provide input to the review of existing policies (Output 1.3)

This activity helps to avoid fragmentation and supports a coherent implementation of the Digital Single Market across Member States.

The legal basis for this activity is Article 5 and Article 6 (1)b of CSA.

OBJECTIVES

- Align horizontal cyber security policies with sectorial polices to avoid implementation inconsistencies
- Contribute to the efficient and effective monitoring of EU cybersecurity policy implementation in MS
- Effective implementation of cybersecurity policy across the Union and harmonization of MS laws, regulations and administrative provisions related to cybersecurity
- Improved cybersecurity practices taking on board lesson learned from incident reports

RESULTS	Link to strategic objective (ENISA STRATEGY)
• Consistent implementation of Union policy and law in the area of cybersecurity • EU cybersecurity policy implementation reflects sectorial specificities and needs • Wider adoption and implementation of good practices	• Cybersecurity as an integral part of EU policies • Empowered and engaged communities across the cybersecurity ecosystem
OUTPUTS	**KPI**
2.1 Support the NIS Cooperation Group and Work Streams as per NIS CG work programme 2.2 Support MS and Commission in the implementation of the 5G toolbox and its individual actions 2.3 Provide advice, Issue technical guidelines and facilitate exchange of good practices (depending on subject matter) to support MS and EC on the implementation of eID, trust services, EECC and its implementing acts, as well as security measures for data protection and privacy 2.4 Assisting in establishing and implementing vulnerability disclosure policies considering also the NIS2 proposal. 2.5 Analyse and report on incidents as required by Art 5(6) of CSA	**Indicator:** Contribution to policy implementation and implementation monitoring at EU and national level (ex-post) **Metric:** 2.1 Number of EU policies and regulations implemented at national level supported by ENISA 2.2 Number of ENISA reports, analysis and/or studies referred to at the EU and national level (survey) 2.3 Satisfaction with ENISA added-value and weight of support (survey) **Frequency:** Annual (1), bi-annual (2 and 3)
VALIDATION	**TARGET GROUPS AND BENEFICIARIES**
• NIS Cooperation Group or established work streams (output 2.1. 2.2.) • Art19 and Art 13a expert groups (output 2.3.) • Formally established bodies and expert groups as necessary (output 2.3, 2.4, 2.5) • NLO Network (as necessary)	• MS Cybersecurity Authorities (NISD CG members), National Supervisory Authorities, Data Protection Authorities, National Accreditation Bodies • EC, EU Institutions/ bodies (e.g. BEREC, EDPS, EDPB, ERA, EMSA) and sectorial EU Agencies (e.g. ACER) and Interinstitutional Committees (e.g. ICTAC, ICDT) • Art. 13a and Art. 19 Expert Group members • EU Citizens • Conformity Assessment Bodies and Trust Service Providers • Operators of Essential Services, including their associations and networks

[10] Indicative forecast, FTE to be updated at a later stage
[11] Indicate forecast, Budget to be updated at a later stage

RESOURCES PLANNED				
Human Resources (FTE)			**Financial Resources**	EUR
Total	14		**Total**	1.036.191,31

Activity 3 Building capacity

OVERVIEW OF ACTIVITY

This activity seeks to improve and develop the capabilities of Member States, Union Institutions, bodies, and agencies, as well as various sectors, to respond to cyber threats and incidents, raise resilience and increase preparedness across the Union. Actions to support this activity include organising large scale exercises, sectorial exercises and trainings, including CSIRT trainings. In addition the activity seeks to develop and raise CSIRT capabilities, support information sharing within the cybersecurity ecosystem and assist in reviewing and developing national and Union level cybersecurity strategies, including cross-border.

The legal basis for this activity is Articles 6 and 7(5) of the CSA.

OBJECTIVES

- Increase the level of preparedness and cooperation within and between Member States and sectors and EU institutions, bodies and agencies
- Prepared and tested capabilities to respond to cybersecurity incidents
- Foster interoperable European risk management, consistent methodology and risk assessment practices
- Increase skill sets and align cybersecurity competencies
- Increase the supply of skilled professionals to meet market demand, and promote cybersecurity education

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Enhanced capabilities across the community • Increased cooperation between communities	• Cutting-edge competences and capabilities in cybersecurity across the Union • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	KPI
3.1 Assist MS to develop National Cybersecurity Strategies 3.2 Organise large scale bi-annual exercises and sectorial exercises (incl Cyber Europe, BlueOLEx, CyberSOPEx etc) including through cyber ranges 3.3 Organise trainings and other activities to support and develop maturity and skills of CSIRTs (incl. NISD sectorial CSIRT) and other communities 3.4 Develop coordinated and interoperable risk management frameworks 3.5 Support the capacity building activities of Cooperation Group and Work Streams as per NIS CG work programme 3.6 Support European Information Sharing schemes based on ISACs through the CEF core service platforms, SOCs, PPPs and other existing mechanisms. 3.7 Organise and support cybersecurity challenges 3.8 Report on cybersecurity skills needs and gaps, and support skills development, maintenance and implementation (incl. Digital Education Action Plan and a report on higher-education programmes)	**Indicator:** increased resilience against cybersecurity risks and preparedness to respond to cyber incidents **Metric:** 3.1 Increase/decrease of maturity indicators 3.2 Outreach, uptake and application of lessons learned from capability-building activities. 3.3 Number of cybersecurity programmes (courses) and participation rates 3.4 Stakeholder assessment on usefulness, added value and relevance of ENISA capacity building activities. (Survey) **Frequency:** 1, 2 & 3 Annual, 4 Bi-annual

VALIDATION	TARGET GROUPS AND BENEFICIARIES
• NLO Network (as necessary) • CSIRTs Network, (output 3.3.) • CyCLONe members (as necessary) • NIS Cooperation Group (output 3.6)	• Cybersecurity professionals • EU Institutions and bodies • Private industry sectors (operators of essential services such as health, transport etc.) • CSIRTs Network and related operational communities • European ISACs • CyCLONe members

RESOURCES PLANNED				
Human Resources (FTE)			**Financial Resources**	EUR
Total	15		**Total**	1.460.119,64

Activity 4 Enabling operational cooperation

OVERVIEW OF ACTIVITY

The activity supports operational cooperation among Member States, Union institutions, bodies, offices and agencies and between operational activities. Actions include establshing synergies with the different national cybersecurity communities (including the civilian, law enforcement, cyber diplomacy and cyber defence) and EU actors notably CERT-EU with the view to exchange know how, best practices, provide advice and issue guidance.

In addition the activity supports Member States with respect to operational cooperation within the CSIRTs network by advising on how to improve capabilities and providing support to ex-post technical inquiries regarding incidents.

Under this activity ENISA is supporting operational communities through helping to develop and maintain secure and highly available networks / IT platforms and communication channels in particular ensuring maintenance, deployment of the MeliCERTes platform.

ENISA will engage in the development of a future JCU, along the lines and the role defined at EU policy level in due course.

The legal basis for this activity is Article 7 of the CSA.

OBJECTIVES

- Enhance and improve incident response capabilities across the Union
- Enable effective European cybersecurity crisis management by continuously improving the cyber crisis management framework
- Improve maturity and capacities of operational communities (incl CSIRTs network, CyCLONe group)
- Contribute to preparedness, shared situational awareness and coordinated response and recovery to large scale cyber incidents and crises across different communities (e.g. through engagement in the development phase of a future Joint Cyber Unit)

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• All communities (EU Institutions and MS) use rationalised and coherent set of SOPs for cyber crises management • Efficient framework, tools (secure & high availability) and methodologies for effective cyber crisis management	• Effective cooperation amongst operational actors within the Union in case of massive cyber incidents • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	KPI
4.1. Support the functioning and operations of the CSIRTs Network (also through MeliCERTes), CyCLONe and Cyber Crisis Management in the EU including cooperation with relevant Blueprint stakeholders (e.g Europol, CERT EU, EEAS and EDA 4.2. Develop and enhance standard operating policies, procedures, methodologies and tools for cyber crisis management (potentially related to a future JCU). 4.3 Maintain and deploy MeliCERTes platform	**Indicator:** Effective use of ENISA's tools, platforms and take up of SOPs in operational cooperation **Metric:** 4.1Number of users both new and recurring and usage per platform/ tool/ SOPs provided by ENISA 4.2 Uptake of the platform/ tool/ SOPs during massive cyber incidents 4.3 Stakeholder satisfaction on the relevance and added value of the platforms/ tools/ SOPs provided by ENISA. (Survey) **Frequency:** 1 & 2 annual and 3 bi-annual

VALIDATION	TARGET GROUPS AND BENEFICIARIES
• Management Board (output 4.2.) • NLO Network (as necessary) • CSIRTs Network and CyCLONe (output 4.1.)	• Blueprint stakeholders • EU decision makers, institutions, agencies and bodies • MS CSIRTs Network Members • NISD Cooperation Group • OESs and DSPs

RESOURCES PLANNED

Human Resources (FTE)			Financial Resources	EUR
Total	10		**Total**	1.163.880,57

Activity 5 Contribute to cooperative response at Union and Member States level

OVERVIEW OF ACTIVITY

The activity contributes to developing a cooperative response at Union and Member States level to large scale cross border incidents or crises related to cybersecurity by aggregating and analyzing reports to establish a common situational awareness, ensuring information flow and escalation measures between CISRTs network and technical, operational and political decision makers at Union level .

In addition, the activity can include, at the request of Member states facilitating the handling of incident or crises, public communication related to such incidents or crisis and testing cooperation plans for such incidents or crises. Supporting Union institutions, bodies, offices and agencies in public communication to incidents and crises. The activity also supports Member States with respect to operational cooperation within the CSIRTs network by providing advice to a specfic cyber threat, assisting in the assessment of incidents, facilitating technical handling of incidents, supporting cross-border information sharing and analyzing vulnerabilities.

Moreover the activity seeks to engage with CERT-EU in structured cooperation. The legal basis for this activity is Article 7 of the CSA

OBJECTIVES

- Effective incident response and cooperation amongst Member States and EU institutions, incl cooperation of technical and political actors during incidents or crisis
- Common awareness on cyber incidents and crisis across the Union
- Information exchange and cooperation, cross layer and cross border between Member States and as well as with EU institutions

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Member States and institutions cooperating effectively during large scale cross border incidents or crises • Public informed of important cybersecurity developments • Stakeholders aware of current cybersecurity situation	• Effective operational cooperation within the Union in case of massive (large-scale, cross-border) cyber incidents • Empowered and engaged communities across the cybersecurity ecosystem
OUTPUTS	**KPI**
5.1. Generate and consolidate information (incl to the general public) on cyber situation awareness, technical situational reports, incident reports, threats and support consolidation and exchange of information on strategic, tactical and technical levels 5.2. Support technical (including through MeliCERTes) and operational cooperation, incident response coordination during crisis and activities with the CSIRTs Network, the CyCLONe and Blueprint stakeholders (e.g and CERT-EU, EC3, EEAS and EDA and provide assistance and support on the basis of Art 7 (4) and (7) of the CSA 5.3. Support EU wide crises communication	**Indicator:** ENISA ability to support response to massive cyber incidents **Metric:** 5.1 Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents ENISA contributes to mitigate (Survey) 5.2 Stakeholders' satisfaction of ENISA's ability to provide operational support (Survey) **Frequency:** 1 & 2 bi-annual
VALIDATION	**TARGET GROUPS AND BENEFICIARIES**
• Blueprint actors	• EU Member States (incl CSIRTs Network members and CyCLONe) • EU Institutions, bodies and agencies • Other type of CSIRTs and PSIRTs

RESOURCES PLANNED

Human Resources (FTE)			Financial Resources	EUR
Total	9		**Total**	1.255.816,83

Activity 6 Development and maintenance of EU cybersecurity certification framework

OVERVIEW OF ACTIVITY

This activity emcompasses actions to develop draft candidate cybersecurity certification schemes to impement the EU cybersecurity certification framework. The Agency takes action in line with Article 49 of the CSA, at the request of the Commission or on the basis of the Union Rolling Work Program. Actions also include evaluating adopted certification schemes (such as schemes for common criteria and cloud services once adopted) and participating in peer reviews. In addition the activity assists the Commission in the ECCG, co-chairing and supporting the secretariat of the SCCG and maintaining a dedicated European cybersecurity certification website.

The legal basis for this activity is Article 8 and Title III Cybersecurity certification framework of the CSA.

OBJECTIVES

- Trusted ICT products, services and processes
- Increase use and uptake of European cybersecurity certification
- Efficient and effective implementation of the European cybersecurity certification framework

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Draft cybersecurity certification schemes developed by ENISA under the European cybersecurity certification framework are adopted • Smooth transition to the EU cybersecurity certification framework • Certified ICT products, services and processes are preferred by consumers and where relevant, Operators of Essential Services or Digital Service Providers	• High level of trust in secure digital solutions) • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	KPI
6.1. Drafting and contributing to the establishment of candidate cybersecurity certification schemes 6.2. Implementation and maintenance of the established schemes including evaluation of adopted schemes, participation in peer review etc. 6.3. Support the statutory bodies in discharging carrying out their duties with respect to governance roles and tasks 6.4. Development and maintenance of necessary tools for making effective use of the Union's cybersecurity certification framework (incl. certification website, CEF core services platform for collaboration as appropriate, and publication, promotion of the implementation of the cybersecurity certification framework etc.)	**Indicator:** 1. Uptake of the European cybersecurity certification framework and schemes as an enabler for secure digital solutions. 2. Effective preparation of candidate certification schemes prepared by ENISA **Metric:** 6.1 Number of stakeholders (public authorities and/or commercial solution providers) on the EU market using the cybersecurity certification framework for their digital solutions 6.2 Stakeholders trust in digital solutions of certification schemes (citizens, public sector and businesses. (Survey) 6.3 Satisfaction with ENISA's support in the preparation of candidate schemes (survey) **Frequency:** 1 annual, 2 and 3 bi-annual

VALIDATION	TARGET GROUPS AND BENEFICIARIES
• Ad hoc certification expert groups (output 6.1.) • ECCG (6.1.-6.2.) • European Commission (outputs 6.1.-6.3) • SCCG (output 6.3. and 6.4.)	• Public authorities, accreditation bodies at Member States & EU level, Certification Supervisory Authorities, Conformity Assessment Bodies, • Product manufacturers and service providers who have an interest in EU schemes for the certification of ICT products and services (industry) • The European Commission, other Institutions, Agencies and competent authorities (e.g. EDPB), public authorities in the Member States, the members of the ECCG and the SCCG

RESOURCES PLANNED

Human Resources (FTE)			Financial Resources	EUR
Total	12		**Total**	918.717,20

Activity 7 Supporting European cybersecurity market and industry

OVERVIEW OF ACTIVITY

The activity seeks to foster cybersecurity market (products and services) in the Union and the development of the cybersecurity industry and services, in particular SMEs and start-ups, to reduce dependence from outside the Union and to reinforce supply chains inside the Union. It involves actions to promote and implement 'security by design' and 'security by default' measures in ICT products, services and processes, including through standardisation. Actions to support this activity include compiling guidelines and good practices on cybersecurity requirements, facilitating the establishment and take up of European and international standards for risk management as well as performing regular analysis of cybersecurity market trends on both the demand and supply side including monitoring, collecting and identifying dependencies among ICT products, services and processes and vulnerabilities present therein. Platforms for collaboration among the cybersecurity market players, improve visibility of trustworthy and secure ICT solutions in the internal digital market.

In addition this activity supports cybersecurity certification by monitoring standardisations being used by European cybersecurity of certification schemes and recommending appropriate technical specifications where such standards are not available.

The legal basis for this activity is Article 8 and Title III Cybersecurity certification framework of the CSA.

OBJECTIVES

- Improve the conditions for the functioning of the internal market
- Foster a robust European cybersecurity industry and market

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Contribution towards understanding market dynamics. • A more competitive European cybersecurity industry, SMEs and start-ups	• High level of trust in secure digital solutions • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	KPI
7.1. Market analysis on the main trends in the cybersecurity market on both the demand and supply side 7.2. Monitoring developments in related areas of standardisation, analysis on standardisation gaps and establishment and take-up of European and international standards for risk management in relation to certification 7.3. Guidelines and good practices on cybersecurity certification requirements for ICT products, services and processes 7.4. Monitoring and documenting the dependencies and vulnerabilities of IICT products and services	**Indicator:** Recognition of ENISAs supporting role for participants in the European cybersecurity market **Metric:** 7.1 Number of market analysis, guidelines and good practices issued by ENISA 7.2 Uptake of lessons learnt / recommendations from ENISA reports 7.3 Stakeholder satisfaction with the added value and quality of ENISA's work (Survey) **Frequency:** 1,2 annual and 3 bi-annual

VALIDATION	TARGET GROUPS AND BENEFICIARIES
• SCCG (outputs 7.2. & 7.3.) • ENISA Advisory Group (output 7.1.) • NLO (as necessary) • ECCG (7.4) •	• European ICT industry, SME's, start-ups, product manufacturers and service providers • European standardisation organisations (CEN, CENELEC and ETSI) as well as international and industry standardisation organisations

RESOURCES PLANNED

Human Resources (FTE)			Financial Resources	EUR
Total	9		**Total**	530.541,87

Activity 8 Knowledge on emerging cybersecurity challenges and opportunities

OVERVIEW OF ACTIVITY

This activity shall provide strategic long-term analysis, guidance and advice on emerging technologies (such as in the area of artifitial intelligence, quantum, distributed ledgers, cloud computing, edge computing, software development, etc). On the basis of risk management frameworks, the Agency will identify cyber threats, vulnerabilities and risks, and map threat landscapes and provides topic-specific as well as general assessments on the expected societal, legal, economic and regulatory impact, as well as targeted recommendations to Member States and Union institutions, bodies, offices and agencies. In addition to this the activity will continue its effforts in developing the EU cybersecurity index. The activity also seeks to identify and give advice on research and innovation needs and priorities in the field of cybersecurity, and contribute to strategic agenda setting for cybersecurity research and innovation.

A key new component of this activity will be the contribution to the work of the Competence Centre and Network. This will include contributing to the development of the Cybersecurity Industrial, Technology and Research Agenda, and the respective work programmes. The Agenda and work programmes should be able to identify effective responses to current and emerging risks and cyber threats and new emerging technologies.

These activities leverage on expertise of relevant legal, regulatory, economic and society trends and data by aggregating and analysing information.

The legal basis for this activity is Article 9 and Article 11 of the CSA.

OBJECTIVES

- Identify and understand future cybersecurity challenges and opportunities and assess the interlinks between cybersecurity and relevant disrupting technologies in current and future digital transformation
- Increase Member States' and Union's resilience and preparedness in handling future cybersecurity challenges and opportunities
- Increase knowledge and information for specialised cybersecurity communities
- Understanding the current state of cybersecurity across the Union
- Link cybersecurity needs with the EU research & innovation agenda in the field of cybersecurity

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Decisions about cybersecurity are future proof and take account of the trends, developments and knowledge across the ecosystem • Stakeholders receive relevant and timely information for policy and decision-making • Research and innovation agenda tied to the cybersecurity needs and requirements	• Foresight on emerging and future cybersecurity challenges • Efficient and effective cybersecurity information and knowledge management for Europe • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	KPI
8.1 Develop EU cybersecurity index 8.2 Mapping and identifying threat landscapes using risk management frameworks. Analysing and providing recommendations on emerging challenges 8.3 Develop and maintain a portal (information hub), a one stop shop to organise and make available to the public information on cybersecurity, and establishment of procedural framework to support knowledge management activities maximising synergies with the European Cybersecurity Atlas 8.4 Support EU research & development programmes and activities of European competences centres in particular the Competence Centre and Network including the 4 EU pilot projects 8.5 Annual report with "ENISA Recommendations on Research and Innovation Needs and Priorities". 8.6 Advise on potential investment priorities (e.g. capacity building and market & industry) and emergent cyber technologies as part of the Competence Centre and Network work programme and Agenda	**Indicator:** ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge including into research and innovation agenda **Metric:** 8.1 Number of users and frequency of usage of dedicated portal (observatory) 8.2 Number of recommendations, analysis, challenges identified and analysed 8.3 Number of requests from Member States and EU research and innovation entities to contribute, provide advice or participate in activities. 8.4 Stakeholder satisfaction on the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges & opportunities incl in research (Survey) **Frequency:** 1,2 & 3 annual, 4 b-annual

VALIDATION	TARGET GROUPS AND BENEFICIARIES
• NLO Network • ENISA Advisory Group (as necessary) • ENISA ad hoc working group (as necessary) • The forthcoming European Cybersecurity Competence Center and Network of National Coordination Centers	• General public • Industry, research and academic institutions and bodies • EU and national decision making bodies and authorities

• Competence Centre Governing Board (output 8.6)	• European Cybersecurity Competence Centre & Network

RESOURCES PLANNED

Human Resources (FTE)			Financial Resources	EUR
Total	9		Total	1.209.848,70

Activity 9 Outreach and education

OVERVIEW OF ACTIVITY

The activity seeks to raise the overall awareness of cybersecurity risks and practices. in cooperation with Member States, Union institutions, bodies, offices and agencies and EU's international partners, it aims to build an empowered global community which can counter risks in line with the values of the Union. Under this activity the Agency will be organising regular outreach campaigns, providing guidance on best practices and support coordination across MS on awareness and education.

The added value of this activity comes from building global communities of stakeholders which improve and enhance current practices in cybersecurity by harmonizing and amplifying stakeholder actions.

The activity will also seek to contribute to the Unions efforts to cooperate with third countries and international organisations on cybersecurity.

The legal basis for this activity are Articles 10 and 12 and Article 42 of the CSA.

OBJECTIVES

- Elevate the understanding of cybersecurity risks and practices across the EU and globally
- Foster EU cybersecurity values and priorities

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Greater understanding of cybersecurity risks and practices • Stronger European cybersecurity through higher global resilience	• Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	KPI
9.1 Implement awareness raising framework 9.2 Implement ENISA international strategy and outreach 9.3 Organise European cybersecurity month (ECSM) and related activities 9.4 Support outreach activities or areas related to ENISA strategy 9.5 Activities to promote and ensure uptake of information on good cybersecurity practices (incl on Union strategies, security by design and privacy by design at Union level, cybersecurity certification schemes) throughout different target groups.	**Indicator:** Level of awareness on cybersecurity, cyber hygiene and cyber literacy across the EU **Metric:** 9.1 Number of activities and participation in awareness raising actions organised by ENISA on cybersecurity topics 9.2 Level of awareness on cybersecurity across the EU/ general public (e.g. EU barometer) **Frequency:** 1 & 2 annual, 3 bi-annual

VALIDATION	TARGET GROUPS AND BENEFICIARIES
• Management Board (for output 9.1. and 9.2.) • SCCG (for certification related issues under output 9.5) • NLO Network • ENISA Advisory Group (outputs 9.1. and 9.5.)	• Public, businesses and organisations • Member States, EU institutions, bodies and agencies • International partners

RESOURCES PLANNED

Human Resources (FTEs)			Financial Resources	EUR
Total	7		Total	561.729,00

1.2 CORPORATE ACTIVITIES

Activities 10 to 11 encompass enabling actions that support the operational activities of the agency.

Activity 10: Performance and risk management

OVERVIEW OF ACTIVITY

The activity seeks to achieve requirements set out in Art 4(1) of the CSA that sets an objective for the Agency to: "be a centre of expertise on cybersecurity by virtue of its **independence**, the scientific and technical **quality of the advice and assistance it delivers**, the information it provides, the **transparency of its operating procedures**, the **methods of operation**, and its **diligence in carrying out its tasks**". This objective requires an efficient performance and risk management framework, which should be developed and implemented Agency wide.

Under this activity ENISA will confinue to enhance key objectives of the reorganisation, as described in the MB decision No MB/2020/5., including the need to adress the gaps in the Agency's quality assessment framework, install proper and functioning internal controls and compliance checks, make best use of the internal resources of the Agency, impose of sound financial and budgetary management, and utilise internal and external synergies within ENISA. These aspects are addressed in the new organisational architecture, but should also be built into the daily operations of the Agency as guided by the Work Programme. Actions undertaken will ensure that Agency's outputs add real value, through making performance and ex-post and ex-ante evaluation integral to the Work Programme througout its lifecycle, including by rigorous quality assurance through proper project management, internal peer-reviews and independent audits and validations. Gaps in skills and trainings as well as resource planning will be reviewed and mitigated. The Agency will carry out a risk assessment of its organisational activities and IT systems and propose mitigation measures. The Agency will associate its main business processes with information systems that serve these processes and will produce a single registry of corporate processes (SOPs).

The legal basis for this activity is Art 4(1) and Art 32 of the CSA, the latter of which strongly focuses on the sound financial management principle with a view to maximise value to stakeholders.

OBJECTIVES

- Increased effectiveness and efficiency in achieving Agency objectives
- To be fully compliant with legal and financial frameworks in our performance (build a culture of compliance)
- Protect the Agencies assets and reputation, while reducing risks
- Full climate neutrality of all operations by 2030

RESULTS	Link to corporate objective:
Maximize quality and value provided to stakeholders and citizens Building lasting credibility and trust	Sound resource and risk management

OUTPUTS	KPI
10.1. Implementation of performance management framework 10.2. Implementation of communications strategy 10.3. Develop and implement risk management plans (including IT systems cybersecurity risk assessment, quality management framework and as well as relevant policies and processes. 10.4. Develop and monitor the implementation of Agency wide budgetary and IT management processes 10.5. Carry out relevant trainings and develop guidelines to staff in relation to efficient administrative practices and performance management 10.6. Carry out an overarching audit on the CO2 impact of the operations of the Agency and propose a targeted action plan	**Indicator**: Organisational performance culture **Indicator:** Trust in ENISA brand **Metrics:** 1 Proportion of KPI's reaching targets 2 Individual contribution to achieving the objectives of the agency via clear link to KPI's (CDR report) 3. Exceptions in Risk Register 4. Number of complaints filed against ENISA incl number of inquiries/ complaints of the EU Ombudsman 5. Results of annual risk assessment exercise 6. Observations from external audit bodies (e.g. ECoA) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings 7. Level of trust in ENISA increases (survey)

	Frequency: 1 to 6 annual, 7 bi-annual
VALIDATION	**TARGET GROUPS AND BENEFICIARIES**
• Management Team • Budget Management Committee • IT Management Committee • IPR Management Committee • Staff Committee • ENISA Ethics Committee	• Citizens • All stakeholders of the Agency

Activity 11 Staff development and working environment

OVERVIEW OF ACTIVITY

This activity seeks to support ENISA aspirations as stipulated in Art 3(4) which obliges the Agency to: "*develop its own resources, including /…/ human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation*".

Moreover, the impact of the pandemic has shed new light on remote working . The Agency will continue to look into flexible (50/50) working arrangements to better balance work requirements in a pragmatic manner.

The actions which will be pursued under this activity will focus on attracting retaining and developing talent and building ENISA's reputation as employer of choice and as an agile and knowledge based organisation where staff can evolve personally and professionaly, keeping staff engaged, motivated and with sense of beloging. The activity will seek to build an attractive workspace by establishing and maintain excellent working conditions (premises, layout of office space) and developing user-centric (tele)working and conferencing tools (incl IT systems and platfoms) delivering state of the art services and supporting ENISA's business owners and stakeholders in line with the Agency's objectives.

OBJECTIVES

- Engaged staff, committed and motivated to deliver, empowered to use fully their talent, skills and competences
- Digitally enabled work-place and environment (incl home work-space) which promotes performance and balances social and environmental responsibility

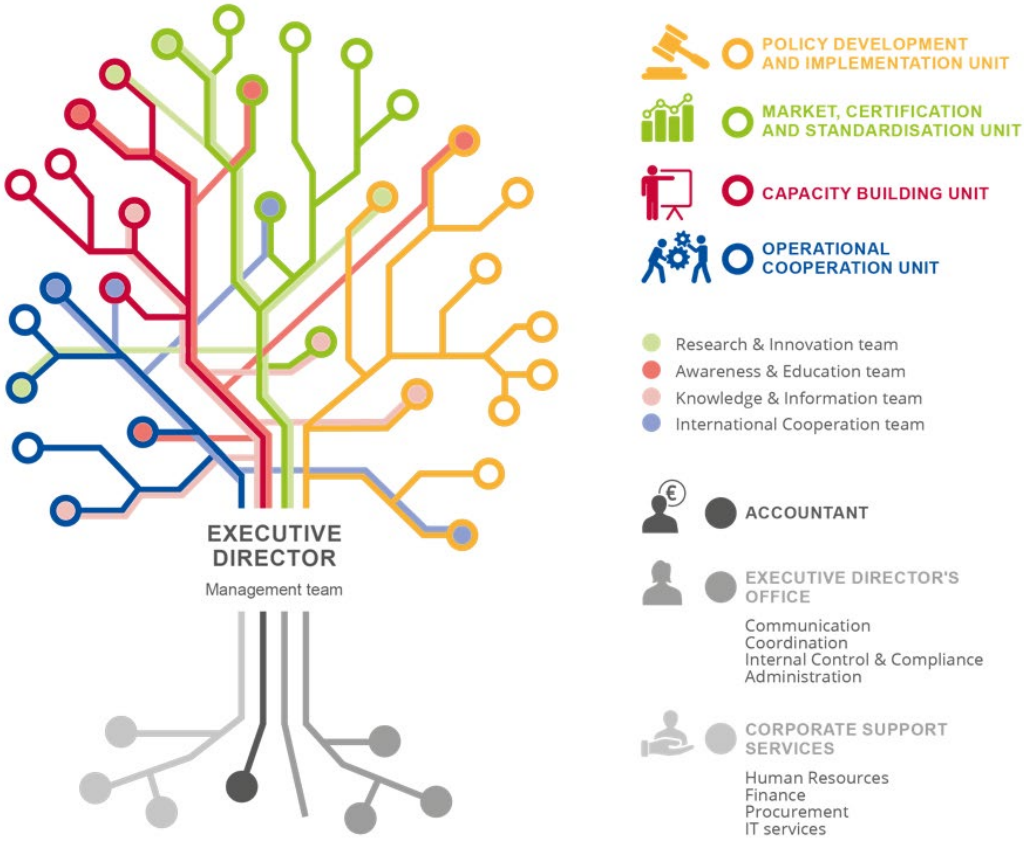
RESULTS	**Link to corporate objective:**
ENISA as an employer of choice	Build an agile organisation focused on people

OUTPUTS	**KPI**
11.1 Maintain and implement the competence framework into all HR processes (incl into training strategy, CDR, internal competitions, exit-interviews etc) 11.2 Develop HR Strategy with emphasis on talent development, growth and innovation 11.3 Undertake actions to develop and nourish talent and conduct necessary management development activities 11.4 Develop and maintain a user friendly and service oriented working environment (including digital tools and services) 11.5 Set up service provisions standards and provide quality support and services for ENISA staff, employees, corporate partners and visitors	**Indicator** Staff commitment, motivation and satisfaction **Metric**: 11.1 Staff satisfaction survey (incl attractiveness of ENISA as employer, staff empowerment, organisational culture, opportunities on internal mobility, work-space, -environment and -tools) 11.2 Quantity and quality of ENISA training and career development activities organised for staff 11.3 Reasons for staff departure (exit interviews) 11.3 Staff retention/turnover rates 11.5 Resilience and quality of ENISA IT systems and services (including ability to consistently increase satisfaction with IT services & tools) **Frequency**: Annual (or ad hoc for metric no 11.3)
VALIDATION	**TARGET GROUPS AND BENEFICIARIES**
• Management Team • Joint Reclassification Committee • IT Management Committee	• ENISA staff members and employees

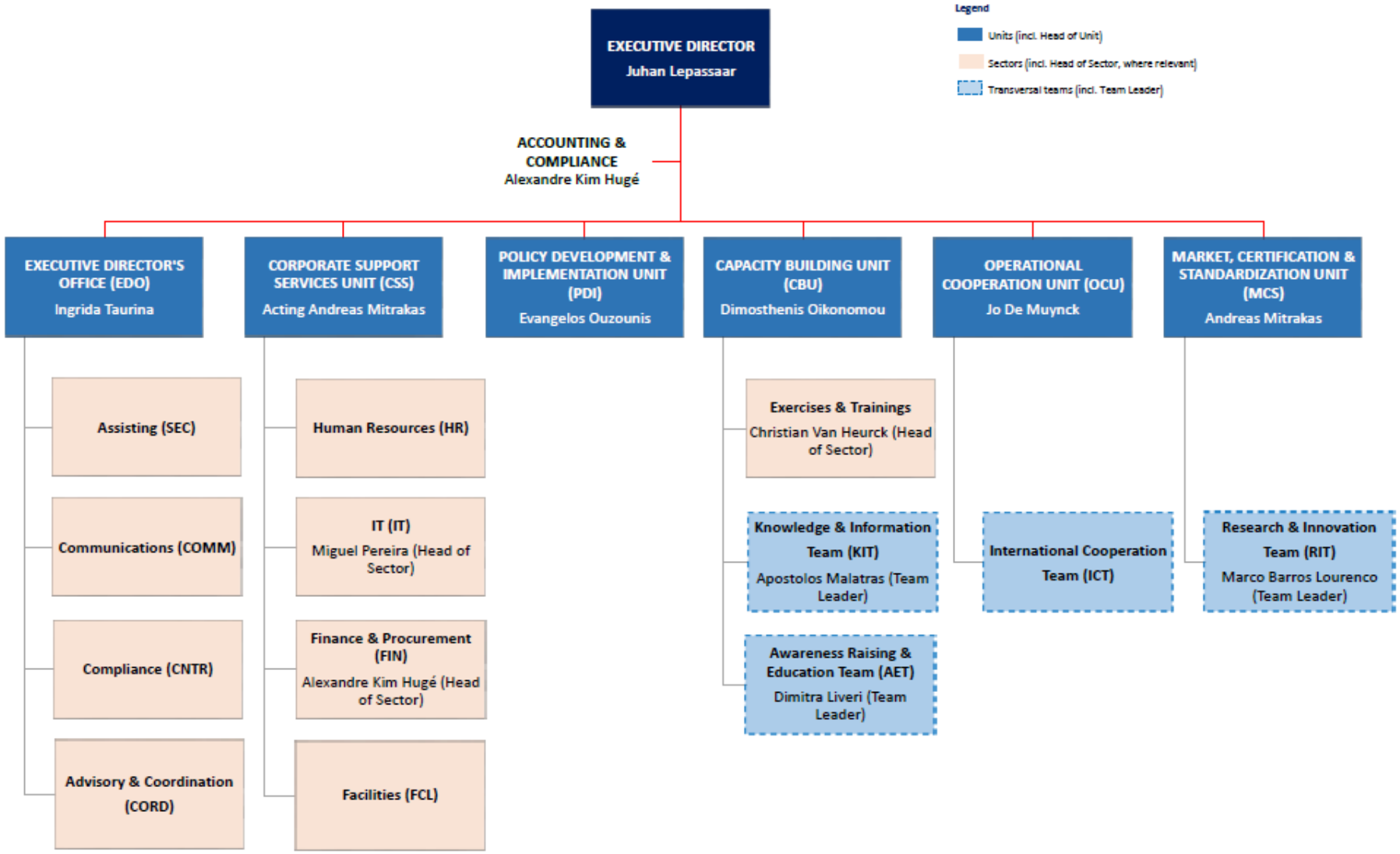
• Task Force on relocation of the Agency • Staff Committee	

ANNEX A

I. ORGANISATION CHART AS OF 01.01.2021



Administrative Organigramme



II. RESOURCE ALLOCATION PER ACTIVITY 2022 - 2024

The indicative allocation of the total 2022 financial and human resources following the activities as described in part 3.1 in Section III and the corporate activities as described in part 3.2 in Section III are presented in the table[12] below. The allocation has been done following direct budget and FTEs indicated for each activity with indirect budget being assigned based on causal relationships.

The following assumptions are used in the simplified ABB methodology:

- Direct Budget is the cost estimate of each of the 9 operational activities and 2 corporate activities as indicated under Section 3 of the SPD 2022-2024 in terms of goods and services to be procured.
- Indirect Budget is the cost estimate of salaries and allowances, buildings, IT, equipment and miscellaneous operating costs, attributable to each activity. The indirect budget is allocated to activities based on different drivers. Main driver for costs allocation was number of foreseen FTEs for each activity in 2022.

[12] Pending final review

ALLOCATION OF HUMAN AND FINANCIAL RESOURCES (2022)	Activities as referred to in Section 3	Direct and Indirect budget allocation[13] (in EUR)	FTE allocation[14]
Providing assistance on policy development	Activity 1	944.830,31	6
Supporting implementation of Union policy and law	Activity 2	2.503.406,28	14
Building capacity	Activity 3	3.032.135,68	15
Enabling operational cooperation	Activity 4	2.107.090,19	10
Contribute to cooperative response at Union and Member States level	Activity 5	2.199.026,45	9
Development and maintenance of EU cybersecurity certification framework	Activity 6	2.176.330,03	12
Supporting European cybersecurity market and industry	Activity 7	1.473.751,49	9
Knowledge on emerging cybersecurity challenges and opportunities	Activity 8	2.153.058,32	9
Outreach and education	Activity 9	1.295.336,48	7
Performance and risk management	Activity 10	2.381.419,25	18
Staff development and working environment	Activity 11	3.341.675,59	18
TOTAL		**23.608.060**	**127**

[13] Indicative budget allocation, to be updated at a later stage
[14] Indicative FTE allocation, to be updated at a later stage

III. FINANCIAL RESOURCES 2022 - 2024

Table 1: Revenue

REVENUES	2020 Executed Budget	2021 Revenue estimated by the agency	2022 As requested by the agency	VAR 2022 / 2021	Envisaged 2023	Envisaged 2024
1 REVENUE FROM FEES AND CHARGES						
2 EU CONTRIBUTION	20.646.000	22.248.000	23.023.000	3%	23.023.000	23.023.000
- of which assigned revenues deriving from previous years' surpluses **	*-110.505,47*					
3 THIRD COUNTRIES CONTRIBUTION (incl. EEA/EFTA and candidate countries)	503.120	585.060	585.060	0%	585.060	585.060
- of which EEA/EFTA (excl. Switzerland)	503.120	585.060	585.060	0%	585.060	585.060
- of which Candidate Countries						
4 OTHER CONTRIBUTIONS	533.764	640.000	*	N/A		
5 ADMINISTRATIVE OPERATIONS						
- of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art. 58)						
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT						
7 CORRECTION OF BUDGETARY IMBALANCES						
TOTAL REVENUES	**21.682.884**	**23.473.060**	**23.608.060**	**1%**	**23.608.060**	**23.608.060**

* - due to move to a new building, it is expected that Hellenic Authorities will make rental payments directly to the building owner, therefore no subsidy will be paid to ENISA

Table 2: Expenditure

EXPENDITURE	2021		2022	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1	10.775.409	10.775.409	11.137.231	11.137.231
Title 2	3.547.651	3.547.651	3.257.960	3.257.960
Title 3	9.150.000	9.150.000	9.212.869	9.212.869
Total expenditure	**23.473.060**	**23.473.060**	**23.608.060**	**23.608.060**

EXPENDITURE (in EUR)	Commitment and Payment appropriations *					
	Executed budget 2020	Budget 2021	Draft Budget 2022 Agency request	VAR 2022 / 2021	Envisaged in 2023	Envisaged in 2024
Title 1. Staff Expenditure	**10.586.452**	**10.775.409**	**11.137.231**	**3%**	**11.137.231**	**11.137.231**
11 Staff in active employment	6.682.169	8.810.319	9.129.864	4%	9.129.864	9.129.864
12 Recruitment expenditure	423.139	410.087	418.910	2%	418.910	418.910
13 Socio-medical services and training	322.047	1.084.064	1.107.387	2%	1.107.387	1.107.387
14 Temporary assistance	3.159.097	470.939	481.071	2%	481.071	481.071
Title 2. Building, equipment and miscellaneous expenditure	**3.865.823**	**3.547.651**	**3.257.960**	**-8%**	**3.257.960**	**3.257.960**
20 Building and associated costs	916.650	1.404.608	689.501	-51%	689.501	689.501
21 Movable property and associated costs	76.684	99.000	81.076	-18%	81.076	81.076
22 Current corporate expenditure	76.383	798.696	815.879	2%	815.879	815.879
23 Corporate ICT	2.796.105	1.245.347	1.671.504	34%	1.671.504	1.671.504
Title 3. Operational expenditure	**6.673.138**	**9.150.000**	**9.212.869**	**1%**	**9.212.869**	**9.212.869**
30 Activities related to meetings and missions	228.544	650.000	760.000	17%	760.000	760.000
32 Horizontal operational activities	1.824.209	0	0		0	0
36/37 Core operational activities	4.620.385	8.500.000	8.452.869	-1%	8.452.869	8.452.869
TOTAL EXPENDITURE	**21.125.412**	**23.473.060**	**23.608.060**	**1%**	**23.608.060**	**23.608.060**

Table 3: Budget outturn and cancellation of appropriations

Budget outturn	2018	2019	2020[15]
Revenue actually received (+)	11.572.995	16.740.086	21.801.460
Payments made (-)	-10.345.736	-11.980.352	-15.050.421
Carry-over of appropriations (-)	-1.348.657	-4.357.734	-6.200.614
Cancellation of appropriations carried over (+)	108.302	62.522	180.023
Adjustment for carry-over of assigned revenue appropriations carried over (+)	124.290	116.393	10.403
Exchange rate difference (+/-)	-689	-1.802	-1.291
Adjustment for negative balance from previous year (-)	-	-	-
Total	**110.505**	**579.113**	**739.560***

* Unaudited preliminary budget outturn

III.a Cancellation of appropriations[16]

- Cancellation of Commitment Appropriations

In 2020 Commitment Appropriations were cancelled for an amount of EUR 560 800 representing 3 % of the total budget. ENISA demonstrates a commitment rate of 97 % of C1 appropriations of the year at the year-end (31/12). The consumption of the 2020 budget at year-end shows the capacity of the Agency to fully implement its annual appropriations. The payment rate reached 69 % and the amount carried forward to 2021 is EUR 6 074 991 representing 29 % of total C1 appropriations in 2020.

- Cancellation of Payment Appropriations for the year

No payment appropriations were cancelled during 2020.

[15] To be updated in January 2021 after calculation of the final result at year end
[16] To be updated in January 2021

• Cancellation of Payment Appropriations carried over

(Fund source "C8" – appropriations carried over automatically from 2019 to 2020.)

The appropriations of 2019 carried over to 2020 were utilised at a rate of 96 % (automatic carry-overs) which indicates a satisfactory capability of estimation of needs. From the amount of EUR 4 347 332 carried forward, the amount of EUR 180 023 was cancelled, mostly due to the circumstances caused by COVID-19. This cancellation represents 0,7 % of the total budget 2020 (fund sources C1 and C8)..

IV. HUMAN RESOURCES- QUANTITATIVE

Overview of all categories of staff and its evolution

Staff policy plan for 2022 - 2024

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

Statutory staff and SNE

STAFF	2020			2021	2022	2023
ESTABLISHMENT PLAN POSTS	**Authorised Budget**	**Actually filled as of 31/12/2020**	**Occupancy rate %**	**Envisaged staff**	**Envisaged staff**	**Envisaged staff**
Administrators (AD)	51	47[17]	92%	57	60	60
Assistants (AST)	18	15	83%	19	19	19
Assistants/Secretaries (AST/SC)						
TOTAL ESTABLISHMENT PLAN POSTS	69	62	90%	76	79	79
EXTERNAL STAFF	**FTE corresponding to the authorised budget**	**Executed FTE as of 31/12/2020**	**Execution Rate %**	**FTE corresponding to the authorised budget**	**Envisaged FTE**	**Envisaged FTE**
Contract Agents (CA)	30	29[18]	97%	30	30	30
Seconded National Experts (SNE)	12	8	67%	12	18[19]	18
TOTAL EXTERNAL STAFF	**5**	**31**	**100%**	**5**	**5**	**5**
TOTAL	**47**	**68**	**100%**	**47**	**53**	**53**
TOTAL STAFF	**116**	**130**	**100%**	**118**	**127**	**127**

Additional external staff expected to be financed from grant, contribution or service-level agreements

[17] Total number includes the in-house AD staff by 31/12/2020 and 9 AD offers sent and accepted by 31/12/2020.
[18] Total number includes the in-house CA staff by 31/12/2020 and 3 offers sent and accepted by 31/12/2020.
[19] Increase is necessary since SNE posts are crucial for the Agency's ability to address the tasks mandated by the CSA, such as: operational cooperation, development of the National Cybersecurity Strategies and incident reporting. In anticipation of the upcoming legislation proposals the knowledge from MS perspective will be crucial for success in completing these tasks.

Human Resources	2020	2021	2022	2023
	Envisaged FTE	Envisaged FTE	Envisaged FTE	Envisaged FTE
Contract Agents (CA)	n/a	n/a	n/a	n/a
Seconded National Experts (SNE)	n/a	n/a	n/a	n/a
TOTAL	n/a	n/a	n/a	n/a

Other Human Resources

- Structural service providers

	Actually in place as of 31/12/2020
Security	5
IT	4

- Interim workers

	Actually in place as of 31/12/2020
Number	31

Table 2: Multi-annual staff policy plan Year 2019, 2020, 2021, 2022, 2023[20]

Function group and grade	2020				2021		2022		2023	
	Authorised budget		Actually filled as of 31/12[21]		Envisaged		Envisaged		Envisaged	
	Permanent posts	Temporary posts	Permanent posts	Temp. posts	Perm. Posts	Temp. posts	Perm. posts	Temp. posts	Perm. posts	Temp. posts
AD 16										
AD 15		1				1		1		1
AD 14				1						
AD 13						1		2		2
AD 12		6		6		5		4		4
AD 11						2		2		2
AD 10		5		3		3		4		4
AD 9		12		7		12		11		11
AD8		19		10		21		22		22
AD 7				11		8		8		8
AD 6				9		4		6		6

[20] The change in the number of establishment plan up to 10% requested for year 2022 is modified as per Art 38 of the ENISA Financial Regulation
[21] Total number includes the in-house AD staff by 31/12/2020 and 9 AD offers sent and accepted by 31/12/2020.. Data available as of 01.01.2021 and refers to the take up duties.

Function group and grade	2020				2021		2022		2023	
	Authorised budget		Actually filled as of 31/12[21]		Envisaged		Envisaged		Envisaged	
	Permanent posts	Temporary posts	Permanent posts	Temp. posts	Perm. Posts	Temp. posts	Perm. posts	Temp. posts	Perm. posts	Temp. posts
AD 5										
AD TOTAL		43		47		57		60		60
AST 11										
AST 10										
AST 9										
AST 8						1		2		2
AST 7		3		3		4		3		3
AST 6		7		1		8		8		8
AST 5		5		5		5		5		5
AST 4		1		3		1		1		1
AST 3				2						
AST 2				1						
AST 1										
AST TOTAL		16		15		19		19		19
AST/SC 6										
AST/SC 5										
AST/SC 4										
AST/SC 3										
AST/SC 2										
AST/SC 1										
AST/SC TOTAL										
TOTAL		59		62		76		79		79
GRAND TOTAL	59		62		76		79		79	

External personnel

Contract Agents

Contract agents	FTE corresponding to the authorised budget 2020	Executed FTE as of 31/12/2020	Headcount as of 31/12/2020	FTE corresponding to the authorised budget 2020	FTE corresponding to the authorised budget 2021	FTE corresponding to the authorised budget 2022	FTE corresponding to the authorised budget 2023
Function Group IV	28	20[22]	20[23]	28	28	28	28
Function Group III	2	8	8	2	2	2	2
Function Group II	0	0	0	0	0	0	0
Function Group I	0	1	1	0	0	0	0

[22] Total number includes the in-house CA staff by 31/12/2020 and 3 offers sent and accepted by 31/12/2020.
[23] Total number includes the in-house CA staff by 31/12/2020 and 3 offers sent and accepted by 31/12/2020.

Contract agents	FTE corresponding to the authorised budget 2020	Executed FTE as of 31/12/2020	Headcount as of 31/12/2020	FTE corresponding to the authorised budget 2020	FTE corresponding to the authorised budget 2021	FTE corresponding to the authorised budget 2022	FTE corresponding to the authorised budget 2023
TOTAL	30	29	29	30	30	30	30

Seconded National Experts

Seconded National Experts	FTE corresponding to the authorised budget 2020	Executed FTE as of 31/12/2020	Headcount as of 31/12/2020	FTE corresponding to the authorised budget 2020	FTE corresponding to the authorised budget 2021	FTE corresponding to the authorised budget 2022	FTE corresponding to the authorised budget 2023
TOTAL	12	8	8	12	12	18[24]	18

Table 3: Recruitment forecasts 2022 following retirement / mobility or new requested posts (indicative table)

Job title in the agency	TYPE OF CONTRACT (OFFICIAL, TA OR CA)		TA/OFFICIAL Function group/grade of recruitment internal (Brackets) and external (single grade) foreseen for publication *		CA Recruitment Function Group (I, II, III and IV)
	Due to foreseen retirement/ mobility	New post requested due to additional tasks	Internal (brackets)	External (brackets)	
Experts		3 AD posts	n/a	n/a	n/a
Assistant		n/a	n/a	n/a	n/a

[24] Increase is necessary since SNE posts are crucial for the Agency's ability to address the tasks mandated by the CSA, such as: operational cooperation, development of the National Cybersecurity Strategies and incident reporting. In anticipation of the upcoming legislation proposals the knowledge from MS perspective will be crucial for success in completing these tasks.

V. HUMAN RESOURCES QUALITATIVE

A. Recruitment policy

Implementing rules in place:

		YES	NO	If no, which other implementing rules are in place
Engagement of CA	Model Decision C(2019)3016	x		
Engagement of TA	Model Decision C(2015)1509	x		
Middle management	Model decision C(2018)2542	x		
Type of posts	Model Decision C(2018)8800		x	C(2013) 8979

B. Appraisal and reclassification/promotions

Implementing rules in place:

		YES	NO	If no, which other implementing rules are in place
Reclassification of TA	Model Decision C(2015)9560	x		
Reclassification of CA	Model Decision C(2015)9561	x		

Table 1: **Reclassification of TA/promotion of official**

AVERAGE SENIORITY IN THE GRADE AMONG RECLASSIFIED STAFF							
Grades	**Year 2016**	**Year 2017**	**Year 2018**	**Year 2019**	**Year 2020**	**Actual average over 5 years**	**Average over 5 years (According to decision C(2015)9563)**
AD05	-	-	-	-	-	-	2.8
AD06	1	1	2	3	-	3,7	2.8
AD07	1	-	-	-	1	3	2.8
AD08	1	1	1	-	2	6	3
AD09	-	-	1	-	-	10	4
AD10	-	-	-	-	-	-	4
AD11	1	-	-	-	-	3	4
AD12	-	-	-	-	-	-	6.7
AD13	-	-	-	-	-	-	6.7
AST1	-	-	-	-	-	-	3
AST2	-	-	-	-	-	-	3
AST3	1	1	1	-	-	4,42	3
AST4	1	1	1	-	1	5,25	3
AST5	1	-	1	-	-	5,5	4
AST6	1	-	-	-	1	4	4
AST7	-	-	-	-	-	-	4

AST8	-	-	-	-	-	-	4
AST9	-	-	-	-	-	-	N/A
AST10 (Senior assistant)	-	-	-	-	-	-	5

There are no AST/SCs at ENISA: n/a

AST/SC1							4
AST/SC2							5
AST/SC3							5.9
AST/SC4							6.7
AST/SC5							8.3

Table 2: Reclassification of contract staff

Function group	Grade	Staff in activity at 1.01.2019	How many staff members were reclassified in year 2020	Average number of years in grade of reclassified staff members	Average number of years in grade of reclassified staff members according to decision c(2015)9561
CA IV	17	1	-	-	Between 6 and 10 years
	16	0	-	-	Between 5 and 7 years
	15	1	-	-	Between 4 and 6 years
	14	9	-	-	Between 3 and 5 years
	13	3	1	3,9	Between 3 and 5 years
CA III	11	1	1	2	Between 6 and 10 years
	10	5	1	3	Between 5 and 7 years
	9	3	1	4,2	Between 4 and 6 years
	8	0	0	-	Between 3 and 5 years
CA II	6	-	-	-	Between 6 and 10 years
	5	-	-	-	Between 5 and 7 years
	4	-	-	-	Between 3 and 5 years
CA I	3	1	-	-	n/a
	2	-	-	-	Between 6 and 10 years
	1	-	-	-	Between 3 and 5 years

C. Gender representation

Table 1: Data on 31/12/2020 statutory staff (only, temporary agents and contract agents, including last entry into service on 16/12/2020)

		OFFICIAL		TEMPORARY		CONTRACT AGENTS		GRAND TOTAL	
		Staff	%	Staff	%	Staff	%	Staff	%
Female	Administrator level	-	-	11	-	15	-	-	-
	Assistant level (AST & AST/SC)	-	-	10	-	-	-	-	-
	Total	-	-	21	58	15	42	36	46
Male	Administrator level	-	-	27	-	11	-	-	-

	Assistant level (AST & AST/SC)	-	-	5	-	-	-	-	-
	Total	-	-	32	74	11	26	43	54
Grand Total		-	-	53	67	26	33	79	100%

Table 2: Data regarding gender evolution over 5 years of the Middle and Senior management (31.12.2020)

	2016		2020	
	Number	%	Number	%
Female Managers	0	0	1	11
Male Managers	10	100	8	89

The focus of the Agency being cybersecurity hints at the reason for a certain gender imbalance. Nevertheless, an improvement has been noted during the past five years. Continuous efforts to encourage female involvement in this domain have borne fruit, however, further efforts should be envisaged in order to achieve a higher percentage of female middle and senior managers at ENISA in the upcoming years.

D. Geographical Balance

Table 1: Provisional data on 31/12/2020 - statutory staff only (TAs, CAs and last entry into service on 16/12/2020)

NATIONALITY	AD + CA FG IV		AST/SC- AST + CA FGI/CA FGII/CA FGIII		TOTAL	
	Number	% of total staff members in AD and FG IV categories	Number	% of total staff members in AST SC/AST and FG I, II and III categories	Number	% of total staff
BE	4	7	2	8,3	6	7,6
BG	2	3,6	-	-	2	2,5%
CY	-	-	2	8,3	2	2,5%
CZ	1	1,8	-	-	1	1,2%
DE	2	3,6	-	-	2	2,5%
Double *25	4	7	3	12,5	7	8,8%
EE	1	1,8	-	-	1	1,2%

[25] Double nationalities comprise staff members who also have non-EU nationalities (i.e. Italian/Australian, Belgian/British, Cypriot/Greek, German/Greek, Dutch/Greek etc.).

ES	2	3,6	1	4	3	3,8%
FR	2	3,6	1	4	3	3,8%
GR	20	36,3	11	46	31	39,2%
IT	2	3,6	-	-	2	2,5%
LT	-	-	1	4	1	1,2%
LV	2	3,6	-	-	2	2,5%
NL	3	5,4	-	-	3	3,8%
PL	1	1,8	1	4	2	2,5%
PT	3	5,4	1	4	4	5%
RO	4	7	0	0	4	5%
SE	2	3,6	-	-	2	2,5%
SK	-	-	1	4	1	1,2%
TOTAL	55	69,7	24	30,3	79	100

Double nationalities comprise staff members who also have non-EU nationalities (i.e. Italian/Australian, Belgian/British, Cypriot/Greek, German/Greek, Dutch/Greek etc.).

Table 2: Evolution over 5 years of the most represented nationality in the Agency

Most represented nationality	2015		2020	
	Number	%	Number	%
Greek	18 (out of 63)	28,5	31 (out of 79)	39

Looking back in 2019 and 2020 positive mesures to improve the diversity of nationalities included broad outreach campaigns on popular media across the European Union, closer consideration on the nationality spread in relation to competencies requested, and specific provisions on the vacancy notices have been continued[26].

[26] The seeming imbalance related to the most represented nationality at ENISA is related to several factors, such as, for example, the level of posts and related salaries which may be perceived as less appealing for job seekers in relatively more advanced member state economies; the fact that ENISA has a better position as employer compared to average conditions offered in the Greek job market; the small job market in Greece for cybersecurity professionals; historic decisions taken by previous AIPNs. Another reason that may be cited is the need for stability during the start up phase of the Agency, as staff from the hosting member state (Greece) is less prone to resign (resulting in lesser turnover), which in combination with the relatively young age of the Agency compared to others, still has its original impact; the relatively better academic profile of Greek candidates that bears for lower level posts; the relatively smaller payroll cost for staff that is relatively better qualified than average while costing less if expatriation allowance is considered, as well as the general predisposition to retain a lower level position in the home country.

.E. Local office in Brussels, Belgium (TBC)

In 2020 ENISA put forward a proposal to open a local office in accordance with CSA Art 20 (5). The CSA provides that the aggregate number of staff in all local offices shall be kept to a minimum and shall not exceed 40 % of the total number of ENISA's staff located in the Member State in which the seat of ENISA is located. The number of the staff in each local office shall not exceed 10 % of the total number of ENISA's staff located in the Member State in which the seat of ENISA is located.. In accordance with Art. 20 (5) ENISA is currently going through the required approval process.

F. Schooling

Agreement in place with the European School of Heraklion	
Contribution agreements signed with the EC on type I European schools	**No**
Contribution agreements signed with the EC on type II European schools	**Yes**
Number of service contracts in place with international schools:	**For the school year 2020-2021, there are 14 service level agreements in place.**

VI. ENVIRONMENT MANAGEMENT

This will depend on the new headquarters building however ENISA is looking into opportunities to strengthen its environmental management.

VII. BUILDING POLICY

In 2021 ENISA will relocate to a new headquarters building in Athens, Greece

VIII. 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 entered in to force on the 04 October 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 entered in to force on the 04 October 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.

IX. EVALUATIONS

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, and coherence and relevance.

The analysis confirmed the overall success of the delivery of ENISA's demanding work programme for 2019 despite the changing circumstances the Agency had to accommodate in 2019 following the signing of the new Cybersecurity

Act and the handover from Prof. Dr. Udo Helmbrecht to Juhan Lepassaar, the newly appointed Executive Director. Stakeholders consulted generally agree that the EU Agency for Cybersecurity is the only entity that could possibly achieve such results, is seen as a key enabler of knowledge, experience and expertise and allowing the creation of a strong cybersecurity community. The report therefore concludes on an extremely positive note, acknowledging the added value of ENISA's activities for the whole EU.

The ex ante evaluation included desk research and interviews with key ENISA stakeholders. It concluded that given the restructuring of the Programming Document 2021-2023, the structure of ENISA's SPD would not require any changes, but it was recommended that certain outputs should be strengthened and new outputs to be developed such as:

- a proactive shaping of the political agenda;
- developing a tranversal focus on digital strategic autonomy and its implications on cybersecurity;
- reinforcing the cooperative response by an insight-driven approach;
- focusing on awareness raising and activities targeting industry.

ENISA uses an internal monitoring system that intends to support the project management function, which includes the project delivery and resources allocation. The regular reporting and the ENISA management team uses this information for managerial purposes. Moreover, ENISA have implemented a mid-term review procedure and regular weekly management team meetings. ENISA expects to undertake a study to upgrade the use of the electronic tool in the internal project management and overall delivery of the Agency WP.

X. STRATEGY FOR THE ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS

The Agency's strategy for an effective internal control is based on best international practices and on the Internal Control Framework (COSO Framework's international Standards).

The Control Environment is the set of standards of conduct, processes and structures that provide the basis for carrying out internal control across ENISA. The Management Team set the tone at the top with respect to the importance of the internal control, including expected standards of conduct.

Risk assessment is the Agency's dynamic and iterative process for identifying and assessing risks which could affect the achievement of objectives, and for determining how such risks should be managed.

The control activities ensure the mitigation of risks related to the achievement of policy, operational and internal control objectives. They are performed at all levels of the organisation, at various stages of business processes, and across the technology environment. They may be preventive or detective and encompass a range of manual and automated activities as well as segregation of duties.

Information is necessary for the organisation to carry out internal control and to support the achievement of objectives. In this aspect it is needed to consider external and internal communication. External communication provides the specific Agency stakeholders and globally the EU citizens with information on ENISA's policy, objectives, actions and achievements. Internal communication provides to ENISA staff with the information required to support the achievement of objectives and the awareness for day-to-day controls.

Continuous and specific assessments are used to ascertain whether each of the five components of internal control is present and functioning. Continuous assessments, built into business processes at different levels of the organisation, provide timely information on any deficiencies. Findings are assessed and deficiencies are communicated and corrected in a timely manner, with serious matters reported as appropriate.

The Common Approach on EU Decentralised Agencies foresees that EU agencies should be more active concerning fraud prevention issues and that the related communication forms an essential part of its success. In order to implement this, the European Anti-Fraud Office (OLAF) recommended that each agency should adopt an anti-fraud

strategy that is proportionate to its fraud risks. Rules for the prevention and management of conflicts of interests are part of the anti-fraud strategy of the Agency.

XI. PLAN FOR GRANT, CONTRIBUTION OR SERVICE-LEVEL AGREEMENTS

ENISA does not receive any form of grant.

Table[27] below provides a summary of the SLA and agreements of the agency including contracted amount where necessary:

Title	Type	Contractor	Contracted amount
SLA with EU-Lisa - Cyber Exercise (new)	SLA	EU-LISA - EUROPEAN AGENCY	
SLA with CEDEFOP	SLA	CEDEFOP	
10th Amendment of SLA with CERT-EU-001-00	SLA	EUROPEAN COMMISSION	€ 24.000,00
Service Level Agreement and Service Delivery Agreement with DG Budget Implementation and usage of ABAC System	SLA	DG BUDG	
SLA for the "Issuance process of the laissez-passer" with EC	SLA	EC	
Collaboration between DG HR and ENISA - SYSPER services	SLA		
SLA with DG HR	SLA	DG HR	
Global SLA with DIGIT	SLA	EUROPEAN COMMISSION	
SLA with Office for Official Publications of the European Communities	SLA	Office for OPEC	
SLA for ABAC System with DG Budget	SLA		
SLA with European Administrative School	SLA	EAS	
Agreement for Provision of ICCA services with BEREC	SLA	OFFICE OF THE BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATIONS (BEREC OFFICE)	€ 15.000,00
SLA for Provision of electronic data back up services with BEREC	SLA	OFFICE OF THE BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATIONS (BEREC OFFICE)	
SLA with EASA - Permanent Secretariat	SLA	EASA	
SLA for Shared Support Office (SSO)_EUAN	SLA	EUROPEAN FOOD SAFETY AUTHORITY - EFSA	€ 2.459,00

[27] To be updated in the course of 2021

SLA with Veritas School	SLA	VERITAS EDUCATION - EDUCACAO E SERVICOS SA	
SLA with Leonteios School	SLA	LEONTEIO LYKEIO PATISION AEE	
SLA with ACS School	SLA	AMERICAN COMMUNITY SCHOOLS OF ATHENS INC	
SLA with Douka School	SLA	DOUKA EKPAIDEFTIRIA AE	
SLA with Neue Schule 2019/20	SLA	NEUE SCHULE AE	
SLA with Trianemi School 2019/20	SLA	TRIANEMI	
SLA with Platon School 2019/20	SLA	PLATON IB SCHOOL	
SLA with Lycee Franco-Hellenique 2019/20	SLA	LYCÉE FRANCO-HELLÉNIQUE EUGÈNE DELACROIX	
SLA with Arsakeio School 2019/20	SLA	H EN ATHINAIS FILEKPAIDEFTIKI ETAIRIA (Arsakeio)	
SLA with Campion School 2019/20	SLA	CAMPION SCHOOL INC	
SLA with Ionios School	SLA	IONIOS SXOLI SA TRAINING COMPANY	
SLA with S.Catherine's 2019/20	SLA	ST. CATHERINES BRITISH SCHOOL	
SLA with Papakosmas Datatechnica No 2020/003, P7EM-100, 1452152	SLA	PAPAKOSMAS NTATATECHNIKA EPE	
SLA with Papakosmas Datatechnica No 2020/004, P7EM-075, 1452165	SLA	PAPAKOSMAS NTATATECHNIKA EPE	
Amendment 3 of the SLA_Implementation and usage of ABAC System	SLA		
Amendment to SLA btwn ENISA and BEREC	SLA	OFFICE OF THE BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATIONS (BEREC OFFICE)	
SLA with PMO	SLA		
SLA with EPSO and EUSA (updated)	SLA	EUROPEAN PERSONNEL SELECTION OFFICE (EPSO)	
Cooperation between EDA and ENISA	Agreement	EUROPEAN DEFENCE AGENCY - EDA	
Agreement with the Hellenic Ministry of Infrastructure, Transport and Networks	Agreement	REPUBLIQUE HELLENIC - HELLENIC MINISTRY OF INFRASTRUCTURE, TRANSPORT AND NETWORKS	
ABAC DWH extraction and transfer for ENISA's needs	Agreement		€ 27.000,00
Mandate and Service agreement for "Type II European School" with EC	Agreement		

Administrative arrangement with DG HR.DS	Agreement		
Agreement with Translation Centre for the Bodies of the EU	Agreement		
Provision of water fountain and water bottles for Athen's office	Agreement		
Collaboration Agreement with CEN & CENELEC	Agreement		
Austrian signature scheme for e-card and mobile signature_A-Trust	Agreement	A-TRUST GESELLSCHAFT FUR SICHERHEITSSYSTEME IM ELEKTRONISCHEN DATENVERKEHR GMBH	
Agreement for Courier Services	Agreement	TNT SKYPAK HELLAS EPE	
Mission Charter of the IAS of the EC	Agreement		
Agreement on Strategic Co-operation with EUROPOL	Agreement	EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION (EUROPOL)	
Agreement with Edenred (Ticket Restaurant Meal Vouchers)	Agreement	VOUCHERS SERVICES SA	
Joint ENISA - EUROPOL /EC3 WG on Security and Safety Online	Agreement	EUROPEAN POLICE OFFICE EUROPOL	
NoN-Disclosure Agreement CT1607860_Confidential and proprietary document between 12 Parties	Agreement		
Working Arrangement Agreement with eu-LISA (MoU)	Agreement	EU-LISA - EUROPEAN AGENCY	
Lease Agreement Athens office (Main building)	Agreement	ATHENIAN PROPERTIES LIMITED	
Lease Agreement Athens office (East Wing)	Agreement	ATHENIAN PROPERTIES LIMITED	
Agreement with Hellenic Postal Services A.E. - Heraklion office	Agreement	ELLINIKA TACHYDROMEIA*ELTA AE	
Agreement with Hellenic Postal Services A.E. - Athens office	Agreement	ELLINIKA TACHYDROMEIA*ELTA AE	
Inter-Agencies Cost-Sharing Agreement (EUAN)	Agreement	EUROPEAN FOOD SAFETY AUTHORITY - EFSA	€ 982,00
Agreement for courier services with DHL	Agreement	DHL INTERNATIONAL SA	
Mission Charter of the IAS_REVISED	Agreement		

XII. STRATEGY FOR COOPERATION WITH THIRD COUNTRIES AND/OR INTERNATIONAL ORGANISATIONS

In 2021 the Agency will draft its international strategy and the text will be provided in due course.

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 2022 (Budget 2022)

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)

Reference acts

1. Impact assesment submitted by the Commission on 13 September 2017, on ENISA, the 'EU Cybersecurity Agency', as 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 2022

The 2021 total revenue amounts to € 23608060 and consists of a subsidy of € 23023000 from the General Budget of the European Union, EFTA countries' contributions € 585060 and a subsidy from the Greek Government for the rent of the offices of ENISA in Greece €0

2.2 Expenditure in 2022

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 **€11.137.231,32**

Title 2 - Buildings, equipment and miscellaneous operating expenditure

Total expenditure under Title 2 amounts to **€3.257.959,69**

Title 3 - Operational expenditure

Operational expenditure is mainly related to the implementation of
Work Programme 2022 and amounts to **€9.212.869,00**

3. STATEMENT OF REVENUE 2022

Title	Heading	Voted Appropriations 2019 in €	Voted Appropriations - Amending Budget 1/2020 in €	Voted Appropriations 2021 €	1st Draft Proposed Appropriations 2022 €	Remarks - budget 2022
1	EUROPEAN COMMUNITIES SUBSIDY	15.910.000	20.646.000	22.248.000	23.023.000	Total subsidy of the European Communities
2	THIRD COUNTRIES CONTRIBUTION	382.952	503.120	585.060	585.060	Contributions from Third Countries.
3	OTHER CONTRIBUTIONS	640.000	435.844	640.000	0	Subsidy from the Government of Greece
4	ADMINISTRATIVE OPERATIONS	0	97.920	0	0	Other expected income.
	GRAND TOTAL	**16.932.952**	**21.682.884**	**23.473.060**	**23.608.060**	

Article Item	Heading	Voted Appropriations 2019 in €	Voted Appropriations - Amending Budget 1/2020 in €	Voted Appropriations 2021 €	1st Draft Proposed Appropriations 2022 €	Remarks - budget 2022
1	EUROPEAN COMMUNITIES SUBSIDY					
10	EUROPEAN COMMUNITIES SUBSIDY					
100	*European Communities subsidy*	15.910.000	20.646.000	22.248.000	23.023.000	Regulation (EU) N° 526/2013 establishing an European Union Agency for Network and Information Security.
	CHAPTER 10	15.910.000	20.646.000	22.248.000	23.023.000	
	TITLE 1	**15.910.000**	**20.646.000**	**22.248.000**	**23.023.000**	
2	THIRD COUNTRIES CONTRIBUTION					
20	THIRD COUNTRIES CONTRIBUTION					
200	*Third Countries contribution*	382.952	503.120	585.060	585.060	Contributions from Associated Countries.
	CHAPTER 2 0	382.952	503.120	585.060	585.060	
	TITLE 2	**382.952**	**503.120**	**585.060**	**585.060**	
3	OTHER CONTRIBUTIONS					
30	OTHER CONTRIBUTIONS					
300	*Subsidy from the Ministry of Transports of Greece*	640.000	435.844	640.000	0	Subsidy from the Government of Greece.
	CHAPTER 30	640.000	435.844	640.000	0	
	TITLE 3	**640.000**	**435.844**	**640.000**	**0**	
4	ADMINISTRATIVE OPERATIONS					
40	ADMINISTRATIVE OPERATIONS					
400	*Administrative Operations*	0	97.920	0	0	Revenue from administrative operations.
	CHAPTER 40	0	97.920	0	0	
	TITLE 4	**0**	**97.920**	**0**	**0**	
	GRAND TOTAL	**16.932.952**	**21.682.884**	**23.473.060**	**23.608.060**	

4. STATEMENT OF EXPENDITURE 2022

Title	Heading	Voted Appropriations 2019 in €	Voted Appropriations - Amending Budget 1/2020 in €	Voted Appropriations 2021 €	1st Draft Proposed Appropriations 2022 €	Remarks - budget 2022
1	STAFF	9.387.948	11.203.334	10.775.409	11.137.231	Total funding for covering personnel costs.
2	BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE	2.677.000	3.150.568	3.547.651	3.257.960	Total funding for covering general administrative costs.
3	OPERATIONAL EXPENDITURE	4.868.004	7.328.981	9.150.000	9.212.869	Total funding for operational expenditures.
	GRAND TOTAL	**16.932.952**	**21.682.884**	**23.473.060**	**23.608.060**	
1	STAFF					
11	STAFF IN ACTIVE EMPLOYMENT					
110	*Staff holding a post provided for in the establishment plan*					

1100	Basic salaries		5.000.000	5.484.400	6.453.819	6.722.667	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	5.000.000	5.484.400	6.453.819	6.722.667	
111	***Other staff***						
1110	Contract Agents		1.650.000	1.476.000	2.106.500	2.151.819	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)		144.000	165.684	250.000	255.379	This appropriation is intended to cover basic salaries and all benefits of SNEs.
		Article 111	1.794.000	1.641.684	2.356.500	2.407.198	
		CHAPTER 11	**6.794.000**	**7.126.084**	**8.810.319**	**9.129.864**	
12	**RECRUITMENT/DEPARTURE EXPENDITURE**						
120	***Expenditure related to recruitment***						
1200	Expenditure related to recruitment		97.000	275.308	49.087	50.143	This appropriation is intended to cover expenditure related to recruitment, e.g. incurred for interviewing candidates, external selection committee members, screening applications and other related costs.
		Article 1 2 0	97.000	275.308	49.087	50.143	
121	***Expenditure on entering/leaving and transfer***						
1210	Expenses on Taking Up Duty and on End of Contract		40.000	48.201	32.000	32.688	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		356.042	137.424	145.000	148.120	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		247.000	111.462	72.000	73.549	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		228.906	132.291	112.000	114.410	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	871.948	429.378	361.000	368.767	
		CHAPTER 1 2	**968.948**	**704.686**	**410.087**	**418.910**	

13	**SOCIO-MEDICAL SERVICES AND TRAINING**						
131	***Medical Service***						
1310	Medical Service		75.000	45.310	53.882	55.041	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	75.000	45.310	53.882	55.041	
132	***Training***						
1320	Language Courses and Other Training		250.000	330.428	280.182	286.210	This appropriation is intended to cover the costs of language and other training needs as well as teambuilding activities.
		Article 1 3 2	250.000	330.428	280.182	286.210	
133	***Social welfare***						
1330	Other welfare expenditure		n/a	n/a	250.000	255.379	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	500.000	510.757	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	750.000	766.136	
		CHAPTER 1 3	**325.000**	**375.738**	**1.084.064**	**1.107.387**	
14	**TEMPORARY ASSISTANCE**						
140	***European Commission Management Costs***						
1400	EC Management Costs		58.000	39.149	70.939	72.465	This appropriation is intended to cover the EC management costs.
		Article 1 4 0	58.000	39.149	70.939	72.465	
141	***Social welfare***						
1411	Other welfare expenditure		110.000	172.537	n/a	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 1330*
1412	Schooling & Education expenditure		420.000	470.000	n/a	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 1331*
		Article 1 4 1	530.000	642.536	0	0	
142	***Temporary Assistance***						
1420	Interim Service		572.000	1.673.006	400.000	408.606	This appropriation is intended to cover the costs of temporary assistance (trainees and interim services).
1421	Consultants		115.000	625.135	n/a	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 2220*
1422	Internal Control and Audit		25.000	17.000	n/a	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 2220*
		Article 1 4 2	712.000	2.315.141	400.000	408.606	
		CHAPTER 1 4	**1.300.000**	**2.996.826**	**470.939**	**481.071**	
		Total Title 1	**9.387.948**	**11.203.334**	**10.775.409**	**11.137.231**	
2	**BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE**						
20	**BUILDINGS AND ASSOCIATED COSTS**						
200	**Buildings and associated costs**						
2000	Rent of buildings		640.000	435.844	640.000	0	This appropriation is intended to cover the payment of rent for buildings or parts of buildings occupied by the Agency and the hiring of parking spaces.
2002	Building Insurance		6.000	4.500	n/a	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 2003*
2003	Water, gas, electricity, heating and insurance		130.000	58.500	76.050	85.372	This appropriation is intended to cover the costs of utitlities and insurance of the premises of the Agency.
2004	Cleaning and maintenance		74.000	100.120	120.000	122.582	This appropriation is intended to cover the costs of cleaning and upkeeping of the premises used by the Agency.
2005	Fixtures and Fittings		25.000	25.650	50.000	51.076	This appropriation is intended to cover the fitting-out of the premises and repairs in the building.

2006	Security equipment		25.000	64.651	n/a	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 2007*
2007	Security Services and Equipment		140.000	134.084	140.000	160.000	This appropriation is intended to cover expenditure on buildings connected with security and safety, in particular contracts governing building surveillance as well as purchases and maintenance cost of equipment related to security and safety of the building and the staff.
2008	Other expenditure on buildings		60.000	106.470	378.558	270.471	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, costs of moving to and/or establishing new premises of the Agency and other handling costs.
		Article 2 0 0	1.100.000	929.820	1.404.608	689.501	
		CHAPTER 2 0	**1.100.000**	**929.820**	**1.404.608**	**689.501**	

21	**MOVABLE PROPERTY AND ASSOCIATED COSTS**						
210	***Technical Equipment and installations***						
2100	Technical Equipment and services		25.000	10.968	30.000	30.645	This appropriation is intended to cover expenditure of acquiring technical equipment, as well as maintenance and services related to it.
		Article 2 1 0	25.000	10.968	30.000	30.645	
211	***Furniture***						
2110	Furniture		15.000	16.303	49.000	30.000	This appropriation is intended to cover the costs of purchasing, leasing, and repairs of furniture.
		Article 2 1 1	15.000	16.303	49.000	30.000	
212	***Transport Equipment***						
2121	Maintenance and Repairs of transport equipment		12.000	9.000	10.000	10.215	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	12.000	9.000	10.000	10.215	
213	***Library and Press***						
2130	Books, Newspapers and Periodicals		6.000	17.803	10.000	10.215	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	6.000	17.803	10.000	10.215	
		CHAPTER 2 1	**58.000**	**54.074**	**99.000**	**81.076**	
22	**CURRENT CORPORATE EXPENDITURE**						
220	***Stationery, postal and telecomunications***						
2200	Stationery and other office supplies		60.000	52.233	30.000	30.645	This appropriation is intended to cover the costs of office stationery and the purchase of office kitchen consumables.
2201	Postage and delivery charges		20.000	30.000	20.000	20.430	This appropriation is intented to cover post office and special courrier costs.
2203	Other Office Supplies		23.000	15.469	n/a	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 2200*
		Article 2 2 0	103.000	97.702	50.000	51.076	
221	***Financial charges***						
2210	Bank charges and interest paid		1.000	1.000	1.000	1.021	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	1.021	
222	***Outsourcing consultancy services for corporate activities***						
2220	Outsourcing consultancy services for corporate activities		n/a	n/a	747.696	763.782	This appropriation is intended to cover expenditure of contracting consultants linked to administrative support services and horizontal tasks, e.g. in HR area, IT area, financial, accounting, internal controls, legal consultancy, advisory, audit, external evaluation, strategic consultancy and/or other administrative support services provided by third parties.
		Article 2 2 2	0	0	747.696	763.782	
		CHAPTER 2 2	**104.000**	**98.702**	**798.696**	**815.879**	
23	**ICT**						
230	***ICT***						
2304	Service Transition		600.000	741.135	n/a	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, these budget lines have been moved to Article 231 Corporate ICT expenditure*
2305	Service Operations		220.000	184.018	n/a	n/a	
2307	Service External		595.000	1.142.819	n/a	n/a	
		Article 2 3 0	1.415.000	2.067.972	0	0	
231	***Corporate ICT expenditure***						
2310	Corporate ICT recurrent costs		n/a	n/a	585.347	n/a	*This appropriation is intended to cover recurrent corporate ICT costs on hardware, software, services and maintenance as well as ENISA website and portals support.*
2311	Corporate ICT new investments and one-off projects		n/a	n/a	660.000	n/a	*This appropriation is intended to cover new investments on corporate ICT as well as one-off projects for hardware, software, services and maintenance as well as ENISA website and portals support.*
2312	Corporate ICT costs - Activity 10		n/a	n/a	n/a	1.337.203	This appropriation is intended to cover corporate ICT costs for Activity 10, recurrent costs and new investments on hardware, software, services and maintenance as well as ENISA website and portals support.

2313	Corporate ICT costs - Activity 11		n/a	n/a	n/a	334.301	This appropriation is intended to cover corporate ICT costs for Activity 11, recurrent costs and new investments on hardware, software, services and maintenance as well as ENISA website and portals support.
		Article 2 3 1		0	1.245.347	1.671.504	
		CHAPTER 2 3	**1.415.000**	**2.067.972**	**1.245.347**	**1.671.504**	
		Total Title 2	**2.677.000**	**3.150.568**	**3.547.651**	**3.257.960**	

3	**OPERATIONAL EXPENDITURE**						
30	**ACTIVITIES RELATED TO OUTREACH AND MEETINGS**						
300	***Outreach, meetings and representation expenses***						
3001	Outreach, meetings, translations and representation expenses		120.000	69.198	650.000	760.000	This appropriation is intended to cover costs of outreach activities (communications, stakeholders' management, publication and translations), meetings (including meetings of ENISA's statutory bodies i.e. MB, AG, NLOs, and meetings with other stakeholders) and other representation costs. It also covers mission costs related to the implementation of Activities 10-11 as defined in the SPD 2021-2023 mainly covering horizontal tasks and other administrative services.
		Article 3 0 0	120.000	69.198	650.000	760.000	
301	***Mission and Representation Costs***						
3011	Entertainment and Representation expenses		15.394	5.000	n/a	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, these budget lines have been moved to budget line 3001*
3016	Missions		897.930	550.767	n/a	n/a	
		Article 3 0 1	913.324	555.767	0	0	
302	***Other meetings***						
3021	Other Operational meetings		10.000	4.000	n/a	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 3001*
		Article 3 0 2	10.000	4.000	0	0	
		CHAPTER 3 0	**1.043.324**	**628.966**	**650.000**	**760.000**	
32	**HORIZONTAL OPERATIONAL ACTIVITIES**						
320	***Conferences and Joint Events***						
3200	Horizontal Operational meetings		214.608	65.448	n/a	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 3001*
		Article 3 2 0	214.608	65.448	0	0	
321	***Communication and Information dissemination***						
3210	Communication activities		150.000	205.763	n/a	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, these budget lines have been moved to budget line 3001*
3211	Internal Communication		0	45.000	n/a	n/a	
3212	Stakeholders' communication		113.000	291.358	n/a	n/a	
		Article 3 2 1	263.000	542.121	0	0	
323	***Translation and interpretation services***						
3230	Translations		30.072	120.000	n/a	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 3001*
		Article 3 2 3	30.072	120.000	0	0	
325	***Operational Systems***						
3250	Operational Systems including website development		57.000	146.079	n/a	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to Article 231 Corporate ICT expenditure*
		Article 3 2 5	57.000	146.079	0	0	
326	***Strategy and Evaluation***						
3260	Strategic consultancy		50.000	251.215	n/a	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, these budget lines have been moved to budget line 2220*
3261	External Evaluations		0	393.100	n/a	n/a	
		Article 3 2 6	50.000	644.315	0	0	
		CHAPTER 3 2	**614.680**	**1.517.962**	**0**	**0**	

36	CORE OPERATIONAL ACTIVITIES						
363	***Activity: Expertise***						
3630	Activity: Expertise		875.000	1.282.536	n/a	n/a	
		Article 3 6 3	875.000	1.282.536	0	0	
364	***Activity: Policy***						
3640	Activity: Policy		1.150.000	1.742.210	n/a	n/a	
		Article 3 6 4	1.150.000	1.742.210	0	0	
365	***Activity: Capacity***						
3650	Activity: Capacity		535.000	798.982	n/a	n/a	
		Article 3 6 5	535.000	798.982	0	0	
366	***Activity: Community***						
3660	Activity: Community		650.000	1.358.326	n/a	n/a	
		Article 3 6 6	650.000	1.358.326	0	0	
		CHAPTER 3 6	**3.210.000**	**5.182.053**	**0**	**0**	

As from 2021, whereas the budget structure has been aligned with the SPD, these budget lines have been moved to Chapter 37

37	**CORE OPERATIONAL ACTIVITIES**						
371	***Activity 1 - Providing assistance on policy development***						
3710	Activity 1 - Providing assistance on policy development		n/a	n/a	280.000	316.024	This appropriation is intended to cover direct operational costs relevant to the Activity 1 (including operational ICT and mission costs).
		Article 3 7 1	0	0	280.000	316.024	
372	***Activity 2 - Supporting implementation of Union policy and law***						
3720	Activity 2 - Supporting implementation of Union policy and law		n/a	n/a	985.000	1.036.191	This appropriation is intended to cover direct operational costs relevant to the Activity 2 (including operational ICT and mission costs).
		Article 3 7 2	0	0	985.000	1.036.191	
373	***Activity 3 - Capacity building***						
3730	Activity 3 - Capacity building		n/a	n/a	1.400.000	1.460.120	This appropriation is intended to cover direct operational costs relevant to the Activity 3 (including operational ICT and mission costs).
		Article 3 7 3	0	0	1.400.000	1.460.120	
374	***Activity 4 - Enabling operational cooperation***						
3740	Activity 4 - Enabling operational cooperation		n/a	n/a	1.110.000	1.163.881	This appropriation is intended to cover direct operational costs relevant to the Activity 4 (including operational ICT and mission costs).
		Article 3 7 4	0	0	1.110.000	1.163.881	
375	***Activity 5 - Contribute to cooperative response at Union and Member States level***						
3750	Activity 5 - Contribute to cooperative response at Union and Member States level		n/a	n/a	1.200.000	1.255.817	This appropriation is intended to cover direct operational costs relevant to the Activity 5 (including operational ICT and mission costs).
		Article 3 7 5	0	0	1.200.000	1.255.817	
376	***Activity 6 - Development and maintenance of EU cybersecurity certification framework***						
3760	Activity 6 - Development and maintenance of EU cybersecurity certification framework		n/a	n/a	870.000	918.717	This appropriation is intended to cover direct operational costs relevant to the Activity 6 (including operational ICT and mission costs).
		Article 3 7 6	0	0	870.000	918.717	
377	***Activity 7 - Supporting European cybersecurity market and industry***						
3770	Activity 7 - Supporting European cybersecurity market and industry		n/a	n/a	490.000	530.542	This appropriation is intended to cover direct operational costs relevant to the Activity 7 (including operational ICT and mission costs).
		Article 3 7 7	0	0	490.000	530.542	
378	***Activity 8 - Knowledge on emerging cybersecurity challenges and opportunities***						
3780	Activity 8 - Knowledge on emerging cybersecurity challenges and opportunities		n/a	n/a	1.155.000	1.209.849	This appropriation is intended to cover direct operational costs relevant to the Activity 8 (including operational ICT and mission costs).
		Article 3 7 8	0	0	1.155.000	1.209.849	
379	***Activity 9 - Outreach and education***						
3790	Activity 9 - Outreach and education		n/a	n/a	1.010.000	561.729	This appropriation is intended to cover direct operational costs relevant to the Activity 9 (including operational ICT and mission costs).
		Article 3 7 9	0	0	1.010.000	561.729	

CHAPTER 3 7	0	0	8.500.000	8.452.869
TITLE 3	**4.868.004**	**7.328.981**	**9.150.000**	**9.212.869**
GRAND TOTAL	**16.932.952**	**21.682.884**	**23.473.060**	**23.608.060**

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 2022[1]

Category and grade	Establishment plan in voted EU Budget 2021		Establishment plan 2022	
	Off.	TA	Off.	TA
AD 16				
AD 15		1		1
AD 14				
AD 13		1		2
AD 12		5		4
AD 11		2		2
AD 10		3		4
AD 9		12		11
AD 8		21		22
AD 7		8		8
AD 6		4		6
AD 5				
Total AD		**57**		**60**
AST 11				
AST 10				
AST 9				
AST 8		1		2
AST 7		4		3
AST 6		8		8
AST 5		5		5
AST 4		1		1
AST 3				
AST 2				
AST 1				
Total AST		**19**		**19**
AST/SC1				
AST/SC2				
AST/SC3				
AST/SC4				
AST/SC5				
AST/SC6				

[1]The change in the number of establishment plan up to 10% requested for year 2022 is modified as per Art 38 of the ENISA Financial Regulation

Total AST/SC				
TOTAL		**76**		**79**