*European Union Agency for Cybersecurity*

# DECISION No MB/2022/1 of the Management Board of the European Union Agency for Cybersecurity (ENISA) endorsing the draft Programming Document 2023-2025, the draft Statement of estimates 2023 and the draft Establishment plan 2023

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 2022;

(2) The Management Board should endorse the draft programming document by 31 January 2022;

(3) The Executive Board has endorsed the draft single programming document 2023-2024 at its meeting held on 20 January 2022.

(4) The Agency should send the draft programming document to the Commission, the European Parliament and the Council no later than 31 January 2022;

[1] *OJ L 151, 7.6.2019, p. 15–69*

HAS DECIDED TO ADOPT THE FOLLOWING DECISION:

**Article 1**

The Programming Document 2023-2025 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 2023 and the Establishment plan 2023 are endorsed as set-out in Annex 2 and Annex 3 of this decision.

**Article 3**

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

Done by written procedure on 31 January 2022

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 2023-2025

Including Multiannual planning,
Work programme 2023 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 2021 | V.01 | MB for consultation | ENISA |
| January 2022 | V.02 | MB feedback | MB |
| January 2022 | V.03 | Sent to EB | ENISA |
| January 2022 | V.1 | For adoption by MB | ENISA |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# TABLE OF CONTENTS

# LIST OF ACRONYMS

To be updated at a later stage

| | |
|---|---|
| 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 |
| CEF | Connecting Europe Facility |
| 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 |
| ECA | 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 |
| JCU | Joint Cyber Unit |
| 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 |
| SOCs | Security Operation Centres |
| SOP | Standard Operating Procedure |
| SPD | Single Programming Document |

# INTRODUCTION

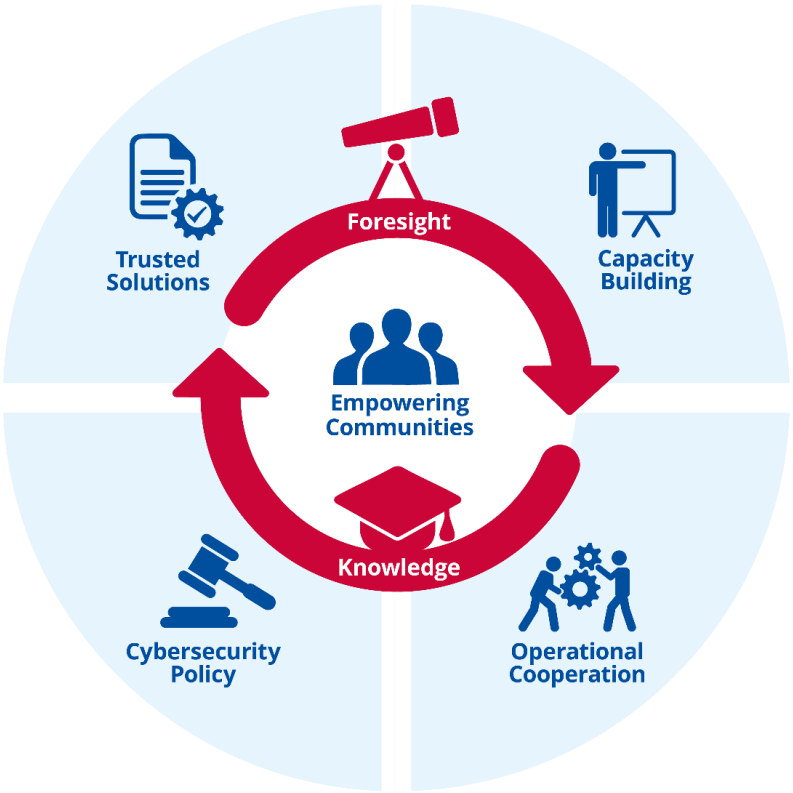
## FOREWORD

To be updated at a later stage

## 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 SOLUTIONS

Digital products and services bring benefits as well as risks, and these risks must be identified and mitigated. In the process of evaluating security of digital solutions and ensuring their trustworthiness, it is essential to adopt a common approach, with the goal to strike a balance between societal, market, economic and cybersecurity needs. A neutral entity acting in a transparent manner will increase customer trust on digital solutions and the wider digital environment.

### 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

To be updated at a later stage

The below general context reflects the time of writing of December 2021. This will be significantly updated in the course of 2022 in accordance with the latest policy developments and taking into account the strategic and prioritisation discussions within the Management Board foreseen in the first half of 2022.

The 2021 State of the Union Address by President von der Leyen[1] kept cybersecurity clearly among the Commission's policy priorities, raising the ambitions to "not just be satisfied to address the cyber threat, but also strive to become a leader in cybersecurity" and recognising that "if everything is connected, everything can be hacked". It also, includes legislation on common standards, under a new European Cyber Resilience Act. The issues covered build on the EU's Cybersecurity Strategy[2] for the Digital Decade, released in December 2020 and efforts to ensure the EU's technological sovereignty. The Agency is ready to utilise fully its mandate and tasks to step up and support the Union to be a leader in cybersecurity and to fulfil its vision of a trusted and cyber secure Europe.

**Cybersecurity threat landscape 2021**

The final general context of the 2023 Single Programming Document will be based on the developments of the Threat Landcape assessment during 2022. Currently at the time of writing, the ENISA's 9th edition of its annual Threat Landscape Report[3] (ETL) confirmed current and future trends that cyberattacks are becoming ever more sophisticated, targeted, widespread, un-attributable and detected too late . These continue to be global trends and their impact has been equally felt in Europe. Cybercriminals are increasingly motivated by monetisation of their activities such as ransomware, the focus of the 9th ETL. The focus on Ransomware as a Service (RaaS) type business models increased over 2021, making proper attribution of individual threat actors difficult, this led to the occurrence of triple extortion ransomware schemes increasing strongly over the course of 2021. Several widespread vulnerabilities with a high risk of exploitation were disclosed in the course of 2021 and led to a highly increased attack surface. During the reporting period, a large number of incidents targeted public administration and government and digital service providers. The health sector was also targeted significantly, and this activity shows signs of increasing during the last few months of the reporting period (May-July 2021).

In addition highly sophisticated and impactful supply chain compromises proliferated, as highlighted by the dedicated ENISA Threat Landscape for Supply Chain. The number of data breach incidents continues to be very high, and the amount of stolen financial information and user credentials is growing. The current escalation and the threat landscape status require ever new methods and a different approaches for Europe to become cyber secure.

**Legislative measures designed to strengthen and respond to the threat landscape**

The adoption and implementation of policy frameworks is one key response area where the EU is making a difference. Indeed, the policies and initiatives being put in place in the coming years are determining

[1] 15th September 2021 State of Union speech 24_4701
[2] 16th December 2020 New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient_20_2391
[3] 27th October 2021 ENISA Threat Landscape 2021

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:

**NIS2**

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 envisages far more entities obliged to take measures to increase the level of cybersecurity in Europe. So far, the NIS2 negotiations in the European Parliament (EP) and the Council have showed a unique cross-party / cross-Member State consensus on the direction of the Directive. Both the Council General Approach and the EP report have taken a constructive approach in the strengthening of cybersecurity in Europe and have placed ENISA in a strong supporting role. Both envisage new and/or strengthened tasks for ENISA, and additional provisions regarding new resources to realise its ambitions and meet expectations supporting those tasks have been included for example in the EP report. While five FTE positions should be 'freed' once the NIS2 proposal is adopted, ENISA continues to call for additional SNE capacity. To meet the ambitious timetable means that the new action areas need to be tackled and prepared immediately. At ENISA level such preparations are already underway and are reflected in this draft Single Programming Document (SPD).

The 2nd ENISA NIS investment study shows that the incentives to invest properly in cybersecurity are not there yet. The majority of Operators of Essential Services (OES) and Digital Service Providers (DSPs) acknowledged a significant positive impact of the NIS Directive particularly in detecting information security incidents. However, the implementation of the NIS Directive did not necessarily result in substantial increases in the cybersecurity budgets of organisations. Specifically, 67% of organisations required additional budgets to implement NIS Directive requirements. Furthermore, the average Information security spent for OES & DSP in the EU is 10,4 M€, but the average is skewed by large organizations spending significant amounts in information security, as the median value for information security spent is 2 M€. On median OES & DSP allocate 7.7% of their IT budget to information security. How these figures evolves over the coming years will be tracked to determine whether investments in cybersecurity are being prioritised.

ENISA is already invested in activities linked to the development and the implementation of the NIS Directive , with its 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, using existing resources and building on these wherever necessary.

**Joint Cyber Unit**

The type of investment described above also supports any increased cooperation under the potential Joint Cyber Unit umbrella. ENISA will contribute to the implementation of the EC Recommendation (4520 (2021) on 'building the Joint Cyber Unit') and Council Conclusions (20 October 2021 (ST 13048 2021) on 'exploring the potential of the Joint Cyber Unit initiative - complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises'), with a view to contributing to the further development of an EU crisis management framework along the lines and according to the roles defined in the on-going discussions amongst Member States and EU operational actors. This could include fostering cooperation among cybersecurity communities, amongst relevant EU institutions, bodies and agencies as well as within civilian (and between) cooperation networks (i.e. the Cyber Crisis Liaison Organisation Network (CyCLONe) or computer security incident response team network (CSIRTs Network) and, to the extent needed, the Cooperation Group). In 2021, ENISA undertook mapping exercises in the form of three dedicated workshops involving Member States and EU Institutions, Bodies and Agencies (EUIBAs).

**Implementation of the EU cybersecurity certification framework**

ENISA is playing a central role in supporting the implementation of the European cybersecurity certification framework by preparing and maintaining the candidate schemes. In this task ENISA is supported by area experts and operates in collaboration with public authorities in the Member States. 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 for the conformity assessment of digital products, services and processes in the Digital Single Market under those schemes, which can contribute to increasing the level of customer trust of digital solutions in the Union. Currently, ENISA has prepared a candidate scheme on EU Common Criteria European candidate cybersecurity certification scheme (EUCC) for which an EU Implementing Act for its final adoption is currently being proposed by the Commission. In early 2022 the candidate scheme on Cloud Services (EUCS) will be submitted to the ECCG for its opinion. Furthermore, an ad hoc working group recently started working to prepare a candidate certification scheme for 5G networks (EU5G), which will further augment the involvement of ENISA in cybersecurity certification.

Finalizing the candidate schemes for specialized product categories under the EU Common Criteria (EUCC) scheme and for cloud services is just the first step and it will likely bring about benefits in terms of recognition and trust across government services, business and citizens during the time period 2023-2025.

**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 Competence Centre and the Network[4]. This leads to a better and balanced coordination of the funding programme objectives between the Member States. In 2021, ENISA worked together in setting up the European Cybersecurity Competence Centre (ECCC) and is involved in advanced discussions on joint administrative services with the new centre. The Agency will provide strategic advice to the Governing Board and act as permanent observer to the Governing Board, play an active part in the activities of the Competence Centre, cooperate and ensure synergies with the Centre, provide relevant input during the preparation of the ECCC Agenda, Work Programmes and Multiannual Work Programme (Articles 5, 8, 10, 12, 18 of the ECCC Regulation EC 2021/887).

**The European Digital Identity Framework**

Digital identity 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 Electronic Identification and Trust Services (eIDAS) Regulation and identified several gaps. In June 2021 the Commission made a proposal for a revised eIDAS regulation establishing a European Digital Identity framework and a European Digital wallet, to be available for all EU citizens, for online transactions with government entities, but also with businesses. In the 2023-2025 period, ENISA will support Member States and the Commission with the development of the Digital Wallet toolbox and the European Digital Identity Framework, as set out in Commission Recommendation of 3.6.2021[5] in addition to promoting the exchange of good practises and capacity building of relevant stakeholders. The revised eIDAS regulation also includes new trust services in scope like distributed ledgers and electronic archiving. The NIS2 proposal for a revised NIS Directive foresees that the security obligations laid down in

[4] Regulation (EU) 2021/887 of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres
[5] Commission Recommendation C(2001) 3968 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework.

this Directive should be considered complementary to the requirements imposed on trust service providers under Regulation (EU) No 910/2014 (eIDAS Regulation If this proposal is adopted, ENISA will support Member States and the Commission with this transition, to ensure that the trust service providers and the national authorities can benefit from the NIS Directive ecosystem

**Artificial Intelligence (AI)**
With the EU's AI agenda advancing rapidly following the European Commission proposal on AI[6] and Coordinated Plan on Artificial Intelligence 2021[7], 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 future AI services and applications.

Building on ENISA's efforts towards securing AI / machine learning of December 2021[8] the existing work of the member states in this area and with the guidance from its Ad Hoc Expert Group on AI[9], the Agency can continue its open dialogue with EU institutions in support of the legislative initiatives reaching into 2023-2025. For this, ENISA should systematically record the existing initiatives from the member states in this area, ENISA could continue supporting the Commission and Member States by providing good security practices and guidelines. Consequently ENISA should coordinate the development of a certification scheme for AI systems on short notice, following adoption of the legislative proposal.

**Digital Operational Resilience Act (DORA)**
In 2021 the European Commission published a legislative proposal for a regulation on Digital Operational Resilience in the EU financial services sector ("DORA"). ENISA welcomes the current European Parliament amendments, which retain and even augment the tasks and responsibilities of ENISA in certain areas, e.g. harmonization and incident reporting templates, risk management framework, the joint report, and the revised text on cross-sector exercises and communication in case of major cyber crises. ENISA's welcomes it role and responsibilities and requests that they should be elaborated further to be effective for the Agency and to meet expectations.

**Further developments**
In 2021 ENISA established a local office in Brussels in accordance with CSA Art 20 (5), and will become operational in 2022. This fortifies ENISA's position in the digital ecosystem of the Union and in particular its role in establishing synergies with Union institutions, bodies, offices and agencies in the field of operational cooperation at the Union level. Moreover, the local office in Brussels aims to ensure regular and systematic cooperation with Union institutions, bodies and agencies and other competent bodies involved in cybersecurity. Indeed, it will support the delivery of tasks mandated to ENISA under Article 7 of the CSA, in particular that of establishing and maintaining structured cooperation with the Computer Emergency Response Team for the Union's institutions, bodies and agencies (CERT-EU). A detailed and annual cooperation plan is being integrated into ENISA's Single Programming Document and is part of the MoU signed in early 2021. Here both organizations will be able to benefit from synergies provided by proximity and daily contact and steer clear from any duplication of activities.

[6] Proposal for a Regulation (EU) 2021/ 206 of 21 April 2021 laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts
[7] https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review
[8] Artificial Intelligence: How to make Machine Learning Cyber Secure? — ENISA (europa.eu)
[9] Artificial_intelligence/ad-hoc-working-group

# SECTION II. MULTI-ANNUAL PROGRAMMING 2023 – 2025

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 medium to 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 medium to long-term goals for the Agency.

## 1. Multi-annual work programme

The following table maps the strategic objectives stemming from ENISA's strategy[10], against the respective articles of the CSA. It furthermore integrates the activities of the Work Programme showing how the progress in the achievement of the objectives is monitored. These objectives shall be reviewed if applicable through the ENISA Management Board as from 1 July 2024.

[10] The ENISA strategy entered into force on the 31 July 2020 and the Management Board shall launch a review procedure, if relevant, as from 1st July 2024.

| STRATEGIC OBJECTIVE | ACTIONS TO ACHIEVE OBJECTIVE | ARTICLE OF THE CSA | EXPECTED RESULTS | KPI | METRICS [11] |
|---|---|---|---|---|---|
| **SO1**<br>**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<br>An EU-wide, state of the art body of knowledge on cybersecurity concepts and practices, that builds cooperation amongst key actors in cybersecurity, promotes lessons learned, EU expertise and creates new synergies | Community-building across the cybersecurity ecosystem | Additional quantitative measures stemming from the stakeholder strategy to be finalised in 2022<br>Stakeholder satisfaction of ENISA's role as facilitator of community-building and collaboration across the cybersecurity ecosystem |
| **SO2**<br>**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<br>2. Number of references to ENISA reports, analysis and/or studies in EU and national policy documents (survey)<br>3. Satisfaction with ENISA added-value of contributions (survey) |
| | | | • Consistent implementation of Union policy and law in the area of cybersecurity<br>• EU cybersecurity policy implementation reflects sectorial specificities and needs<br>• 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<br>2 Number of ENISA reports, analysis and/or studies referred to at the EU and national level (survey)<br>3 Satisfaction with ENISA added-value of support (survey) [12] |

[11] Baselines for these metrics should be known by the end of 2021, Therefore targets linked to these baselines will be developed for the 2023 work programme only in 2022.
[12] Surveys will be designed and developed in order to solicit a measurable response from participants to determine the added value of ENISAs contribution.

| | | | | | |
|---|---|---|---|---|---|
| **SO3**<br>**Effective cooperation amongst operational actors within the Union in case of massive[13] cyber incidents** | Activities 4 & 5 | Art.7 | • All communities (EU Institutions and MS) use streamlined and coherent set of SOPs for cyber crises management<br>• Efficient, 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<br>2. Uptake of the platform/ tool/ SOPs during massive cyber incidents<br>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<br>• Public informed on a regular basis of important cybersecurity developments<br>• Stakeholders aware of current cybersecurity situation | ENISA ability and preparedness 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<br>2. Number of relevant incident responses ENISA contributed to as per CSA Art7<br>3.Stakeholders' satisfaction of ENISA's ability to provide operational support |
| **SO4**<br>**Cutting-edge competences and capabilities in cybersecurity across the Union** | Activities 3 & 9 | Art.6 and Art.7(5) | • Enhanced capabilities across the community<br>• Increased cooperation between communities | Increased resilience against cybersecurity risks and preparedness to respond to cyber incidents | 1. Increase/decrease of maturity indicators<br>2. Outreach, uptake and application of lessons learnt from capability-building activities.<br>3. Number of cybersecurity programmes (courses) and participation rates<br>4. The number of exercises executed annually.<br>5. Stakeholder assessment on usefulness, added value an relevance of ENISA; and cooperation amongst communities in capacity building activities |

[13] large scale and cross-border

| | | | | | |
|---|---|---|---|---|---|
| | | Art.10 & Art.12 | • Greater understanding of cybersecurity risks and practices<br>• Stronger European cybersecurity through higher global resilience. | Level of awareness on cybersecurity, cyber hygiene and cyber literacy across the EU<br>Level of outreach | 1. Number of cybersecurity incidents reported having human error as a root cause<br>2. Number of activities and participation to awareness raising actions organised by ENISA on cybersecurity topics<br>3. Geographical and community coverage of outreach in the EU<br>4. Level of awareness, on cybersecurity across the EU/ general public (e.g. EU barometer) |
| **SO5**<br>**High level of trust in secure digital solutions** | Activities 6 & 7 | Art.8 | Draft cybersecurity certification schemes developed by ENISA under the European cybersecurity certification framework are adopted<br>Smooth transition to the EU cybersecurity certification framework<br>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 more secure digital solutions<br>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<br>2. Stakeholders trust in digital solutions of certification schemes ( Citizens, public sector, businesses)<br>3. Uptake of certified digital solutions (products, services and processes) using certification schemes under the CSA framework<br>4. Number of candidate certification schemes prepared by ENISA<br>5. Number of people/organizations engaged in the preparation of certification schemes<br>6. Satisfaction with ENISA's support in the preparation of candidate schemes (survey) |
| | | | • Contribution towards understanding market dynamics<br>• A more competitive European cybersecurity industry, SMEs and start-ups | Effectiveness of ENISAs supporting role for participants in the European cybersecurity market | 1. Number of market analysis, guidelines and good practices issued by ENISA<br>2. Uptake of lessons learnt / recommendations from ENISA reports<br>3. Stakeholder satisfaction with the |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | added value and quality of ENISA's work |
| **SO6**<br>**Foresight on emerging and future cybersecurity challenges** | Activity 8 | Art.11 & Art. 9 | • Research and innovation areas tied to the cybersecurity needs and requirements, including contributing to the work of the European Cybersecurity Competence Centre | 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.<br>2. Stakeholder satisfaction on the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges & opportunities (incl in research) |
| **SO7**<br>**Efficient and effective cybersecurity information and knowledge management for Europe** | Activity 8 | Art.9 & 11 | •<br>Decisions about cybersecurity are future proof and to take account the trends, developments and knowledge across the ecosystem<br>• 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)<br>2 Number of recommendations, analysis, challenges identified and analysed<br>3 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<br>Building lasting credibility and trust | 1. Organisational performance<br>2. Trust in ENISA brand | 1. Proportion of KPI's reaching targets<br>2. Individual contribution to achieving the objectives of the agency via clear link to KPI's (CDR report)<br>3. Exceptions in Risk Register<br>4. Number of complaints filed against ENISA incl number of inquiries/ complaints of the EU Ombudsman<br>5. Number of complaints addressed timely and according to relevant procedures<br>6. Results of annual risk assessment exercise<br>7. Observations from external audit bodies European Court of Auditors (ECoA) |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings and number of observations successfully completed and closed<br>8. Level of trust in ENISA (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)<br>2. Quantity and quality of ENISA training and career development activities organised for staff<br>3.Reasons for staff departure (exit interviews)<br>4.Staff retention/turnover rate<br>5.Resilience and quality of ENISA IT systems and services (including ability to consistently increase satisfaction with IT services & tools) |

# 2. HUMAN AND FINANCIAL RESOURCES - OUTLOOK FOR YEARS 2023 – 2025

## 2.1 OVERVIEW OF THE PAST AND CURRENT SITUATION

To be updated at a later stage

**Table 1a**

| | 2019 | 2020 | 2021 | 2022[14] |
|---|---|---|---|---|
| **Number of posts in the Establishment Plan** | 59 | 69 | 76 | 82 |
| **% of fulfilment of the establishment plan (on 1st of January)** | 76% | 80% | 80% | 94% |

As an Agency, ENISA has historically always struggled to meet its human resources needs and take steps to ensure timely and rapid fulfilment of its Establishment Plan. The gap between the available posts and the fulfilment is evidenced in the table above. This has hampered the Agency to make use of its potential capabilities in the most efficient manner, resulting in a smaller real capacity of the Agency in terms of its human resources.

In 2021 the Agency put in place was to introduce an annual strategic workforce planning framework, which prompts the organisation to analyse its human resources needs ahead, on multiannual basis on the basis of the Single Programming Document, and plan and review the allocation of human resources between different activities as well as prepare new recruitment calls well in advance of the enactment of the applicable annual Establishment Plans. It also enables the Agency to take corrective action if and when necessary, to achieve the aims set out in Article 3(3) of the MB decision MB/2020/9, which foresees that the Executive Director will ensure that: "The average number of staff members assigned to the Executive Directors Office (EDO) and Corporate Support Services (CSS) [offices and services supporting the functioning of the Agency] shall not exceed the average number of staff members assigned to units [executing the objectives and tasks of the Agency]."

In the course of the 2021 Strategic Workforce Review, the Agency, along with other measures, reallocated altogether 4 posts from EDO and CSS, to be able to meet the threshold foreseen in Article 3(3) of MB/2020/9. This resulted in a termination of 1 contract and the prolongation of 2 contracts was put under review. The posts are now allocated to the operational units of Policy Development & Implementation Unit (PDI), Capacity Building Unit (CBU) and Market, Certification and Standardisation Unit (MCS), to be fulfilled via ongoing recruitment calls. The original impact that the conclusions of the 2021 Strategic Workforce Review was supposed to bring are summarised in the table below:

[14] 3 AD posts subject to budget approval EC-NIS2 activities; projection of EP fulfilment on 01.01.2022 depends on successful conclusions of ongoing selections Q4 2021.

Table 1b

| | Operational units | | Supporting offices and services | |
|---|---|---|---|---|
| | *Established staff (TAs & CAs)* | ***average*** | *Established staff (TAs & CAs)* | ***average*** |
| **Allocated as of 01.01.2021** | 48 | **12** | 38 | **19** |
| **Current allocation (01.10. 2021)** | 67 | **16.75** | 40 | **20** |
| **Projected allocation (01.01.2022)** | 79 | **19.75** | 40 | **20** |

## 2.2 OUTLOOK FOR THE YEARS 2023 – 2025

## 2.3 RESOURCE PROGRAMMING FOR THE YEARS 2023 – 2025

### 2.3.1 Financial Resources

To be updated at a later stage

In 2021 the financial structure of the title 3 budget was revised to match the activities of Single Programming Document, in accordance with the CSA. This budget structure aims to implement activity based budgeting and cost based reporting thus allowing ENISA to make budgetary decisions based on specific activity budgetary drivers and their importance to the Agency's activities.

To strengthen budget management, the Agency established the Budget Management Committee (BMC) in 2021 to ensure the coherent planning, implementation and follow-up of the Agency's budget. The mandate of the BMC encompasses the entire lifecycle of the budget, including assisting in setting the overall framework and guiding the development, roll-out and implementation as well as follow-up and analysis of the budget. The committee gives recommendations to the Executive Director (ED) on the execution of the budget including the steps, which should be taken in order to ensure proper planning and implementation of the annual budget of the Agency, and give feedback on the utilization and budget implementation of the relevant units and managers.

The introduction of the BMC and activity based budgeting have allowed enhanced monitoring of financial planning, leading to a more efficient execution of the budget. Concretely, higher budgetary execution rate and fewer budgetary transfers are expected as a result of this, as evidenced in 2021. The budgetary execution rate in 2021 increased to 99,51% of the budget vs 97,35% in 2020 and there were five internal transfers by ED decision versus seven in 2020 and ten in 2019.

As such and based on lesson learned from 2021 the Agency has extended this efficiency to title 1 and title 2 by merging budget lines of these titles in the 2023 budget. By reducing the number of budget lines from 30 to 11 for title 1 and 2, the Agency will be able to reduce the number of ED decisions required to transfer budget lines thus reducing administrative burden and enhance the quality of the monitoring and reporting of the budget. The budget lines consolidated were those budget lines with less 500 kEUR within the same type / category of expenditure in title 1 and 2. The consolidated budget lines are reflected in the statement of estimates submitted and adopted along-side the draft SPD23-25.

The total EU contribution to ENISA over the period from 2023 to 2025, as well as for the full period of the new multiannual financial framework 2021–2027, is planned to remain stable, with a slight annual increase of circa 2% to reflect inflation (see the table below).

**Table 2**

| | 2022 (*) | 2023 (**) | 2024 (**) | 2025 (**) |
|---|---|---|---|---|
| **Total appropriations for ENISA *(thousand EUR)*** | 24 208 | 24 707 | 25 219 | 25 629 |

*Source: (*) Draft Union's annual budget for financial year 2022 COM (2021) 300 (**) Fiche no. 68 – MFF 2021-2027 dated of 08/06/2020 and an additional amount of EUR 610.000 has been added subject to the approval of the NIS2 proposal.*

As from 2023, ENISA's revenue is composed of 97.6 % of ENISA's revenue from the EU contribution and 2.4 % was from the European Economic Area (EEA) country contribution (Table 6 in Annex III). In absolute term, the EU and EEA contribution for 2023 is estimated respectively to reach EUR 24.1 million and EUR 0.6 million.

The general allocation of funds across titles is expected to remain stable over the period 2023–2025. Expenditure in 2023 is expected to amount to EUR 24.7 million, of which EUR 13 million in Title 1 covers all staff-related costs (53%), EUR 2.9 million in Title 2 covers main items such as building related expenditure and ICT expenses (12%) and EUR 8.8 million in Title 3 covers all core operating expenditure (35%). Total expenditures include the reserve budget of EUR 610 thousand expected to be allocated to cover additional staff (3 TAs and 2 CAs) to manage part of the activities linked to the NIS directive in discussion by legislators.

### 2.3.2 Human Resources

In its budget proposal for the Single Programming Document (SPD) 2023 – 2025, the Agency asks for an extra four SNE posts (introduced gradually 2+2 over 2 years as of 2023). The four additional SNE posts requested would be justified both by the Agency's current activity areas, particularly the operational needs stemming from Article 7 of the CSA as well as by those extra activities and requirements, as foreseen especially in the initial phases laid out in the Commission's Recommendation on the Joint Cyber Unit (JCU) of 23 June 2021.

**This is also the most cost effective solution for the Agency to fulfil its mandate and adds the most value for Member States.**

The collective knowledge acquired from the Member State's perspective through such posts will be crucial for the success of these tasks. In fact, by importing unique expertise and knowledge into the Agency through SNE posts rather than having to outsource certain tasks or create any dependencies on other external staff, ENISA is catering for the increasing activities which require close cooperation with Member States as part of its mandate. Higher SNE turnovers will in turn be of direct benefit for all Member States and offer a rich experience to SNEs following their posting.

In 2021 the Agency's request for two additional SNEs for 2022 did not materialise, the Agency therefore has taken the decision to transfer two SNE posts that were earmarked for other operational units and will transfer them to the Operational Cooperation unit in 2022 specifically for tasks related to Article 7 of the CSA.

This decision to transfer posts from other operational units will have consequences in terms of those units' capacity to carry out their tasks. Therefore the Agency will need to seek alternative ways to compensate for this decision in order to fulfil its mandate and tasks. Such measures include the re-allocation of further resources from across the

Agency to the operational units and specifically to the Operational Cooperation Unit, inevitably leading to gaps across certain functions of the Agency that will need to be covered by externalising these tasks to contractors. This affect is further compounded by the lower than required graded posts stemming from the NIS2 proposal (3 AD posts) which was authorised by the draft EU general budget for 2022.

**As such, the Agency will put forward a request for a budget increase of approximately 1.000.000 EUR to cover the two SNEs that didn't materialise in 2022 and the lower graded posts from the NIS2 proposal.**

Lastly the strategic discussions stemming from the MB meeting in the first half of 2022 could lead to additional resource requirements for the Agency.

## 2.4 STRATEGY FOR ACHIEVING EFFICIENCY GAINS

To be updated at a later stage

ENISA is committed to continuously implementing measures to obtain efficiency gains in all activities. In 2021 the ENISA organisational structure was 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 Stakeholder Cybersecurity Certification Group (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 as 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 European Union Intellectual Property Office (EUIPO) and in 2021 the Agency signed a cooperation plan with European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA). In addition ENISA and European Centre for the Development of Vocational Training (CEDEFOP) are strengthening their cooperation to streamline procurement, share financial services, increase efficiency gains in human resources, explore IT solutions together and to support each other in the area of data protection. The aim is to share knowledge and utilise human resources in the most efficient manner between the two agencies that results in better value for EU citizens.

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 accrual-based accounting (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 Missions Integrated Processing System (MIPS) and Advanced Record System (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…).

In 2021 the Agency has established a 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 2023

To be updated at a later stage and reviewed on the basis of the strategic discussions taking place in the MB in March and June

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 nine operational activities and two corporate activities have been identified to support the implementation of ENISA's mandate in 2023.

The activities of the work programme seek to mirror and align with the tasks set out in chapter two of the CSA, demonstrating concretely not only the specific objectives, results and outputs expected for each task but also the resources assigned.

## 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 and on the basis of the 2020 EU Cybersecurity Strategy. While aspects such as privacy and personal data protection are taken into consideration (incl encryption).

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 , 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 for policy development, as well as develop monitoring capabilities and tools to regularly and consistently be able to provide advice on the effectiveness of the existing Union policy and law in accordance with the EU's institutional competencies in the 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 risk- based analysis of cybersecurity not only in the areas of critical infrastructure and sectors, but also by providing advice 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 the existing frameworks and 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 cybersecurity policy frameworks<br>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 and cyber insurance and other potential initiatives (e.g. The Once Only Technical Solution)<br>1.3 Assist the Commission in reviewing existing policy initiatives and maintain a catalogue of all relevant cyber security legislation and policies at the EU level | **Indicator:** ENISA's added value to EU institutions, bodies and Member States in providing support to policy-making (ex-ante)<br>**Metric:**<br>1.1 Number of relevant contributions to EU and national policies and legislative initiatives[15]<br>1.2 Number of references to ENISA reports, analysis and/or in EU and national policy documents (survey)<br>1.3 Satisfaction with ENISA added-value of contributions (survey)<br>**Frequency:** Annual 1 &2, biennial 3 |
| **VALIDATION** | **TARGET GROUPS AND BENEFICIARIES** |
| • NIS Cooperation Group (NIS CG) and other formally established Groups (outputs 1.1 and 1.2)<br>• ENISA ad hoc working groups[16] (outputs 1.1 and 1.2)<br>• NLO Network, 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) and of electronic communications services |

**RESOURCES PLANNED**

| Human Resources (FTE) | | | Financial Resources | EUR |
|---|---|---|---|---|
| Total | [17] | | Total | [18] |

[15] Baselines for these metrics should be known by the end of 2021, Therefore targets linked to these baselines will be developed for the 2023 work programme only in 2022.
[16] created under Art 20(4) of CSA
[17] FTEs to be updated at a later stage
[18] budgetary figures to be updated at a later stage

# Activity 2 Supporting implementation of Union policy and law

## OVERVIEW OF ACTIVITY

The activity provides support to Member States 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, electronic identification (eID), including the European Digital Identity Framework and trust services, vulnerability disclosure policies and the general availability or integrity of the public core of the open internet.

It further supports initiatives related to implementation of policy frameworks such as 5G and European Electronic Communications Code (EECC) and on novel digital technologies such as 5G, and assisting the work of the NIS Cooperation Group and its work streams.

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, following a consistent approach between cybersecurity, privacy and data protection.

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

## OBJECTIVES

- Consistent development of sectorial Union policies with horizontal Union policy 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 aiming to support consistency 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<br>• EU cybersecurity policy implementation reflects sectorial specificities and needs<br>• Wider adoption and implementation of good practices | • Cybersecurity as an integral part of EU policies<br>• Empowered and engaged communities across the cybersecurity ecosystem |

| OUTPUTS | KPI |
|---|---|
| 2.1 Support the implementation of the NIS Directive and the activities of the NIS Cooperation Group<br>2.2 Support MS and the EC in the implementation of cybersecurity aspects of sectorial Union policy e.g. Digital Operational Resilience Act (DORA), Electricity Network Code on cybersecurity and on security of the public core of the open internet.<br>2.3 Support MS and EC in the implementation and monitoring of Union policy in the area of electronic communications security, EECC and 5G (e.g. 5G Cybersecurity Toolbox).<br>2.4 Provide advice, Issue technical guidelines and facilitate exchange of good practices to support MS and EC on the implementation of cybersecurity policies in the areas of eID, trust services, and security measures for data protection and privacy<br>2.5 Assisting in establishing and implementing vulnerability disclosure policies considering also the NIS2 proposal. | **Indicator:** Contribution to policy implementation and implementation monitoring at EU and national level (ex-post)<br>**Metric:**<br>2.1 Number of EU policies and regulations implemented at national level supported by ENISA<br>2.2 Number of ENISA reports, analysis and/or studies referred to at the EU and national level (survey)<br>2.3 Satisfaction with ENISA added-value of support (survey)<br>**Frequency:** Annual 1 & 2, biennial 3 |

| VALIDATION | TARGET GROUPS AND BENEFICIARIES |
|---|---|
| • NIS Cooperation Group or established work streams (Outputs 2.1, 2.4, 2.5)<br>• Art19 and European Competent Authorities for Secure Electronic Communications (ECASEC) expert groups (Output 2.3)<br>• Formally established bodies and expert groups as necessary (Outputs 2.2, 2.4, 2.5)<br>• ENISA Ad Hoc Working Groups and Expert Groups (Outputs 2.1, 2.4)<br>• NLO Network (as necessary) | • MS Cybersecurity Authorities (NISD CG members), National Supervisory Authorities, Data Protection Authorities, National Accreditation Bodies, National Regulatory Authorities<br>• EC, EU Institutions/ bodies (e.g. Body of European Regulators for Electronic Communications (BEREC), European Data Protection Supervisor (EDPS), European Data Protection Board (EDPB), European Railway Agency (ERA), European Maritime Safety Agency (EMSA) and sectorial EU Agencies (e.g. ACER) and Interinstitutional Committees (e.g. EU Agencies ICT Advisory Committee (ICTAC), Interinstitutional Committee for Digital Transformation (ICDT)<br>• European Competent Authorities for Secure Electronic Communications<br>• ECASEC<br>• EU Citizens<br>• Conformity Assessment Bodies; Trust Service Providers and Telecommunication Providers |

| | |
|---|---|
| | • Operators of Essential Services, including their associations and networks |

| RESOURCES PLANNED | | | | |
|---|---|---|---|---|
| **Human Resources (FTE)** | | | **Financial Resources** | EUR |
| **Total** | | | **Total** | |

## 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 including cross-border, and assist in reviewing and developing national and Union level cybersecurity strategies,.

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

### OBJECTIVES

- Increase the level of preparedness, capabilities and cooperation within and between Member States and sectors and EU institutions, bodies and agencies
- Prepare and test capabilities to respond to cybersecurity incidents
- Foster interoperable, consistent European risk management, methodologies 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<br>• Increased cooperation between communities | • Cutting-edge competences and capabilities in cybersecurity across the Union<br>• Empowered and engaged communities across the cybersecurity ecosystem |

| OUTPUTS | KPI |
|---|---|
| 3.1 Assist MS to develop, implement and assess National Cybersecurity Strategies<br>3.2 Organise large scale biennial exercises and sectorial exercises (including Cyber Europe, Blueprint operational level exercise (BlueOLEx), Cyber Exercise to test SOPs (CyberSOPEx etc) and through cyber ranges<br>3.3 Organise trainings and other activities to support and develop maturity and skills of CSIRTs (including NIS sectorial CSIRT) and other communities<br>3.4 Develop coordinated and interoperable risk management frameworks<br>3.5 Support the capacity building activities of the NIS Cooperation Group (NIS CG) and Work Streams as per NIS CG work programme<br>3.6 Support the creation and evolution European Information Sharing communities through Information Sharing and Analysis Centers (ISACs)[19] also through providing the EU ISAC platform[20] based on the Connecting Europe Facility (CEF) Core Service Platform as well as other collaboration mechanisms such as PPPs.<br>3.7 Support the reinforcement of Security Operational Centres (SOCs) as well as their collaboration, assisting the Commission and Member States initiatives in this area in line with the objectives of the EU Cybersecurity Strategy in the building and improving of SOCs[21].<br>3.8 Organise and support cybersecurity challenges including the European Cyber Security Challenge (ECSC)<br>3.9 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<br>**Metric:**<br>3.1Increase/decrease of maturity indicators<br>3.2 Outreach, uptake and application of lessons learned from capability-building activities.<br>3.3 Number of cybersecurity programmes (courses) and participation rates<br>3.4 The number of exercises executed annually<br>3.5 Stakeholder assessment on usefulness, added value and relevance of ENISA; and cooperation amongst communities in capacity building activities. (Survey)<br>**Frequency:** Annual 1, 2, 3 & 4, biennial 5 |

| VALIDATION | TARGET GROUPS AND BENEFICIARIES |
|---|---|

[19] Further consideration required in the course of 2022 whether the evolution of ISACs should be carried out within activity 4

[20] This is especially relevant for the year 2023 and onwards because the support contract procured by the Commission finishes by the end of 2022

[21] Further consideration required in the course of 2022 whether the evolution of SOCs should be carried out within activity 4
Tasks include:
(a) Continue developing and updating the mapping of the current landscape of SOCs in the EU, incl. both public and private, in-house or as a service; main operators of SOCs services in the EU;
(b) Provide other relevant support to the Commission in implementing the SOCs- related objectives of the EU Cybersecurity Strategy (, e.g. support to the design of calls for expression of interest, procurements, etc. liaison with stakeholders and research activities.)

| | |
|---|---|
| • NLO Network (as necessary)<br>• CSIRTs Network, (output 3.3.)<br>• CyCLONe members (as necessary)<br>• NIS Cooperation Group (output 3.5 and 3.6)<br>• EU ISACs (output 3.6)<br>• Ad-hoc WG on SOCs (output 3.7) | • Cybersecurity professionals<br>• EU Institutions and bodies<br>• Private industry sectors (operators of essential services such as health, transport etc.)<br>• CSIRTs Network and related operational communities<br>• European ISACs<br>• CyCLONe members |

| RESOURCES PLANNED | | | | |
|---|---|---|---|---|
| **Human Resources (FTE)** | | | **Financial Resources** | EUR |
| **Total** | | | **Total** | |

# Activity 4 Enabling operational cooperation

## OVERVIEW OF ACTIVITY

The activity supports operational cooperation among Member States, Union institutions, bodies, offices and agencies and betwe en operational activities inparticular through its established local office in Brussels, Belgium. Actions include establishing synergies with and between 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, as well as within the CyCLONe.

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 and uptake of the MeliCERTes platform[22].

In view of the EC Recommendation 4520 (2021) and Council Conclusions of the 20 October 2021 (ST 13048 2021) on 'exploring the potential of the Joint Cyber Unit initiative - complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises', ENISA will engage in exploring the potential of the JCU, along the lines and the roles defined according to on-going discussions amongst MS and relevant EU institutions, bodies and agencies. 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
- Ensure coordination in cybersecurity crisis management among relevant EU institutions, bodies and agencies (e.g. CERT -EU, European External Action Service (EEAS), European Union Agency for Law Enforcement Cooperation (EUROPOL)
- Improve maturity and capacities of operational communities (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

| RESULTS | Link to strategic objectives (ENISA STRATEGY) |
|---|---|
| • All communities (EU Institutions and MS) use a streamlined and coherent set of SOPs for cyber crises management<br>• Efficient 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<br>• 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, potential JCU, SOCs Network[23] and Cyber Crisis Management in the EU including cooperation with relevant Blueprint stakeholders (e.g Europol, CERT EU, EEAS and EDA)<br>4.2. Develop and enhance standard operating policies, procedures, methodologies and tools for cyber crisis management (also related to a future potential JCU).<br>4.3. Deploy , maintain and promote operational cooperation platforms and tools (MeliCERTes, CyCLONe, MOU, etc) including preparations for a secure virtual platform for a future potential JCU | **Indicator:** Effective use of ENISA's tools, platforms and take up of SOPs in operational cooperation<br>**Metric:**<br>4.1 of users both new and recurring and usage per platform/ tool/ SOPs provided by ENISA<br>4.2 Uptake of the platform/ tool/ SOPs during massive cyber incidents<br>4.3 Stakeholder satisfaction on the relevance and added value of the platforms/ tools/ SOPs provided by ENISA. (Survey)<br>**Frequency:** Annual 1 & 2, biennial 3 |

| VALIDATION | TARGET GROUPS AND BENEFICIARIES |
|---|---|
| • NLO Network (as necessary)<br>• CSIRTs Network and CyCLONe (output 4.1.)<br>• Blueprint actors | • Blueprint stakeholders<br>• EU decision makers, institutions, agencies and bodies<br>• MS CSIRTs Network Members<br>• NISD Cooperation Group<br>• OESs and DSPs |

## RESOURCES PLANNED

[22] This is especially relevant for the year 2023 and onwards because the support contract procured by the Commission finishes by the end of 2022.
[23] Provide support for the design and development of cross-border platforms for pooling of CTI data at EU level (incl. definition of a blueprint architecture, data infrastructure requirements, data processing and analytics tools, data sharing protocols) CTI exchange initiatives already working; legal aspects; interoperability, etc.

| Human Resources (FTE) | | | Financial Resources | EUR |
|---|---|---|---|---|
| Total | | | Total | |

# 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 (including analysis and exchange of technical information), public communication related to such incidents or crises 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.

This activity supports operational cooperation, including mutual assistance and the situational awareness in the framework of the proposed potential JCU.

Moreover the activity seeks to engage with CERT-EU in structured cooperation (Annex XIII Annual Cooperation Plan). The legal basis for this activity is Article 7 of the CSA

## OBJECTIVES

- Effective incident response and cooperation amongst Member States and EU institutions, including cooperation of technical, operational and political actors during incidents or crisis
- Common situational 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<br>• Stakeholders and public aware of current cybersecurity development | • Effective operational cooperation within the Union in case of massive (large-scale, cross-border) cyber incidents<br>• Empowered and engaged communities across the cybersecurity ecosystem |

| OUTPUTS | KPI |
|---|---|
| 5.1. Generate and consolidate information (including to the general public) on common cyber situational awareness, technical situational reports, incident reports, threats and support consolidation and exchange of information on strategic, operational and technical levels[24]<br>5.2. Support technical (including through MeliCERTes) and operational cooperation, incident response coordination and EU wide crisis communication during large-scale cross border incidents or crises<br>5.3. Maintain, develop and promote the trusted network of vendors/suppliers for information exchange and situational awareness | **Indicator:** ENISA ability and preparedness to support response to massive cyber incidents<br>**Metric:**<br>5.1 Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents ENISA contributes to mitigate (Survey)<br>5.2 Stakeholders' satisfaction of ENISA's preparedness and ability to provide operational support (Survey)<br>5.3 Number of relevant incident responses ENISA contributed to as per CSA Art.7<br>**Frequency:** Annual 3, biennial 1 & 2 |

| VALIDATION | TARGET GROUPS AND BENEFICIARIES |
|---|---|
| • Blueprint actors | • EU Member States (incl CSIRTs Network members and CyCLONe)<br>• EU Institutions, bodies and agencies<br>• Other type of CSIRTs and PSIRTs<br>• Blueprint actors |

## RESOURCES PLANNED

| Human Resources (FTE) | | | Financial Resources | EUR |
|---|---|---|---|---|
| Total | | | Total | |

[24] Advisory group proposal for standby emergency incident analysis team provisioned within output 5.1

# Activity 6 Development and maintenance of EU cybersecurity certification framework

## OVERVIEW OF ACTIVITY

This activity emcompasses actions to establish a European cybersecurity certification framework by preparing and reviewing candidate European cybersecurity certification schemes in accordance with Article 49 of the CSA, at the request of the Commission on the basis of the Union Rolling Work Program. Actions also include evaluating adopted certification schemes and participating in peer reviews. In addition the activity assists the Commission in providing secretariat of the European Cybersecurity Certification Group (ECCG), providing secretariat of the Stakeholder Cybersecurity Certification Group (SCCG); ENISA also makes available and maintains a dedicated European cybersecurity certification website according to Article 50 of the CSA.

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) |
|---|---|
| • Certified ICT products, services and processes are preferred by consumers and businesses | • High level of trust in secure digital solutions<br>• Empowered and engaged communities across the cybersecurity ecosystem |

| OUTPUTS | KPI |
|---|---|
| 6.1. Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes<br>6.2. Implementing and maintaining of the established schemes including evaluation of adopted schemes, participation in peer reviews etc.<br>6.3. Supporting the statutory bodies in carrying out their duties with respect to governance roles and tasks<br>6.4. Developing and maintaining the necessary tools to make effective use of the Union's cybersecurity certification framework (incl. certification website, the core service platform of CEF (Connecting Europe Facility) for collaboration, and publication, promotion of the implementation of the cybersecurity certification framework etc.) | **Indicator:**<br>1. Uptake of the European cybersecurity certification framework and schemes as an enabler for secure digital solutions.<br>2. Effective preparation of candidate certification schemes prepared by ENISA<br>**Metric:**<br>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<br>6.2 Stakeholders trust in digital solutions of certification schemes (citizens, public sector and businesses. (Survey)<br>6.3 Uptake of certified digital solutions (products, services and processes) using certification schemes under the CSA framework<br>6.4. Number of candidate certification schemes prepared by ENISA<br>6.5 Number of people/organizations engaged in the preparation of certification schemes<br>6.6 Satisfaction with ENISA's support in the preparation of candidate schemes (survey)<br>**Frequency:** Annual 1,4,5, biennial 2, 3 & 6 |

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

# Activity 7 Supporting European cybersecurity market and industry

## OVERVIEW OF ACTIVITY

This activity seeks to foster the cybersecurity market for products and services in the European Union along with the development of the cybersecurity industry and services, in particular SMEs and start-ups, to reduce dependence from outside and increase the capacity of the Union and to reinforce supply chains to the benefit of internal market. 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 producing analyses and guidelines as well as good practices on cybersecurity requirements, facilitating the establishment and take up of European and international standards across applicable areas such as 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) |
|---|---|
| • Contributing towards understanding cybersecurity market dynamics.<br>• A more competitive European cybersecurity industry, SMEs and start-ups | • High level of trust in secure digital solutions<br>• 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, and evaluation of certified products, services and processes<br>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<br>7.3. Guidelines and good practices on cybersecurity certification requirements for ICT products, services and processes<br>7.4. Monitoring and documenting the dependencies and vulnerabilities of ICT products and services<br>7.5 Policy recommendations to the EC and the ECCC, including particularly critical technological capacities and market segments. | **Indicator:** Effectiveness of ENISA's supporting role for participants in the European cybersecurity market<br>**Metric:**<br>7.1 Number of market analysis, guidelines and good practices issued by ENISA<br>7.2 Uptake of lessons learnt / recommendations from ENISA reports<br>7.3 Stakeholder satisfaction with the added value and quality of ENISA's work (Survey)<br>**Frequency:** Annual 1 & 2, biennial 3 |

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

## RESOURCES PLANNED

| Human Resources (FTE) | | | Financial Resources | EUR |
|---|---|---|---|---|
| Total | | | Total | |

# 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 and future technologies such as the ones in the area of artificial intelligence, quantum, distributed ledgers, cloud computing, cryptography, edge computing, software development, and others with special relevance to future research and innovation in the field of cybersecurity. On the basis of risk management principles, and consolidation of information and knowledge; and taking into account work on incident reporting. 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. Furthermore, the Agency will continue analysing and reporting on incidents as required by Art 5(6) of CSA.

The activity also seeks to identify and give advice on research and innovation (including facilitating deployment) needs and priorities in the field of cybersecurity, and contribute to the EU strategic research agenda setting for public sector investment in cybersecurity .. The Agency will provide strategic advice to the Governing Board and act as permenant observer to the Governing Board, play an active part in the activities of the Competence Centre, cooperate and ensure synergies with the Centre, provide relevant input during the preparation of the ECCC Agenda, Work Programmes and Multiannual Work Programme (Articles 5, 8, 10, 12, 18 of the ECCC Regualtion EC 2021/887).

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 & 11 and Article 5(6) of the CSA.

## OBJECTIVES

- Identify and understand emerging and 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<br>• Stakeholders receive relevant and timely information for policy and decision-making<br>• Research and innovation areas tied to the cybersecurity needs and requirements | • Foresight on emerging and future cybersecurity challenges<br>• Efficient and effective cybersecurity information and knowledge management for Europe<br>• Empowered and engaged communities across the cybersecurity ecosystem |

| OUTPUTS | KPI |
|---|---|
| 8.1 Develop and maintain EU cybersecurity index<br>8.2 Collect and analyse information to report on the cyber threat landscapes<br>8.3 Analyse and report on incidents as required by Art 5(6) of CSA<br>8.4 Develop and maintain a portal (information hub), respectively identify appropriate tools for 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<br>8.5 Foresight on emerging and future cybersecurity challenges and recommendations.<br>8.6 Contribute to the Union's strategic research and innovation agenda and programmes in the field of cybersecurity (annual report).<br>8.7 Advise on potential research and innovation investment needs and priorities (e.g. capacity building and market & industry) and emergent cyber technologies) in the field of cybersecurity in particular supporting the activities of the Competence Centre and the Network.<br>8.8 Building and exchanging knowledge on ransomware threat (incl. capacity building and awareness raising and education) | **Indicator:** ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge including into research and innovation agenda<br>**Metric:**<br>8.1 Number of users and frequency of usage of dedicated portal (observatory)<br>8.2 Number of recommendations, analysis, challenges identified and analysed<br>8.3 Number of requests from Member States and EU research and innovation entities to contribute, provide advice or participate in activities.<br>8.4 Stakeholder satisfaction on the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges & opportunities including in research (Survey)<br>**Frequency:** Annual 1,2 & 3, biennial 4 |

| VALIDATION | TARGET GROUPS AND BENEFICIARIES |
|---|---|
| • NLO Network<br>• ENISA Advisory Group (as necessary)<br>• ENISA ad hoc working groups (as necessary)<br>• CSIRT Network (output 8.2)<br>• Formally established bodies and expert groups as necessary (output 8.3) | • General public<br>• Industry, research and academic institutions and bodies |

| | |
|---|---|
| • The European Cybersecurity Competence Centre and Network of National Coordination Centres and Competence Centre Governing Board (output 8.6 & 8.7) | • ECASEC and Art. 19 Expert Group members<br>• EU and national decision making bodies and authorities<br>• European Cybersecurity Competence Centre & Network |

| **RESOURCES PLANNED** | | | | |
|---|---|---|---|---|
| **Human Resources (FTE)** | | | **Financial Resources** | EUR |
| **Total** | | | **Total** | |

# 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

- Advance cyber-secure behaviour by essential service providers in critical sectors
- 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<br>• Stronger European cybersecurity through higher global resilience | • Empowered and engaged communities across the cybersecurity ecosystem |

| OUTPUTS | KPI |
|---|---|
| 9.1 Develop activities to enhance behavioural change by essential service providers in critical sectors (as defined by the NISD)<br>9.2 Promote cybersecurity topics, education and good practices in the basis of the ENISA stakeholders' strategy<br>9.3 Implement ENISA international strategy and outreach<br>9.4 Organise European cybersecurity month (ECSM) and related activities<br>9.5 Policy recommendations to the EC and the ECCC, including particularly critical technological capacities and market segments | **Indicator:**<br>Level of awareness on cybersecurity, cyber hygiene and cyber literacy across the EU<br>Level of outreach<br>**Metric:**<br>9.1 Number of cybersecurity incidents reported having human error as a root cause<br>9.2 Number of activities and participation in awareness raising actions organised by ENISA on cybersecurity topics<br>9.3 Geographical and community coverage of outreach in the EU<br>9.4 Level of awareness on cybersecurity across the EU/ general public (e.g. EU barometer and other)<br>**Frequency:** Annual 1,2 & 3, biennial 4 |

| VALIDATION | TARGET GROUPS AND BENEFICIARIES |
|---|---|
| • Management Board (output 9.1. and 9.3.) SCCG (for certification related issues under output 9.2)<br>• NLO Network<br>• ENISA Advisory Group (outputs 9.1. and 9.2) | • Public, businesses and organisations<br>• Member States, EU institutions, bodies and agencies<br>• International partners |

## RESOURCES PLANNED

| Human Resources (FTEs) | | | Financial Resources | EUR |
|---|---|---|---|---|
| Total | | | Total | |

## 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 continue 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 (Standard Operating Proceduress).

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
- Compliant with legal and financial frameworks in the performance of the Agency (build a culture of compliance)
- Protect the Agency's 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<br>Building lasting credibility and trust | Sound resource and risk management |

| OUTPUTS | KPI |
|---|---|
| 10.1. Maintain performance management framework<br>10.2. Develop and implement annual communications strategy<br>10.3. Develop and implement risk management plans including IT systems cybersecurity risk assessment, including focus on quality management framework and business processes as well as relevant policies<br>10.4. Maintain and monitor the implementation of Agency wide IT management processes and develop budgetary management processes<br>10.5. Maintenance of single administrative practices across the Agency<br>10.6. Implement targeted action plan of overarching audit on the CO2 impact of all operations of the Agency | **Indicator**: Organisational performance culture<br>**Indicator:** Trust in ENISA brand<br>**Metrics:**<br>1 Proportion of KPI's reaching targets<br>2 Individual staff contribution to achieving the objectives of the agency via clear link to KPI's in staff career development report (CDR report)<br>3. Exceptions in Risk Register<br>4. Number of complaints filed against ENISA incl number of inquiries/ complaints of the EU Ombudsman<br>5. Number of complaints addressed timely and according to relevant procedures<br>6. Results of annual risk assessment exercise<br>7. Observations from external audit bodies (e.g. European Court of Auditors ECoA) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings and number of observations successfully completed and closed<br>8. Level of trust in ENISA (survey)<br>**Frequency:** 1 to 7 annual, biennial 8 |

| VALIDATION | TARGET GROUPS AND BENEFICIARIES |
|---|---|
| • Management Team<br>• Budget Management Committee<br>• IT Management Committee<br>• Intellectual Property Rights Management Committee<br>• Staff Committee<br>• ENISA Ethics Committee | • Citizens<br>• 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*".

The actions which will be pursued under this activity will focus on making sure that the Agency's HR resources fit the needs and objectives of ENISA, 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 belonging. 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

- Consistent and regular review of the Agency's resources, to seek appropriate match with the organisation's needs, along with obtaining internal and external efficiency gains across the organisation
- Engaged staff, committed and motivated to deliver, empowered to use fully their talent, skills and competences
- Digitally enabled work-place and environment (including home work-space) which promotes performance and balances social and environmental responsibility

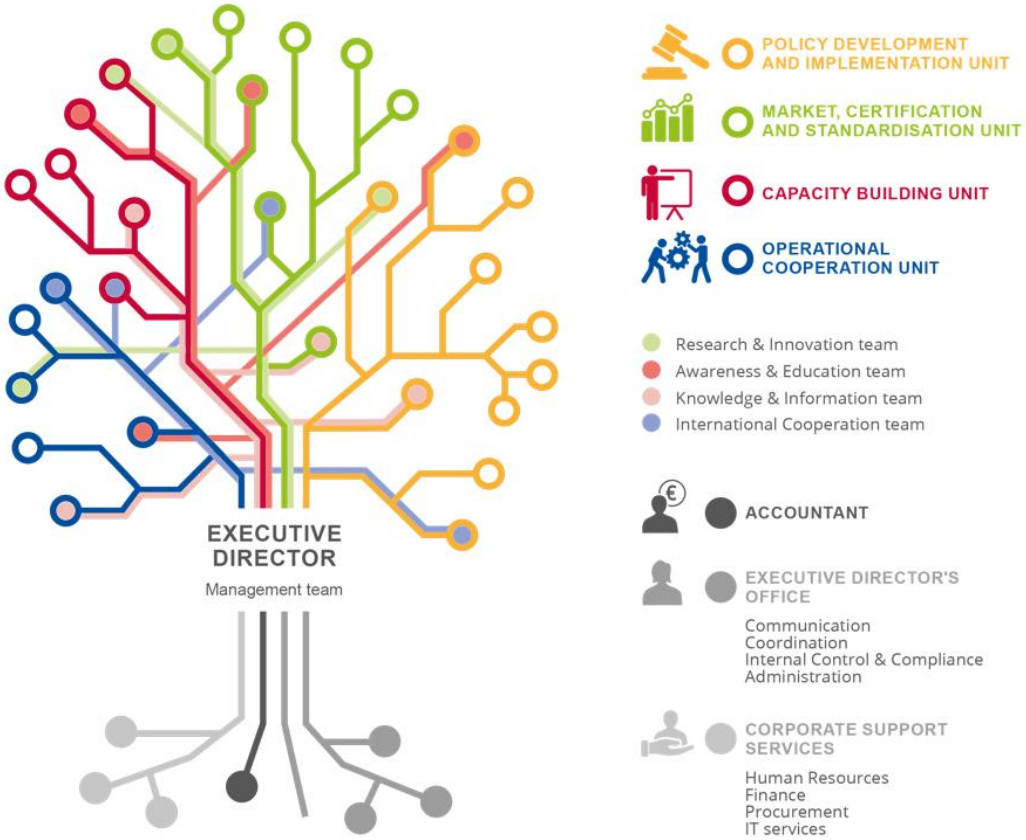
| RESULTS | Link to corporate objective: |
|---|---|
| ENISA as an employer of choice | Build an agile organisation focused on people |

| OUTPUTS | KPI |
|---|---|
| 11. Maintain and implement the competence framework into all HR processes (including into training strategy, CDR, internal competitions, exit-interviews etc)<br>11.2 Develop HR Strategy with emphasis on talent development, growth and innovation<br>11.3 Undertake actions to develop and nourish talent and conduct necessary management development activities<br>11.4 Develop and maintain a user friendly and service oriented teleworking and office environment (including digital tools and services)<br>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<br>**Metric**:<br>11.1 Staff satisfaction survey (incl attractiveness of ENISA as employer, staff empowerment, organisational culture, opportunities on internal mobility, work-space, -environment and -tools)<br>11.2 Quantity and quality of ENISA training and career development activities organised for staff<br>11.3 Reasons for staff departure (exit interviews)<br>11.4 Staff retention/turnover rate<br>11.5 Resilience and quality of ENISA IT systems and services (including ability to consistently increase satisfaction with IT services & tools)<br>**Frequency**: Annual (ad hoc for metric no 11.3) |

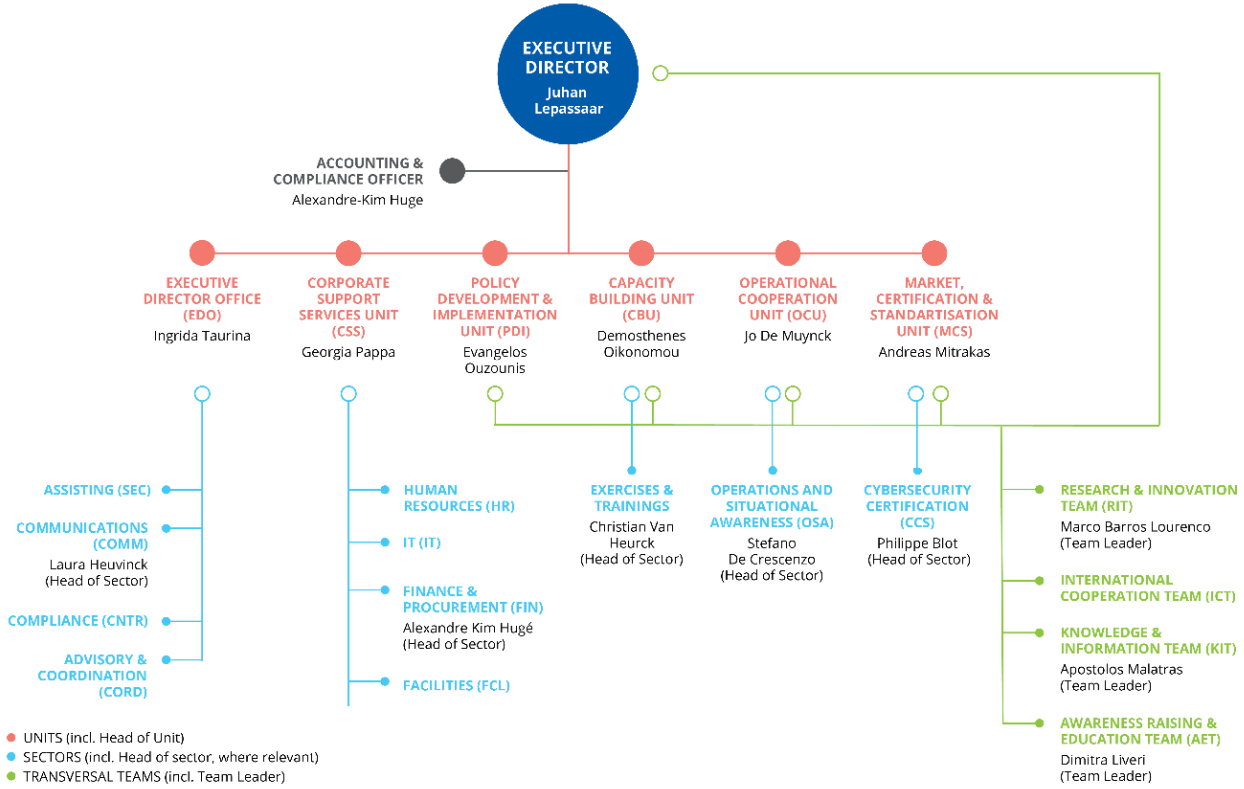
| VALIDATION | TARGET GROUPS AND BENEFICIARIES |
|---|---|
| • Management Team<br>• Joint Reclassification Committee<br>• IT Management Committee<br>• Task Force on relocation of the Agency<br>• Staff Committee | • ENISA staff members and employees |

# ANNEX A

## I. ORGANISATION CHART AS OF 01.01.2022



## Administrative Organigramme




**Status in-house staff (AD;AST;CA;SNEs) on 01.12.2021**

| ED* | |
|---|---|
| AD | 2 |
| **Total** | **2** |

* ED and accountant

| EDO | |
|---|---|
| AD | 8 |
| AST | 8 |
| CA | 2 |
| SNE | 1 |
| **Total** | **19** |

| CSS | |
|---|---|
| AD | 2 |
| AST | 7 |
| CA | 10 |
| SNE | 0 |
| **Total** | **19** |

| PDI | |
|---|---|
| AD | 10 |
| AST | 0 |
| CA | 5 |
| SNE | 2 |
| **Total** | **17** |

| CBU | |
|---|---|
| AD | 7 |
| AST | 2 |
| CA | 5 |
| SNE | 2 |
| **Total** | **16** |

| OCU | |
|---|---|
| AD | 9 |
| AST | 0 |
| CA | 2,5 |
| SNE | 3 |
| **Total** | **14,5** |

| MCS | |
|---|---|
| AD | 14 |
| AST | 0 |
| CA | 2,5 |
| SNE | 2 |
| **Total** | **18,5** |

| SUMMARY | |
|---|---|
| **AD** | **52** |
| **AST** | **17** |
| **CA** | **27** |
| **SNE** | **9** |
| **Total** | **106** |

## II. RESOURCE ALLOCATION PER ACTIVITY 2023 - 2025

To be updated at a later stage

The indicative allocation of the total 2023 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 will be presented in the table[25] below. The allocation will be 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 2023-2025 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 2023.
- The allocation of 5 additional FTEs from the proposed NIS Directive will be allocated in due course according to the final agreement of regulators and once the tasks have been finalised.

[25] To be updated at a later stage

| ALLOCATION OF HUMAN AND FINANCIAL RESOURCES (2023) | Activities as referred to in Section 3 | Direct and Indirect budget allocation (in EUR) | FTE allocation |
|---|---|---|---|
| Providing assistance on policy development | | | |
| Supporting implementation of Union policy and law | | | |
| Building capacity | | | |
| Enabling operational cooperation | | | |
| Contribute to cooperative response at Union and Member States level | | | |
| Development and maintenance of EU cybersecurity certification framework | | | |
| Supporting European cybersecurity market and industry | | | |
| Knowledge on emerging cybersecurity challenges and opportunities | | | |
| Outreach and education | | | |
| Performance and risk management | | | |
| Staff development and working environment | | | |
| **TOTAL** | | | |

# III. FINANCIAL RESOURCES 2023 - 2025

**Table 1:** Revenue

| REVENUES | 2021 Executed Budget | 2022 Adopted budget | VAR 2023 / 2022 | Draft Estimated budget 2023 | Envisaged 2024 | Envisaged 2025 |
|---|---|---|---|---|---|---|
| 1 REVENUE FROM FEES AND CHARGES | | | | | | |
| 2 EU CONTRIBUTION | 22.248.000 | 23.633.000 | 2% | 24.110.000 | 24.610.000 | 25.010.000 |
| *- of which assigned revenues deriving from previous years' surpluses* ** | *-579.113,00* | | | | | |
| *- of which Reserve conditional to approval of NIS2 Directive* | | 610.000 | | 610.000 | 610.000 | 610.000 |
| 3 THIRD COUNTRIES CONTRIBUTION (incl. EEA/EFTA and candidate countries) | 585.060 | 574.625 | 4% | 597.182 | 609.888 | 619.474 |
| *- of which EEA/EFTA (excl. Switzerland)* | 585.060 | 574.625 | 4% | 597.182 | 609.888 | 619.474 |
| *- of which Candidate Countries* | | | | | | |
| 4 OTHER CONTRIBUTIONS | 317.071 | * | 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** | **23.150.131** | **24.207.625** | **2%** | **24.707.182** | **25.219.888** | **25.629.474** |

* - 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

**Table 2:** Expenditure

| EXPENDITURE | 2022 | | 2023 | |
|---|---|---|---|---|
| | Commitment appropriations | Commitment appropriations | Commitment appropriations | Payment appropriations |
| **Title 1** | 12.494.335 | 12.494.335 | 12.988.814 | 12.988.814 |
| **Title 2** | 2.824.300 | 2.824.300 | 2.895.940 | 2.895.940 |
| **Title 3** | 8.888.990 | 8.888.990 | 8.822.428 | 8.822.428 |
| **Total expenditure** | **24.207.625** | **24.207.625** | **24.707.182** | **24.707.182** |

| EXPENDITURE (in EUR) | Commitment and Payment appropriations | | | | | |
|---|---|---|---|---|---|---|
| | Executed budget 2021 | Adopted Budget 2022 Agency request | Draft estimated budget 2023 | VAR 2023 / 2022 | Envisaged in 2024 | Envisaged in 2025 |
| **Title 1. Staff Expenditure** | **10.799.493** | **12.494.335** | **12.988.814** | **4%** | **13.258.348** | **13.473.672** |
| 11 Staff in active employment * | 8.370.300 | 10.837.880 | 11.358.518 | 5% | 11.594.222 | 11.782.519 |
| 12 Recruitment expenditure | 306.022 | 412.000 | 422.796 | 3% | 431.569 | 438.578 |
| 13 Socio-medical services and training | 1.371.493 | 853.000 | 932.500 | 9% | 951.851 | 967.309 |
| 14 Temporary assistance | 751.678 | 391.455 | 275.000 | -30% | 280.707 | 285.265 |
| **Title 2. Building, equipment and miscellaneous expenditure** | **3.855.317** | **2.824.300** | **2.895.940** | **3%** | **2.956.035** | **3.004.042** |
| 20 Building and associated costs | 1.312.041 | 914.550 | 1.018.350 | 11% | 1.039.482 | 1.056.364 |
| 21 Movable property and associated costs | 271.592 | 160.000 | 0 | -100% | 0 | 0 |
| 22 Current corporate expenditure | 686.263 | 320.000 | 549.840 | 72% | 561.250 | 570.365 |
| 23 Corporate ICT | 1.585.422 | 1.429.750 | 1.327.750 | -7% | 1.355.303 | 1.377.313 |
| **Title 3. Operational expenditure** | **8.383.370** | **8.888.990** | **8.822.428** | **-1%** | **9.005.505** | **9.151.760** |
| 30 Activities related to meetings and missions | 504.740 | 387.000 | 386.108 | 0% | 394.120 | 400.521 |
| 32 Horizontal operational activities | 0 | 0 | 0 | | 0 | 0 |
| 36/37 Core operational activities | 7.878.630 | 8.501.990 | 8.436.320 | -1% | 8.611.385 | 8.751.239 |
| **TOTAL EXPENDITURE** | **23.038.179** | **24.207.625** | **24.707.182** | **2%** | **25.219.888** | **25.629.474** |

* for years 2022-2024 chapter 11 includes an amount of EUR 610 thou as a reserve conditional to approval of NIS Directive (for salaries of ne

**Table 3:** Budget outturn and cancellation of appropriations

| Budget outturn | 2019 | 2020 | 2021 |
|---|---|---|---|
| **Revenue actually received (+)** | 16.740.086 | 21.801.460 | 23.058.211 |
| **Payments made (-)** | -11.980.352 | -15.050.421 | -17.989.374 |
| **Carry-over of appropriations (-)** | -4.357.734 | -6.200.614 | -5.082.548 |
| **Cancellation of appropriations carried over (+)** | 62.522 | 180.023 | 209.385 |
| **Adjustment for carry-over of assigned revenue appropriations carried over (+)** | 116.393 | 10.403 | 125.622 |
| **Exchange rate difference (+/-)** | -1.802 | -1.291 | -428 |
| **Total** | **579.113** | **739.560** | **320.868** |

## III.a Cancellation of appropriations

In 2021, out of an EU budget contribution to ENISA's budget of 22 833 kEUR (C1 funds), 22 721 kEUR were committed, representing a budget execution rate of 99,51%, and a total of 112 kEUR representing 0,49% of the budget was not used. A total of 17 672 kEUR representing 77.4% of the 2021 budget were paid in 2021 and a total of 5 049 kEUR representing 22.11% of the 2021 budget were carried forward into 2022.

## IV. HUMAN RESOURCES- QUANTITATIVE

Overview of all categories of staff and its evolution

Staff policy plan for 2023 - 2025

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

Statutory staff and SNE

| STAFF | 2021 | | | 2022 | 2023 | 2024 | 2025 |
|---|---|---|---|---|---|---|---|
| ESTABLISHMENT PLAN POSTS | Authorised Budget | Actually filled as of 31/12/2021 | Occupancy rate % | Adopted | Envisaged staff | Envisaged staff | Envisaged staff |
| Administrators (AD) | 57 | 52 | 91% | 63 | 63 | 63 | 63 |
| Assistants (AST) | 19 | 17 | 89% | 19 | 19 | 19 | 19 |
| Assistants/Secretaries (AST/SC) | | | | | | | |
| TOTAL ESTABLISHMENT PLAN POSTS | 76 | 69 | 91% | 82 | 82 | 82 | 82 |
| EXTERNAL STAFF | FTE corresponding to the authorised budget 2021 | Executed FTE as of 31/12/2021 | Execution Rate % | Adopted FTE | Envisaged FTE | Envisaged FTE | Envisaged FTE |
| Contract Agents (CA) | 30 | 27 | 90% | 32 | 32 | 32 | 32 |
| Seconded National Experts (SNE) | 12 | 10 | 83% | 12 | 14[26]** | 16** | 16 |
| TOTAL External Staff | **42** | **49** | **N/A** | **44** | **46** | **48** | **48** |
| TOTAL STAFF[27] | **118** | **106** | **90%** | **126** | **128** | **130** | **130** |

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

[26]** In its budget proposal for the Single Programming Document (SPD) 2023 – 2025, the Agency asks for an extra 4 SNE posts introduced gradually (2+2 over 2 years).

[27] Refers to TA, CA and SNEs figures.

| Human Resources | 2021 | 2022 | 2023 | 2024 | 2025 |
|---|---|---|---|---|---|
| | Envisaged FTE | Envisaged FTE | Envisaged FTE | Envisaged FTE | Envisaged FTE |
| **Contract Agents (CA)** | n/a | n/a | n/a | n/a | n/a |
| **Seconded National Experts (SNE)** | n/a | n/a | n/a | n/a | n/a |
| **TOTAL** | n/a | n/a | n/a | n/a | n/a |

Other Human Resources

- Structural service providers

| | Actually in place as of 31/12/2020 | Actually in place as of 31/12/2021 |
|---|---|---|
| Security | 5 | 5 |
| IT | 4 | 5 |

- Interim workers

| | Actually in place as of 31/12/2020 | Actually in place as of 31/12/2021 |
|---|---|---|
| Number | 31 | 11 |

**Table 2:** Multi-annual staff policy plan Year , 2021, 2022, 2023, 2024, 2025[28]

| Function group and grade | 2021 | | | | 2022 | | 2023 | | 2024 | | 2025 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Authorised budget | | Actually filled as of 31/12/2021[29] | | Authorised | | Envisaged | | Envisaged | | Envisaged |
| | Perm. Posts | Temp. posts | Perm. Posts | Temp posts | Perm. posts | Temp. posts | Perm. posts | Temp. posts | Perm. posts | Temp. posts | Temp. posts |
| AD 16 | | | | | | | | | | | |
| AD 15 | | 1 | | | | 1 | | 1 | | 1 | 1 |
| AD 14 | | | | 1 | | | | | | | |
| AD 13 | | 1 | | 1 | | 2 | | 2 | | 2 | 2 |
| AD 12 | | 5 | | 5 | | 4 | | 4 | | 4 | 4 |
| AD 11 | | 2 | | | | 2 | | 2 | | 2 | 3 |
| AD 10 | | 3 | | 3 | | 4 | | 3 | | 4 | 3 |
| AD 9 | | 12 | | 9 | | 11 | | 12 | | 15 | 16 |
| AD8 | | 21 | | 9 | | 22 | | 25 | | 23 | 24 |
| AD 7 | | 8 | | 12 | | 8 | | 10 | | 9 | 8 |
| AD 6 | | 4 | | 12 | | 9 | | 4 | | 3 | 2 |
| AD 5 | | | | | | | | | | | |

[28] 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. In 2022, ENISA will review its staffing strategy and will update a forecast for reclassification also in line with job mapping.
[29] The figures include actually filled posts as of 31.12.2021.

| Function group and grade | 2021 | | | | 2022 | | 2023 | | 2024 | | 2025 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Authorised budget | | Actually filled as of 31/12/2021[29] | | Authorised | | Envisaged | | Envisaged | | Envisaged |
| | Perm. Posts | Temp. posts | Perm. Posts | Temp posts | Perm. posts | Temp. posts | Perm. posts | Temp. posts | Perm. posts | Temp. posts | Temp. posts |
| AD TOTAL | | 57 | | 52 | | 63 | | 63 | | 63 | 63 |
| AST 11 | | | | | | | | | | | |
| AST 10 | | | | | | | | | | | |
| AST 9 | | | | | | | | | | | |
| AST 8 | | 1 | | 1 | | 2 | | 2 | | 2 | 2 |
| AST 7 | | 4 | | 3 | | 3 | | 4 | | 5 | 6 |
| AST 6 | | 8 | | 2 | | 8 | | 7 | | 6 | 5 |
| AST 5 | | 5 | | 4 | | 5 | | 5 | | 5 | 5 |
| AST 4 | | 1 | | 4 | | 1 | | 1 | | 1 | 1 |
| AST 3 | | | | 2 | | | | | | | |
| AST 2 | | | | 1 | | | | | | | |
| AST 1 | | | | | | | | | | | |
| AST TOTAL | | 19 | | 17 | | 19 | | 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 | | 76 | | 69 | | 82 | | 82 | | 82 | 82 |
| GRAND TOTAL | 76 | | 69 | | 82 | | 82 | | 82 | | 82 |

**External personnel**

*Contract Agents*

| Contract agents | FTE corresponding to the authorised budget 2021 | Executed FTE as of 31/12/2021 | FTE corresponding to the authorised budget 2022 | FTE corresponding to the authorised budget 2023 | FTE corresponding to the authorised budget 2024 | FTE corresponding to the authorised budget 2025 |
|---|---|---|---|---|---|---|
| Function Group IV | 28 | 19 | 30 | 30 | 30 | 30 |
| Function Group III | 2 | 7 | 2 | 2 | 2 | 2 |
| Function Group II | 0 | 0 | 0 | 0 | 0 | 0 |
| Function Group I | 0 | 1 | 0 | 0 | 0 | 0 |
| TOTAL | **30** | **27** | **32** | **32** | **32** | **32** |

*Seconded National Experts*

| Seconded National Experts | FTE corresponding to the authorised budget 2021 | Executed FTE as of 31/12/2021 | FTE corresponding to the authorised budget 2022 | FTE corresponding to the authorised budget 2023 | FTE corresponding to the authorised budget 2024 | FTE corresponding to the authorised budget 2025 |
|---|---|---|---|---|---|---|
| TOTAL | **12** | **10** | **12** | **14**[30]***** | **16*** | **16*** |

[30] In its budget proposal for the Single Programming Document (SPD) 2023 – 2025, the Agency asks for an extra 4 SNE posts introduced gradually 2+2 over 2 years).

**Table 3**: Recruitment forecasts 2023 following retirement / mobility or new requested posts (indicative table)

To be updated in due course

| JOB TITLE IN THE AGENCY | TYPE OF CONTRACT (OFFICIAL, TA OR CA) | | TA/OFFICIAL<br>**Function group/grade of recruitment internal (Brackets) and external (single grade) foreseen for publication *** | | CA<br>**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** | | n/a | n/a | n/a | n/a |
| **Officers** | | n/a | n/a | n/a | n/a |
| **Assistant** | | n/a | n/a | n/a | n/a |

# 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** | **Year 2021** | **Actual average over 5 years** | **Average over 5 years (According to decision C(2015)9563)** |
| **AD05** | - | - | - | - | - | - | - | 2.8 |
| **AD06** | 1 | 1 | 2 | 3 | - | 1 | 3,7 | 2.8 |
| **AD07** | 1 | - | - | - | 1 | - | - | 2.8 |
| **AD08** | 1 | 1 | 1 | - | 2 | 1 | 4,3 | 3 |
| **AD09** | - | - | 1 | - | - | - | - | 4 |
| **AD10** | - | - | - | - | - | - | - | 4 |
| **AD11** | 1 | - | - | - | - | - | - | 4 |
| **AD12** | - | - | - | - | - | - | - | 6.7 |
| **AD13** | - | - | - | - | - | 1 | 10 | 6.7 |
| **AST1** | - | - | - | - | - | - | - | 3 |
| **AST2** | - | - | - | - | - | - | - | 3 |
| **AST3** | 1 | 1 | 1 | - | - | - | - | 3 |
| **AST4** | 1 | 1 | 1 | - | 1 | - | - | 3 |
| **AST5** | 1 | - | 1 | - | - | 1 | 5,5 | 4 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **AST6** | 1 | - | - | - | 1 | 1 | 3,5 | 4 |
| **AST7** | - | - | - | - | - | 1 | 5 | 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 31.12.2021 | HOW MANY STAFF MEMBERS WERE RECLASSIFIED IN YEAR 2021 | 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 | 13 | 5 | 3 | Between 3 and 5 years |
| | 13 | 1 | - | - | Between 3 and 5 years |
| CA III | 11 | 1 | - | - | Between 6 and 10 years |
| | 10 | 5 | 1 | 3 | Between 5 and 7 years |
| | 9 | 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 31.12.2021 statutory staff (only temporary agents and contract agents on 31.12.2021 and accepted offers and resignations up until and including 16.12.2021)

| | | OFFICIAL | | TEMPORARY | | CONTRACT AGENTS | | GRAND TOTAL | |
|---|---|---|---|---|---|---|---|---|---|
| | | Staff | % | Staff | % | Staff | % | Staff | % |
| Female | Administrator level | - | - | 18 | - | 15 | - | - | - |
| | Assistant level (AST & AST/SC) | - | - | 11 | - | - | - | - | - |
| | Total | - | - | 29 | 66 | 15 | 34 | 44 | 45,8 |
| Male | Administrator level | - | - | 34 | - | 12 | - | - | - |
| | Assistant level (AST & AST/SC) | - | - | 6 | - | - | - | - | - |
| | Total | - | - | 40 | 77 | 12 | 23 | 52 | 54,2 |
| Grand Total | | - | - | 69 | 71,9 | 27 | 28,1 | 96 | 100% |

**Table 1:** Data on 31/12/2020 statutory staff (only, temporary agents and contract agents)

| | | 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 (31.12.2021)

| | 2016 | | 31.12.2021 | |
|---|---|---|---|---|
| | Number | % | Number | % |
| Female Managers | 0 | 0 | 3 | 33,3 |
| Male Managers | 10 | 100 | 6[31] | 66,7 |

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 31.12.2021 - statutory staff only

| 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 | 5 | 7 | 2 | 8 | 7 | 7,3 |
| BG | 2 | 2,8 | - | - | 2 | 2,1 |
| CY | 1 | 1,4 | 2 | 8 | 3 | 3,1 |
| CZ | 1 | 1,4 | - | - | 1 | 1 |
| DE | 2 | 2,8 | - | - | 2 | 2,1 |
| Double *32 | 4 | 5,6 | 3 | 12 | 7 | 7,3 |

[31] This category comprises Heads of Unit and Team Leaders
[32] Double nationalities comprise staff members who also have non-EU nationalities (i.e. Italian/Australian, Belgian/British, Cypriot/Greek, German/Greek, Dutch/Greek etc.).

| | | | | | | |
|---|---|---|---|---|---|---|
| EE | 1 | 1,4 | - | - | 1 | 1 |
| ES | 3 | 4,2 | 1 | 4 | 4 | 4,2 |
| FR | 3 | 4,2 | 1 | 4 | 4 | 4,2 |
| GR | 26 | 36,6 | 12 | 48 | 38 | 39,6 |
| IT | 5 | 7 | - | - | 5 | 5,2 |
| LT | - | - | 1 | 4 | 1 | 1 |
| LV | 2 | 2,8 | - | - | 2 | 2,1 |
| NL | 2 | 2,8 | - | - | 2 | 2,1 |
| PL | 3 | 4,2 | 1 | 4 | 4 | 4,2 |
| PT | 3 | 4,2 | 1 | 4 | 4 | 4,2 |
| RO | 7 | 9,9 | 0 | 0 | 7 | 7,3 |
| SE | 1 | 1,4 | - | - | 1 | 1 |
| SK | - | - | 1 | 4 | 1 | 1 |
| TOTAL | 71 | 74 | 25 | 26 | 96 | 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 | 2016 | | 31.12. 2021 | |
|---|---|---|---|---|
| | Number | % | Number | % |
| Greek | 27 (out of 68) | 39,7 | 38 (out of 96) | 39,6 |

Looking back to 2021, it has been noted that the positive mesures to improve the diversity of nationalities which had taken place in 2020 and 2021, have borne fruit. This can be attributed to the 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[33].

### .E. Local office in Brussels, Belgium

In 2020 ENISA put forward a proposal to open a local office in accordance with CSA Art 20 (5). 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.

During 2021 initial negotiations were carried out with the OIB concerning an office in the One Building in Brussels. In parrellel work was carried out with DGHR.DS to specify conditions for a secure area, which is required in order for Brussels staff to work on EUCI projects. To date, building specifications are complete and are waiting for formal approval by HR.DS3 to launch implementation of secure area. Work has also started on defining / adapting the necessary service level agreements and is expected to complete by Q1 2022.

Indicative resources foreseen:

| | 2022 | 2023 | 2024 | 2025 |
|---|---|---|---|---|
| **Head count (FTEs)** | **4 -7** | **4-10** | **4-10** | **4 - 10** |
| **Budget (one-off & maintenance costs)** | **500.000** | **170.000** | **170.000** | **170.000** |

### 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 2021-2022, the process for the financial support for the staff of ENISA in relation to the cost of schooling has been updated via EDD 2021-41, leading to the abolishment of SLAs** |

## VI. ENVIRONMENT MANAGEMENT

[33] 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.

This will depend on the new headquarters building however ENISA is looking into opportunities to strengthen its environmental management as such a new output has been introduced in 2022 to carry out an overarching audit on the CO2 impact of all operations of the Agency and develop and implement a targeted action plan The objective of this undertaking is for the Agency to be climate neutrality by 2030.

## VII. BUILDING POLICY

In 2021 ENISA relocated to a new headquarters building in Athens, Greece. The building policy will be developed in the course of 2022.

## 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.<br>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.<br>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.<br>There is no European School operating in Athens. |

## IX. EVALUATIONS

To be updated at a later stage

Ex-ante and ex-poste evaluations were issued in 2021 and need for evaluation to be reconsidered during 2022

## X. STRATEGY FOR THE ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS

To be updated at a later stage

As adopted by the Management Board[34], 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.

[34] https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/MB%20Decision%202019-12%20on%20internal%20controls%20framework.pdf

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 2021 ENISA adopted an anti-fraud strategy[35] as recommended by the European Anti-Fraud Office (OLAF) .

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

To be updated at a later stage

ENISA does not receive any form of grant.

Table[36] below provides a summary of the SLA and agreements of the agency including contracted amount where necessary:

| Title | Type | Contractor | Contracted amount |
|---|---|---|---|
| **10th Amendment of SLA with CERT-EU-001-00** | SLA | EUROPEAN COMMISSION | €24.480,00 |
| **Global SLA with DIGIT** | SLA | EUROPEAN COMMISSION | |
| **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 and SDA with DG BUDG Implementation and usage of ABAC System** | SLA | EUROPEAN COMMISSION | €46.000,00 |

[35] https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/mb-decision-2021-5-on-anti-fraud-strategy
[36] To be updated in the course of 2022

| | | | |
|---|---|---|---|
| **SLA for Shared Support Office (SSO)_EUAN** | SLA | EUROPEAN FOOD SAFETY AUTHORITY EFSA | €2.828,17 |
| **SLA with CEDEFOP** | SLA | CEDEFOP | |
| **SLA with DG HR** | SLA | EUROPEAN COMMISSION | |
| **SLA with EASA - Permanent Secretariat** | SLA | EASA | |
| **SLA with EPSO and EUSA (updated)** | SLA | EUROPEAN PERSONNEL SELECTION OFFICE (EPSO) | |
| **SLA with European Administrative School** | SLA | EAS | |
| **SLA with Office for Official Publications of the European Communities** | SLA | OPOCE Publications Office | |
| **SLA with PMO** | SLA | PMO | |
| **Agreement on Strategic Co-operation with EUROPOL** | Agreement | EUROPEAN POLICE OFFICE EUROPOL | |
| **Agreement with Hellenic Postal Services A.E. - Athens office** | Agreement | ELLINIKA TACHYDROMEIA ELTA AE | 50 EUR/month |
| **Agreement with Hellenic Postal Services A.E. - Heraklion office** | Agreement | ELLINIKA TACHYDROMEIA ELTA AE | 80 EUR/month |
| **Agreement with Translation Centre for the Bodies of the EU** | Agreement | CdT | |
| **Austrian signature scheme for e-card and mobile signature_A-Trust** | Agreement | A-TRUST GESELLSCHAFT FUR SICHERHEITSSYSTEME IM ELEKTRONISCHEN DATENVERKEHR GMBH | |
| **Collaboration Agreement in the field of standardization** | Agreement | CEN & CENELEC | |
| **Cooperation Agreement between ETSI and ENISA** | Agreement | European Telecommunications Standards Institute (ETSI) | |
| **Cooperation Plan 2021 – 2023 between EU-LISA and ENISA** | Agreement | EU-LISA - EUROPEAN AGENCY | |
| **Joint ENISA - EUROPOL /EC3 WG on Security and Safety Online** | Agreement | EUROPEAN POLICE OFFICE EUROPOL | |

| | | | |
|---|---|---|---|
| **Lease Agreement Athens office** | Agreement | Prodea Investments | |
| **Maintenance Agreement for Franking machines** | Agreement | PAPAKOSMAS NTATATECHNIKA EPE | 57 EUR/month |
| **Mandate and Service agreement for "Type II European School" with EC** | Agreement | DG HR | |
| **Mission Charter of the IAS_REVISED** | Agreement | IAS | |
| **Non-Disclosure Agreement CT1607860_Confidential and proprietary document between 12 Parties** | Agreement | | |
| **Provision of water fountain and water bottles for Athens office** | Agreement | EFODIASTIKI KATALANOTIKI AGATHON EPE | 6 EUR/pc |
| **Cooperation Agreement with FORTH** | Memorandum of Understanding | FORTH | |
| **Cooperation between EDA and ENISA** | Memorandum of Understanding | EUROPEAN DEFENCE AGENCY - EDA | |
| **MoU on bilateral cooperation with EUIPO** | Memorandum of Understanding | EUIPO | €16.803,58 |
| **MoU with Universität der Bundeswehr München** | Memorandum of Understanding | Universität der Bundeswehr München (UniBw M) | |
| **Structured cooperation between ENISA and CERT EU** | Memorandum of Understanding | CERT-EU | |
| **Working Arrangement Agreement with eu-LISA** | Memorandum of Understanding | EU-LISA - EUROPEAN AGENCY | |

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

The international strategy foresees a continuation of the strong focus on the EU and EU actors, while also allowing increased flexibility to engage with international partners in line with the strategic objectives outlined in the ENISA Strategy for a Trusted and Cyber Secure Europe of July 2020. The Agency's international strategy was adopted by the MB during the November 2021 meeting.

## XIII. ANNUAL COOPERATION PLAN 2023

To be updated at a later stage.

The 2023 Annual Cooperation Plan between ENISA, the EU Agency for Cybersecurity, and CERT-EU, the CERT of the EU institutions, bodies and agencies will be annexed to the Single Programming Document 2023-2025 as a separate document.

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**
Agamemnonos 14, Chalandri 15231, 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

European Union Agency
for Cybersecurity
Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

Draft Establishment plan 2023[1]

| Category and grade | Establishment plan in draft EU Budget 2022 | | Establishment plan 2023 | |
|---|---|---|---|---|
| | Off. | TA | Off. | TA |
| AD 16 | | | | |
| AD 15 | | 1 | | 1 |
| AD 14 | | | | |
| AD 13 | | 2 | | 2 |
| AD 12 | | 4 | | 4 |
| AD 11 | | 2 | | 2 |
| AD 10 | | 4 | | 3 |
| AD 9 | | 11 | | 12 |
| AD 8 | | 22 | | 25 |
| AD 7 | | 8 | | 10 |
| AD 6 | | 9 | | 4 |
| AD 5 | | | | |
| **Total AD** | | **63** | | **63** |
| AST 11 | | | | |
| AST 10 | | | | |
| AST 9 | | | | |
| AST 8 | | 2 | | 2 |
| AST 7 | | 3 | | 4 |
| AST 6 | | 8 | | 7 |
| 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 | | | | |

[1]The change in the number of establishment plan up to 10% requested for year 2023 is modified as per Art 38 of the ENISA Financial Regulation. In 2022, ENISA will review its staffing strategy and will update a forecast for reclassification also in line with job mapping.

| | | | | |
|---|---|---|---|---|
| AST/SC5 | | | | |
| AST/SC6 | | | | |
| **Total AST/SC** | | | | |
| **TOTAL** | | **82** | | **82** |

# DRAFT Statement of Estimates 2023 (Budget 2023)

*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 2023**

The 2023 total revenue amounts to € 24707182 and consists of a subsidy of € 24110000 from the General Budget of the European Union and EFTA countries' contributions € 597182
Subsidy from the Greek Government for the rent of the offices of ENISA in Greece is no longer available as rent is directly covered by Greece

**2.2 Expenditure in 2023**

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 2023, which contains 81 Temporary Agent posts.

| | | |
|---|---|---|
| Total expenditure under Title 1 amounts to | € | 12.988.813,60 |

**Title 2 - Buildings, equipment and miscellaneous operating expenditure**

| | | |
|---|---|---|
| Total expenditure under Title 2 amounts to | € | 2.895.940,00 |

**Title 3 - Operational expenditure**

| | | |
|---|---|---|
| Operational expenditure is mainly related to the implementation of Work Programme 2023 and amounts to | € | 8.822.428,00 |

# 3. STATEMENT OF REVENUE 2023

| Title | Heading | Voted Appropriations 2021 € | Voted Appropriations 2022 € | Proposed Draft Appropriations 2023 € | Remarks - budget 2023 |
|---|---|---|---|---|---|
| 1 | EUROPEAN COMMUNITIES SUBSIDY | 22.248.000 | 23.633.000 | 24.110.000 | Total subsidy of the European Communities |
| 2 | THIRD COUNTRIES CONTRIBUTION | 585.060 | 574.625 | 597.182 | Contributions from Third Countries. |
| 3 | OTHER CONTRIBUTIONS | 640.000 | 0 | 0 | Subsidy from the Government of Greece |
| 4 | ADMINISTRATIVE OPERATIONS | 0 | 0 | 0 | Other expected income. |
| | **GRAND TOTAL** | **23.473.060** | **24.207.625** | **24.707.182** | |

| Article Item | Heading | Voted Appropriations 2021 € | Voted Appropriations 2022 € | Proposed Draft Appropriations 2023 € | Remarks - budget 2023 |
|---|---|---|---|---|---|
| 1 | EUROPEAN COMMUNITIES SUBSIDY | | | | |
| 10 | EUROPEAN COMMUNITIES SUBSIDY | | | | |
| *100* | *European Communities subsidy* | 22.248.000 | 23.633.000 | 24.110.000 | Regulation (EU) N° 526/2013 establishing an European Union Agency for Network and Information Security. |
| | CHAPTER 10 | 22.248.000 | 23.633.000 | 24.110.000 | |
| | TITLE 1 | 22.248.000 | 23.633.000 | 24.110.000 | |
| 2 | THIRD COUNTRIES CONTRIBUTION | | | | |
| 20 | THIRD COUNTRIES CONTRIBUTION | | | | |
| *200* | *Third Countries contribution* | 585.060 | 574.625 | 597.182 | Contributions from Associated Countries. |
| | CHAPTER 2 0 | 585.060 | 574.625 | 597.182 | |
| | TITLE 2 | 585.060 | 574.625 | 597.182 | |
| 3 | OTHER CONTRIBUTIONS | | | | |
| 30 | OTHER CONTRIBUTIONS | | | | |
| *300* | *Subsidy from the Ministry of Transports of Greece* | 640.000 | 0 | 0 | Subsidy from the Government of Greece. |
| | CHAPTER 30 | 640.000 | 0 | 0 | |
| | TITLE 3 | 640.000 | 0 | 0 | |
| 4 | ADMINISTRATIVE OPERATIONS | | | | |
| 40 | ADMINISTRATIVE OPERATIONS | | | | |
| *400* | *Administrative Operations* | 0 | 0 | 0 | Revenue from administrative operations. |
| | CHAPTER 40 | 0 | 0 | 0 | |
| | TITLE 4 | 0 | 0 | 0 | |
| | GRAND TOTAL | 23.473.060 | 24.207.625 | 24.707.182 | |

# 4. STATEMENT OF EXPENDITURE 2023

| Title | Heading | Voted Appropriations 2021 € | Voted Appropriations 2022 € | Proposed Draft Appropriations 2023 € | Remarks - budget 2023 |
|---|---|---|---|---|---|
| 1 | STAFF | 10.775.409 | 12.494.335 | 12.988.814 | Total funding for covering personnel costs. |
| 2 | BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE | 3.547.651 | 2.824.300 | 2.895.940 | Total funding for covering general administrative costs. |
| 3 | OPERATIONAL EXPENDITURE | 9.150.000 | 8.888.990 | 8.822.428 | Total funding for operational expenditures. |
| | GRAND TOTAL | 23.473.060 | 24.207.625 | 24.707.182 | |
| 1 | STAFF | | | | |
| 11 | STAFF IN ACTIVE EMPLOYMENT | | | | |
| *110* | *Staff holding a post provided for in the establishment plan* | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 1100 | Basic salaries | | 6.453.819 | 8.361.489 | 8.762.162 | 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 | 6.453.819 | 8.361.489 | 8.762.162 | |
| ***111*** | ***Other staff*** | | | | | |
| 1110 | Contract Agents | | 2.106.500 | 1.819.391 | 1.902.614 | 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) | | 250.000 | 657.000 | 693.742 | This appropriation is intended to cover basic salaries and all benefits of SNEs. |
| | | Article 1 1 1 | 2.356.500 | 2.476.391 | 2.596.356 | |
| | | **CHAPTER 11** | **8.810.319** | **10.837.880** | **11.358.518** | |
| **12** | **RECRUITMENT/DEPARTURE EXPENDITURE** | | | | | |
| ***120*** | ***Expenditure related to recruitment*** | | | | | |
| 1200 | Expenditure related to recruitment | | 49.087 | 10.000 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 1201* |
| 1201 | Recruitment and Departure expenditure | | n/a | n/a | 422.796 | This appropriation is intended to cover the travel expenses of staff (including members of their families), the installation allowances for staff obliged to change residence after taking up their duty, the removal costs of staff obliged to change residence after taking up duty, the costs of daily subsistance allowances as per Staff Regulations applicable to officials of the European Communities (SR) and in particular Articles 20 and 71 thereof and Articles 5, 6, 7, 9, 10 of Annex VII thereto, as well as Articles 25 and 67 of the Conditions of Employment of other Servants. 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 | 49.087 | 10.000 | 422.796 | |
| ***121*** | ***Expenditure on entering/leaving and transfer*** | | | | | |
| 1210 | Expenses on Taking Up Duty and on End of Contract | | 32.000 | 17.000 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 1201* |
| 1211 | Installation, Resettlement and Transfer Allowance | | 145.000 | 204.000 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 1201* |
| 1212 | Removal Expenses | | 72.000 | 89.000 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 1201* |
| 1213 | Daily Subsistence Allowance | | 112.000 | 92.000 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 1201* |
| | | Article 1 2 1 | 361.000 | 402.000 | 0 | |
| | | **CHAPTER 1 2** | **410.087** | **412.000** | **422.796** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **13** | **SOCIO-MEDICAL SERVICES AND TRAINING** | | | | | |
| ***131*** | ***Medical Service*** | | | | | |
| 1310 | Medical Service | | 53.882 | 63.000 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 1332* |
| | | Aticle 1 3 1 | 53.882 | 63.000 | 0 | |
| ***132*** | ***Staff Development*** | | | | | |
| 1320 | Staff Development | | 280.182 | 220.000 | 245.000 | This appropriation is intended to cover the costs of language and other training needs as well as teambuilding and other staff development activities. |
| | | Article 1 3 2 | 280.182 | 220.000 | 245.000 | |
| ***133*** | ***Staff Welfare*** | | | | | |
| 1330 | Other welfare expenditure | | 250.000 | 40.000 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 1332* |
| 1331 | Schooling & Education expenditure | | 500.000 | 530.000 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 1332* |
| 1332 | Staff Welfare | | n/a | n/a | 687.500 | This appropriation is intended to cover staff welfare measures such as 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, health related activities to promote well-being of staff, other activities related to internal events, other welfare measures.<br>This appropriation is also 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. |
| | | Article 1 3 3 | 750.000 | 570.000 | 687.500 | |
| | | **CHAPTER 1 3** | **1.084.064** | **853.000** | **932.500** | |
| **14** | **TEMPORARY ASSISTANCE** | | | | | |
| ***140*** | ***European Commission Management Costs*** | | | | | |
| 1400 | EC Management Costs | | 70.939 | 70.000 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2220* |
| | | Article 1 4 0 | 70.939 | 70.000 | 0 | |
| ***142*** | ***Temporary Assistance*** | | | | | |
| 1420 | External Temporary Staffing | | 400.000 | 321.455 | 275.000 | This appropriation is intended to cover the costs of temporary assistance (trainees and interim services). |
| | | Article 1 4 2 | 400.000 | 321.455 | 275.000 | |
| | | **CHAPTER 1 4** | **470.939** | **391.455** | **275.000** | |
| | | **Total Title 1** | **10.775.409** | **12.494.335** | **12.988.814** | |
| **2** | **BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE** | | | | | |
| **20** | **BUILDINGS AND ASSOCIATED COSTS** | | | | | |
| ***200*** | **Buildings and associated costs** | | | | | |
| 2000 | Rent of buildings | | 640.000 | 78.151 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2001* |
| 2001 | Building costs | | n/a | n/a | 1.018.350 | This appropriation is intended to cover various building related costs including the payment of rent for buildings or parts of buildings occupied by the Agency and the hiring of parking spaces, utilities and insurance of the premises of the Agency, cleaning and maintenance of the premises used by the Agency, fitting-out of the premises and repairs in the buildings, costs of building surveillance as well as purchases and maintenance cost of equipment related to security and safety of the building and the staff, expenditure of acquiring technical equipment, as well as maintenance and services related to it, and other costs such as 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. |
| 2003 | Water, gas, electricity, heating and insurance | | 76.050 | 145.317 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2001* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2004 | Cleaning and maintenance | | 120.000 | 250.083 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2001* |
| 2005 | Fixtures and Fittings | | 50.000 | 40.000 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2001* |
| 2007 | Security Services and Equipment | | 140.000 | 157.590 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2001* |
| 2008 | Other expenditure on buildings | | 378.558 | 243.409 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2001* |
| | | Article 2 0 0 | 1.404.608 | 914.550 | 1.018.350 | |
| | | **CHAPTER 2 0** | **1.404.608** | **914.550** | **1.018.350** | |
| **21** | **MOVABLE PROPERTY AND ASSOCIATED COSTS** | | | | | |
| ***210*** | ***Technical Equipment and installations*** | | | | | |
| 2100 | Technical Equipment and services | | 30.000 | 10.000 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2001* |
| | | Article 2 1 0 | 30.000 | 10.000 | 0 | |
| ***211*** | ***Furniture*** | | | | | |
| 2110 | Furniture | | 49.000 | 125.000 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2230* |
| | | Article 2 1 1 | 49.000 | 125.000 | 0 | |
| ***212*** | ***Transport Equipment*** | | | | | |
| 2121 | Maintenance and Repairs of transport equipment | | 10.000 | 10.000 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2230* |
| | | Article 2 1 2 | 10.000 | 10.000 | 0 | |
| ***213*** | ***Library and Press*** | | | | | |
| 2130 | Books, Newspapers and Periodicals | | 10.000 | 15.000 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2230* |
| | | Article 2 1 3 | 10.000 | 15.000 | 0 | |
| | | **CHAPTER 2 1** | **99.000** | **160.000** | **0** | |
| **22** | **CURRENT CORPORATE AND ADMINISTRATIVE EXPENDITURE** | | | | | |
| ***220*** | ***Stationery, postal and telecomunications*** | | | | | |
| 2200 | Stationery and other office supplies | | 30.000 | 27.000 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2230* |
| 2201 | Postage and delivery charges | | 20.000 | 22.000 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2230* |
| | | Article 2 2 0 | 50.000 | 49.000 | 0 | |
| ***221*** | ***Financial charges*** | | | | | |
| 2210 | Bank charges and interest paid | | 1.000 | 1.000 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2230* |
| | | Article 2 2 1 | 1.000 | 1.000 | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***222*** | ***Consultancy and other outsourced services*** | | | | | |
| 2220 | Consultancy and other outsourced services (incl. legal services) | | 747.696 | 270.000 | 328.000 | This appropriation is intended to cover expenditure of contracting consultants linked to administrative support services and horizontal tasks, e.g. in HR area, financial, accounting, internal controls, legal consultancy, advisory, audit, external evaluation, strategic consultancy and/or other administrative support services provided by third parties including EC management costs. |
| | | Article 2 2 2 | 747.696 | 270.000 | 328.000 | |
| ***223*** | ***Corporate and Administrative Expenditures*** | | | | | |
| 2230 | Corporate and Administrative Expenditures | | n/a | n/a | 221.840 | This appropriation is intended to cover corporate and administrative expenditure such as the costs of purchasing, leasing, and repairs of furniture, the costs of maintenance and repairs of transport equipment as well as insurance and fuel, 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, the costs of office stationery and the purchase of office kitchen consumables, post office and special courrier costs, bank charges, interest paid and other financial and banking costs and other costs of corporate administrative nature. |
| | | Article 2 2 3 | 0 | 0 | 221.840 | |
| | | **CHAPTER 2 2** | **798.696** | **320.000** | **549.840** | |
| **23** | **ICT** | | | | | |
| ***231*** | ***Core and Corporate ICT expenditure*** | | | | | |
| 2310 | Corporate ICT recurrent costs | | 585.347 | 1.065.000 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2312* |
| 2311 | Corporate ICT new investments and one-off projects | | 660.000 | 364.750 | n/a | *As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2312* |
| 2312 | Core and corpororate ICT costs | | n/a | n/a | 1.327.750 | This appropriation is intended to cover core and corporate ICT costs including recurrent corporate ICT costs (including support and consulting services) as well as new investments and one-off projects for hardware, software, services and maintenance as well as ENISA website and portals support. |
| | | Article 2 3 1 | 1.245.347 | 1.429.750 | 1.327.750 | |
| | | **CHAPTER 2 3** | **1.245.347** | **1.429.750** | **1.327.750** | |
| | | **Total Title 2** | **3.547.651** | **2.824.300** | **2.895.940** | |
| **3** | **OPERATIONAL EXPENDITURE** | | | | | |
| **30** | **ACTIVITIES RELATED TO OUTREACH AND MEETINGS** | | | | | |
| ***300*** | ***Outreach, meetings and representation expenses*** | | | | | |
| 3001 | Outreach, meetings, translations and representation expenses | | 650.000 | 387.000 | 386.108 | 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 | 650.000 | 387.000 | 386.108 | |
| | | **CHAPTER 3 0** | **650.000** | **387.000** | **386.108** | |

| | | | | | |
|---|---|---|---|---|---|
| **37** | **CORE OPERATIONAL ACTIVITIES** | | | | |
| ***371*** | ***Activity 1 - Providing assistance on policy development*** | | | | |
| 3710 | Activity 1 - Providing assistance on policy development | 280.000 | 363.000 | 314.500 | This appropriation is intended to cover direct operational costs relevant to the Activity 1 (including operational ICT and mission costs). |
| | Article 3 7 1 | 280.000 | 363.000 | 314.500 | |
| ***372*** | ***Activity 2 - Supporting implementation of Union policy and law*** | | | | |
| 3720 | Activity 2 - Supporting implementation of Union policy and law | 985.000 | 798.475 | 803.000 | This appropriation is intended to cover direct operational costs relevant to the Activity 2 (including operational ICT and mission costs). |
| | Article 3 7 2 | 985.000 | 798.475 | 803.000 | |
| ***373*** | ***Activity 3 - Capacity building*** | | | | |
| 3730 | Activity 3 - Capacity building | 1.400.000 | 1.921.265 | 2.028.000 | This appropriation is intended to cover direct operational costs relevant to the Activity 3 (including operational ICT and mission costs). |
| | Article 3 7 3 | 1.400.000 | 1.921.265 | 2.028.000 | |
| ***374*** | ***Activity 4 - Enabling operational cooperation*** | | | | |
| 3740 | Activity 4 - Enabling operational cooperation | 1.110.000 | 1.703.350 | 1.631.520 | This appropriation is intended to cover direct operational costs relevant to the Activity 4 (including operational ICT and mission costs). |
| | Article 3 7 4 | 1.110.000 | 1.703.350 | 1.631.520 | |
| ***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 | 1.200.000 | 824.500 | 1.162.000 | This appropriation is intended to cover direct operational costs relevant to the Activity 5 (including operational ICT and mission costs). |
| | Article 3 7 5 | 1.200.000 | 824.500 | 1.162.000 | |
| ***376*** | ***Activity 6 - Development and maintenance of EU cybersecurity certification framework*** | | | | |
| 3760 | Activity 6 - Development and maintenance of EU cybersecurity certification framework | 870.000 | 1.025.750 | 830.000 | This appropriation is intended to cover direct operational costs relevant to the Activity 6 (including operational ICT and mission costs). |
| | Article 3 7 6 | 870.000 | 1.025.750 | 830.000 | |
| ***377*** | ***Activity 7 - Supporting European cybersecurity market and industry*** | | | | |
| 3770 | Activity 7 - Supporting European cybersecurity market and industry | 490.000 | 373.800 | 325.000 | This appropriation is intended to cover direct operational costs relevant to the Activity 7 (including operational ICT and mission costs). |
| | Article 3 7 7 | 490.000 | 373.800 | 325.000 | |
| ***378*** | ***Activity 8 - Knowledge on emerging cybersecurity challenges and opportunities*** | | | | |
| 3780 | Activity 8 - Knowledge on emerging cybersecurity challenges and opportunities | 1.155.000 | 1.051.950 | 961.300 | This appropriation is intended to cover direct operational costs relevant to the Activity 8 (including operational ICT and mission costs). |
| | Article 3 7 8 | 1.155.000 | 1.051.950 | 961.300 | |
| ***379*** | ***Activity 9 - Outreach and education*** | | | | |
| 3790 | Activity 9 - Outreach and education | 1.010.000 | 439.900 | 381.000 | This appropriation is intended to cover direct operational costs relevant to the Activity 9 (including operational ICT and mission costs). |
| | Article 3 7 9 | 1.010.000 | 439.900 | 381.000 | |
| | **CHAPTER 3 7** | **8.500.000** | **8.501.990** | **8.436.320** | |
| | **TITLE 3** | **9.150.000** | **8.888.990** | **8.822.428** | |
| | **GRAND TOTAL** | **23.473.060** | **24.207.625** | **24.707.182** | |