EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA SINGLE PROGRAMMING DOCUMENT 2021–2023

Including multiannual planning, work programme 2021 and multiannual staff planning

JANUARY 2021

CONTACT

For contacting ENISA please use the following details:
info@enisa.europa.eu
website: www.enisa.europa.eu

LEGAL NOTICE

COPYRIGHT NOTICE

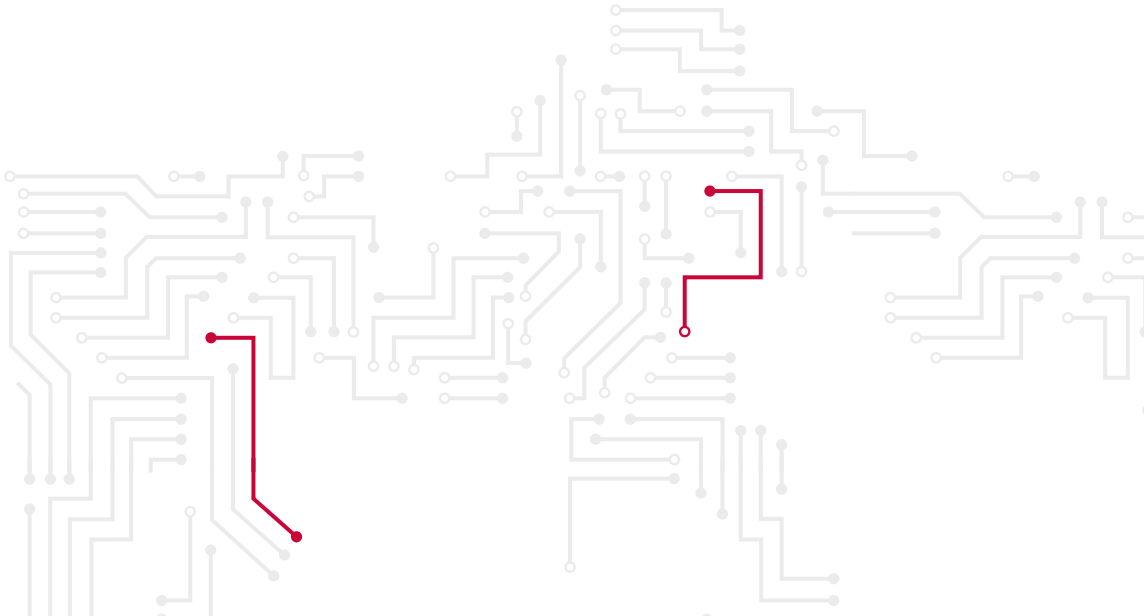
Luxembourg: Publication Office of the European Union, 2020

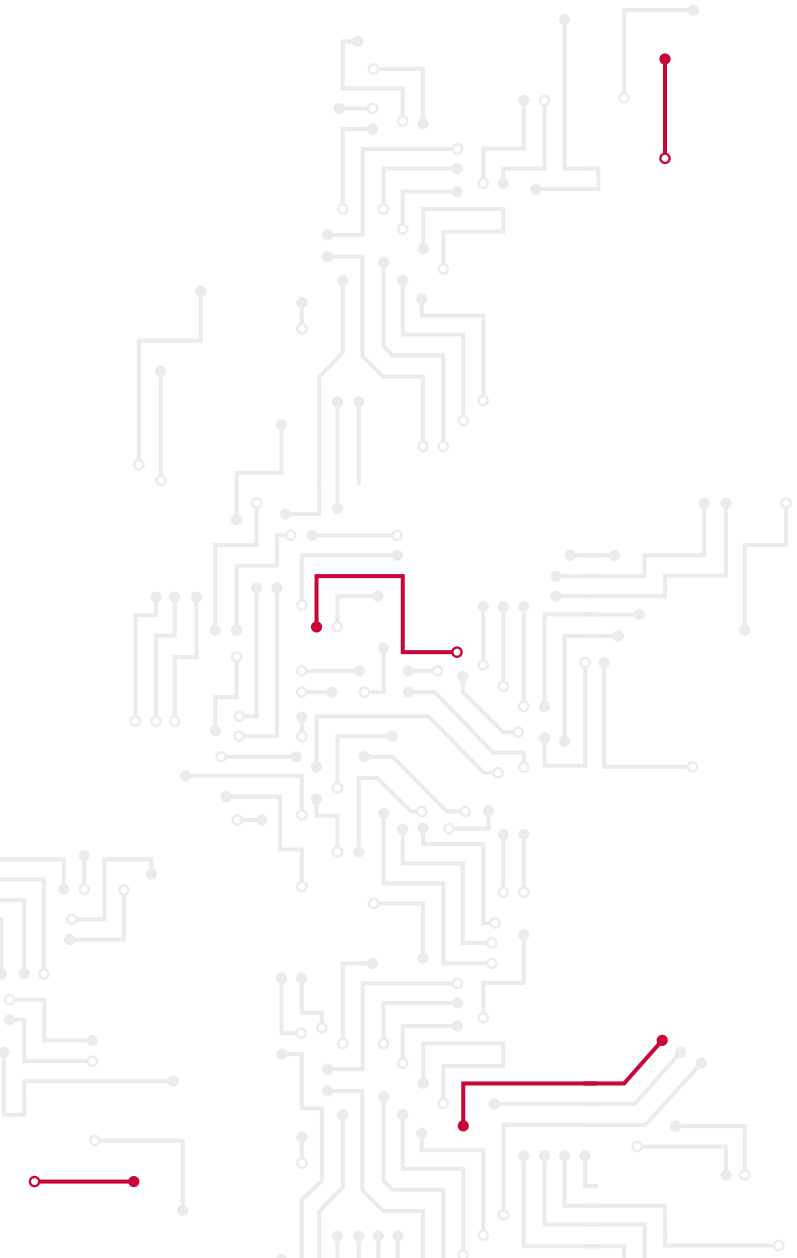
Book	ISBN 978-92-9204-459-6	ISSN 2467-4397	DOI 10.2824/325038	TPAH-21-001-EN-C
PDF	ISBN 978-92-9204-460-2	ISSN 2467-4176	DOI 10.2824/668201	TPAH-21-001-EN-N

ENISA SINGLE PROGRAMMING DOCUMENT 2021–2023

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TABLE OF CONTENTS





FOREWORD

This new **Single Programming Document (SPD) 2021–2023** marks a new step in the planning of the operations and activities, as well as the planning and use of resources by the European Union Agency for Cybersecurity (ENISA).

First, it has been developed to enable the Agency to fully exploit its permanent mandate and fulfil all the tasks given to it by the EU Cybersecurity Act (CSA), while taking into account all other changes in the EU's regulatory framework. All the activities and outputs in this work programme stem from, and are clearly derived from, the statutory obligations of the Agency; none of the statutory tasks is neglected.

Moreover, the planning document also makes full use of the different statutory bodies set up by the CSA (such as the National Liaison Officers (NLO) Network) and EU law to guide and help the Agency to design and validate the specific deliverables that the Agency will produce across the activities anticipated in this SPD. This will ensure that the activities undertaken in accordance with this SPD will be carried out in cooperation and in synergy with all relevant actors at EU and national levels.

The new SPD is fully aligned with and incorporates the changes introduced to the design and set-up of the SPDs of EU bodies, as adopted by the European Commission in April 2020[1].

Second, the new SPD is in line with ENISA's new strategy, which was adopted by the management board in June 2020 and has been used as a baseline to set the strategic objectives and priorities for programming the Agency's work using a multiannual framework.

Third, this programming document has been drawn up in parallel with the reorganisation of the Agency, which was agreed by the management board in June 2020 and will become effective on 1 January 2021, the same day that this SPD will become operational. As the

1 Communication from the Commission on the strengthening of the governance of Union bodies under Article 70 of the Financial Regulation 2018/1046 and on the guidelines for the Single Programming Document and the Consolidated Annual Activity Report, C(2020)2297 final, 20.04.2020, Brussels.

new organisational structure aligns the tasks and functions of the Agency's structural set-up with the CSA, it will not only allow more efficient delivery of the activities foreseen in the SPD but also ensure that there are sufficient capabilities within the Agency to fulfil its obligations and undertakings in an effective manner.

Finally, this SPD acknowledges and takes into account the ever-shifting cyber landscape and evolving wider socioeconomic context. The COVID-19 crisis has demonstrated the ability of the Agency to rapidly shift its priorities, as well as rise to the challenge of catering for the cybersecurity needs of a society that has undergone a massive digital transition of its functions, posing new risks as well as opportunities. This SPD, while being clear on the scope of different activities and outputs, allows for sufficient flexibility in designing individual deliverables to ensure that the Agency's activities and contributions will be able to take into account the most recent developments, thus providing high added value to the EU at large and the best value for money for the European taxpayer.

Juhan Lepassaar
Executive Director

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 cyber 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

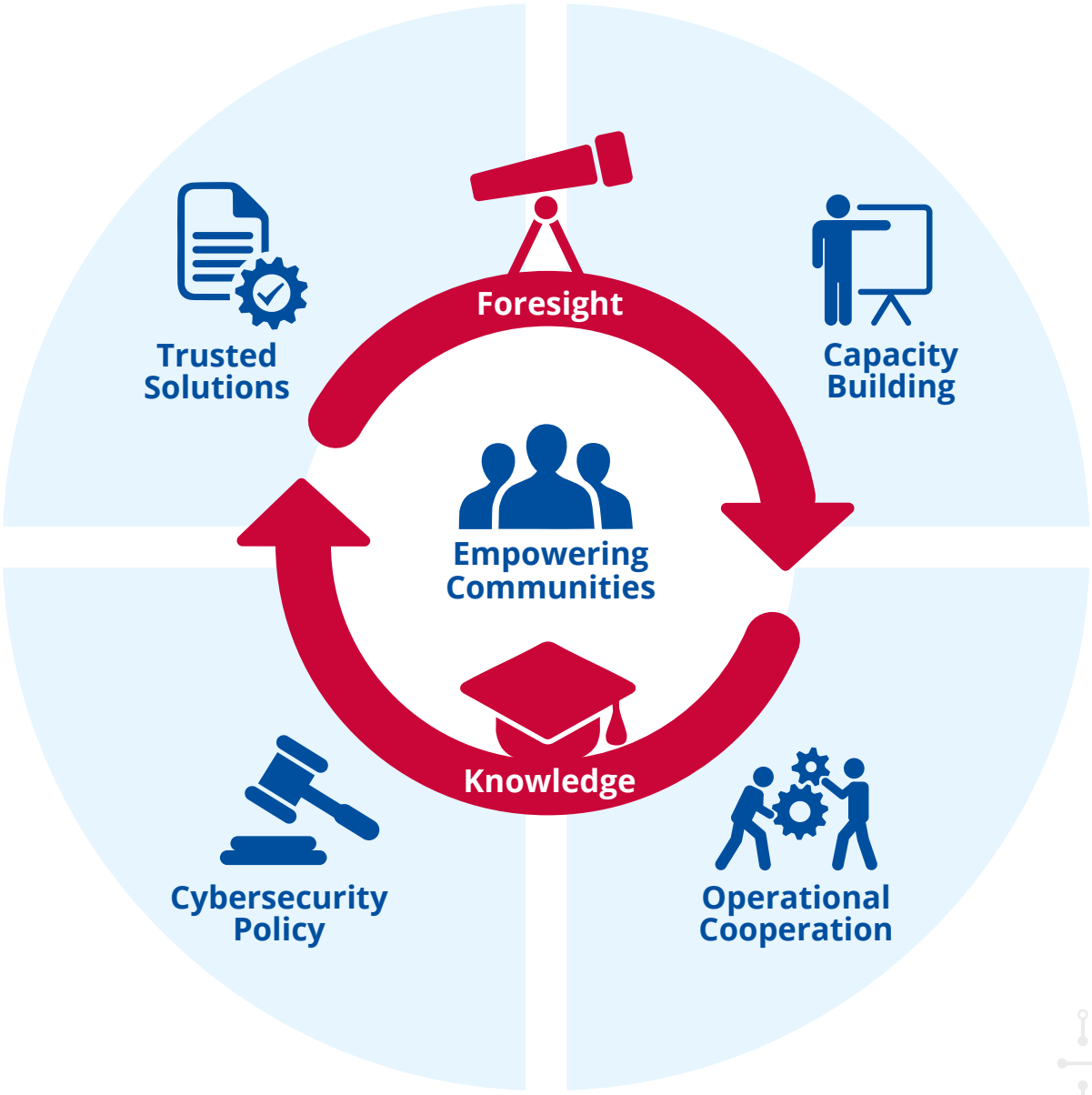
Cybersecurity is the cornerstone of digital transformation and the need for it permeates all sectors, therefore it needs to be considered across a broad range of policy fields and initiatives. Cybersecurity must not be restricted to a specialist community of technical cyber experts. Cybersecurity must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

OPERATIONAL COOPERATION

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

CAPACITY BUILDING

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



TRUSTED SOLUTION

Digital products and services bring 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, we need a continuous process of collecting, organising, summarising, analysing, communicating, and maintaining cybersecurity information and knowledge. All phases are essential to ensure that information and knowledge is shared and expanded within the EU cybersecurity ecosystem.

PART I
GENERAL CONTEXT

On 27 November 2019, during the plenary session in Strasbourg, President von der Leyen presented the views and objectives of the European Commission for the entirety of its mandate 2019–2024, noting that[2]:

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

With the enactment of the Cybersecurity Act (CSA) in June 2019, the European Union Agency for Cybersecurity (ENISA) became a key instrument for realising the EU's ambition of significantly reinforcing cybersecurity across Europe. The strengthened and expanded tasks of the Agency in the field of operational cooperation were tested in 2020 with the need to ensure adequate cybersecurity throughout the coronavirus disease 2019 (COVID-19) crisis presenting the Agency with a challenge. Acting in the context of Article 7 of the CSA, ENISA undertook a number of activities[3] that played an important role in helping EU bodies coordinate their activities throughout the initial phases of the pandemic and in raising the resilience of the EU. These practical steps and actions are not expected to be one-off endeavours, but will continue to be pursued through the evolving Blueprint and could be merged, if necessary, with the Joint Cyber Unit framework, as this concept, announced by President von der Leyen in 2019, is due to be developed further. The year 2021 will also mark the point when structured cooperation between ENISA and CERT-EU in the field of operational cooperation (pending endorsement by the management board) becomes fully operational, influencing the activities anticipated in the 2021 work programme of this SPD and beyond.

The CSA also set up a framework for European cybersecurity certification schemes with a view to creating a digital single market for ICT products, services and processes. The Agency began to execute this function fully in 2020, in particular for candidate schemes for common criteria and cloud services. This work will continue in 2021, taking into account not

2 Ursula von der Leyen, President-elect of the European Commission, 'Speech in the European Parliament Plenary Session: As delivered', pp. 9–10 (https://ec.europa.eu/info/sites/info/files/comm-2019-00612-00-00-en-tra-00_0.pdf).

3 Including initiating contacts with the European Commission, the European Union Agency for Law Enforcement Cooperation's (Europol) European Cybercrime Centre (EC3) and the Computer Emergency Response Team for the EU (CERT-EU) to establish an information exchange network, which subsequently attracted the participation of the European External Action Service (EEAS) and the Council of the European Union; contributing to the technical annex of the Commission's recommendation on contact tracing apps.

only the demands of the emerging EU rolling work programme for European cybersecurity certification, but also the increasing calls to take practical steps in order to ensure the EU's digital sovereignty and autonomy. The need to contribute to raising the competitiveness of the European cybersecurity market and industry, including by advising and assisting EU bodies (including the Cybersecurity Competence Centre and Network[4]) in setting cybersecurity research and innovation priorities, as well as by providing regular insights into how both the supply side and the demand side of the market function, will begin in 2021 and continue to grow in the years to come.

The Agency will continue to support EU decision-making institutions in relation to the announced review of the security of networks and information systems (NIS) directive. This renewal and strengthening of a key pillar of the EU's regulatory framework, which underpins the cybersecurity of critical sectors across our society, could further make use of the expanded and permanent mandate given to the Agency and thus also influence the development of the ENISA work programme in the years to come. The Agency will need to anticipate and be ready to contribute to the development and implementation of EU laws and policies in different sectors, including in relation to the European Electronic Communications Code (EECC), by providing expertise in and technical input to cybersecurity aspects across different policy fields and helping to fulfil new tasks, should it be called to do so by EU institutions and Member States.

Beyond the context of political and legislative developments, the COVID-19 pandemic has dramatically altered the EU's economic outlook and posed new challenges to the functioning of European society. The almost overnight global transition to digital solutions, in order to keep the essential functions of societies working across different fields, is unprecedented. Never before have people been forced to embrace the digital world over the physical world on such a scale, and this poses new risks, as well as challenges, in terms of ensuring a high level of cybersecurity across the EU. The Agency, rising to meet this challenge, has dramatically increased its capabilities, as well as channelled resources to this work programme, to assist with capacity-building activities in critical areas touched by the crisis. It has furthermore prioritised both targeted and general actions to raise awareness of and foster education in cybersecurity.

During these unprecedented times, it is more important than ever that the Agency increases its outreach activities and builds and utilises synergies among all relevant actors at the EU level and beyond, to ensure a coherent and joined-up approach to enhancing cybersecurity across the EU, as well as contributing to efforts to ensure that global developments across the cybersecurity landscape are aligned with and enlightened by the EU's values, to increase its competitiveness. The development of stakeholder and international strategies of the Agency will establish important baselines that will frame actions to this end, and thus impact the evolvement of the work programme in the future.

4 In September 2018, the European Commission proposed a regulation setting up a European Cybersecurity Competence Centre and Network. The (draft) regulation ensures cooperation and complementarity with ENISA. In particular, ENISA will have an important role in contributing to the Centre's strategic role in coordinating cybersecurity technology-related investments by the EU, Member States and industry. The Council agreed its negotiating position in June 2020 and the trilogies with the European Parliament began in summer 2020.

II

PART II

MULTIANNUAL PROGRAMMING 2021–2023

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 CSA and outlines how the Agency will strive to meet the expectations of the cybersecurity ecosystem in the long term in a manner that is open, innovative and agile, as well as being socially and environmentally responsible. The strategy sets out a vision of 'a trusted and cybersecure Europe' in which all citizens and organisations of Europe not only benefit from but also are key components in the effort to secure Europe. Importantly, the new ENISA strategy outlines seven strategic objectives, which are derived from the CSA and set the expected long-term goals for the Agency.

The most fundamental objective, which weaves across all other objectives because of the nature of cyber-security being a shared responsibility, is the strategic objective of **empowered and engaged communities across the cybersecurity ecosystem.** The Agency strives to ensure complementarity of common efforts, exploring synergies and the effective use of limited cybersecurity expertise and resources, which can be achieved only through organised interactions between all players in the cybersecurity ecosystem.

The following two strategic objectives both have an integral role in relation to the other strategic objectives because they are the lenses with which the other objectives operate. The objective of **foresight on emerging and future cybersecurity challenges** provides an understanding of emerging trends and patterns in order to define early mitigation strategies that improve the EU's resilience to cybersecurity threats.

The energy that fuels the mill of cybersecurity is information and knowledge, which relates to the strategic objective of **efficient and effective cybersecurity information and knowledge management for Europe.** To address the challenges of our time, we need to undergo a continuous process of collecting, organising, summarising, analysing, communicating and maintaining cybersecurity information and knowledge. All of these phases are essential for ensuring that information and knowledge are shared and expanded within the EU cybersecurity ecosystem.

The remaining strategic objectives tackle vertical domains of cybersecurity. The strategic objective of **cybersecurity as an integral part of EU policies** seeks to embed cybersecurity across all domains of EU policy. Avoiding fragmentation and ensuring a coherent approach while taking into account the specificities of each sector are essential.

The strategic objective of **effective cooperation among operational actors within the EU in case of massive cyber incidents** seeks to strengthen effective cooperation between Member States and EU

institutions in order to respond to large-scale cross-border cyberattacks and cyber crises.

The strategic objective of **cutting-edge competences and capabilities in cybersecurity across the EU** seeks to address the gap between the supply of and need for cybersecurity knowledge and competences and ensure that different operational communities have the appropriate capacity to deal with the cyberthreat landscape.

The strategic objective of a **high level of trust in secure digital solutions** seeks to generate trust in citizens with regard to ICT products, services and processes through the deployment of certification schemes.

Table 1. The strategic objectives against the articles of the CSA and the activities of the work programme

Strategic objective	Actions to achieve objective	Article of the CSA	Expected results	
SO1 – Empowered and engaged communities across the cybersecurity ecosystem	Activities 1–9	Articles 5–12	• Empowered ecosystem encompassing Member States authorities, EU institutions, agencies and bodies, associations, research centres and universities, industry, and private actors and citizens, who all play their role in making Europe cybersecure	
SO2 – Cybersecurity as an integral part of EU policies	Activities 1 and 2	Article 5	• Where relevant, support the European Commission in ensuring that EU and national policies take account of cybersecurity aspects	
			• Consistent implementation of EU policy and law in the area of cybersecurity • EU cybersecurity policy implementation reflects sectorial specificities and needs • Exchange of good practice	
SO3 – Effective cooperation amongst operational actors within the Union in case of massive[5] cyber incidents	Activities 4 and 5	Article 7	• All communities (EU institutions and Member States) use a rationalised set of standardised operating procedures (SOPs) • An agreed CSIRTs Network approach for selecting, operating and decommissioning tools • Coherent SOPs for cyber crisis management • Efficient framework, tools and methodologies for effective cyber crisis management	
			• Member States and institutions cooperating effectively during large-scale cross-border incidents or crises • Public informed on a regular basis of important cybersecurity developments • Stakeholders aware of current cybersecurity situation	
SO4 – Cutting-edge competences and capabilities in cybersecurity across the EU	Activities 3 and 9	Articles 6 and 7(5)	• Enhanced capabilities across the community • Increased cooperation between communities	
		Articles 10 and 12	• Greater understanding of cybersecurity risks and practices • Stronger European cybersecurity through higher global resilience	

5 Large scale and cross-border.

	Key performance indicator	Metrics
	Community building across the cybersecurity ecosystem	**1.** Additional quantitative measures stemming from the stakeholder strategy that will be developed in 2021 **2.** Stakeholder satisfaction with ENISA's role as a facilitator of community building and collaboration across the cybersecurity ecosystem
	ENISA's added value to EU institutions, bodies and Member States in providing support for policymaking (ex ante)	**1.** Number of relevant contributions to EU and national policies and legislative initiatives **2.** Number of references to ENISA reports, analysis and/or studies in EU and national policy documents **3.** Satisfaction with ENISA added value and weight of contributions (survey)
	Contribution to policy implementation and implementation monitoring at EU and national levels (ex post)	**1.** Number of EU policies and regulations implemented at national level supported by ENISA **2.** Number of ENISA reports, analysis and/or studies referred to at EU and national levels (survey) **3.** Satisfaction with ENISA added value and weight of support (survey)
	Effective use of ENISA's tools and platforms and take-up of SOPs in operational cooperation	**1.** Number of users, both new and recurring, and usage per platform/tool/SOP provided by ENISA **2.** Uptake of platforms/tools/SOPs during massive cyber incidents **3.** Stakeholder satisfaction with regard to the relevance and added value of platforms/tools/SOPs provided by ENISA
	ENISA's ability to support responses to massive cyber incidents	**1.** Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents for which ENISA contributes to mitigation efforts **2.** Stakeholders' satisfaction with ENISA's ability to provide operational support survey
	Increased resilience to cybersecurity risks and preparedness to respond to cyber incidents	**1.** Increase/decrease in maturity indicators **2.** Outreach, uptake and application of lessons learned from capability-building activities **3.** Number of cybersecurity programmes (courses) and participation rates **4.** Stakeholder assessment of the usefulness, added value and relevance of ENISA capacity-building activities
	Level of awareness of cybersecurity, cyber hygiene and cyber literacy across the EU	**1.** Number of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics **2.** Level of awareness of cybersecurity across the EU / general public (e.g. EU barometer)

Strategic objective	Actions to achieve objective	Article of the CSA	Expected results	
SO5 – High level of trust in secure digital solutions	Activities 6 and 7	Article 8	• Support for schemes chosen to run under the European cybersecurity certification framework • Certified ICT products, services and processes are preferred by consumers and, where relevant, Operators of Essential Services and Digital Service Providers	
			• Where relevant, contribution towards a more competitive European cybersecurity industry, small and medium-sized enterprises and start-ups	
SO6 – Foresight on emerging and future cybersecurity challenges and **SO7 – Efficient and effective cybersecurity information and knowledge management for Europe**	Activity 8	Articles 9 and 11	• Decisions about cybersecurity are future-proof and take account of trends, developments and knowledge across the ecosystem • Stakeholders receive relevant and timely information for policy- and decision-making	

ENISA's strategy also establishes a set of values that guide the execution of its mandate and its functioning, as follows.

Community mindset. ENISA works with communities, respecting their competences 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 with regard to its services and working environment, ensuring fairness and inclusiveness.

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

Responsibility. ENISA assumes responsibility, ensuring the integration of 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 encapsulated 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 Article 4(1) of the CSA, which obliges 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 the management board decision MB/2020/5 on the principles to be applied for organising ENISA. The aim is 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 Article 3(4) of the CSA, which obliges the Agency to 'develop its own resources, including … human capabilities and skills, necessary to perform

	Key performance indicator	Metrics
	Uptake of the European cybersecurity certification framework and schemes as an enabler of secure digital solutions Effective preparation of candidate certification schemes prepared by ENISA	**1.** Number of stakeholders (governments or commercial solution providers) on the EU market using the cybersecurity certification framework for their digital solutions **2.** Citizens' trust in digital solutions **3.** Satisfaction with ENISA's support for the preparation of candidate schemes (survey)
	Recognition of ENISA's supporting role for participants in the European cybersecurity market	**1.** Number of market analyses, guidelines and good practices issued by ENISA **2.** Uptake of lessons learned / recommendations from ENISA reports **3.** Stakeholder satisfaction with the added value and quality of ENISA's work
	ENISA's ability to contribute to Europe's cyber resilience through the provision of timely and effective information and knowledge	**1.** Number of users and frequency of use of dedicated portal (observatory) **2.** Number of recommendations, analyses and challenges identified and analysed **3.** Stakeholder satisfaction with the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges and opportunities (including in research)

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 management board decision MB/2020/5 on the principles to be applied for organising ENISA. The aim is for ENISA to respect fundamental European rights and values in its working environment, assume responsibility for the social and environmental dimensions of its procedures and develop its staff competences, expertise and talent.

Table 2.

Corporate objective	Activity to achieve objective	Article of the CSA	Expected results	
Sound resource and risk management	Activity 10	Article 4(1)	Maximise value for money provided to stakeholders and citizens Build lasting credibility and trust	
Build an agile organisation focused on people	Activity 11	Article 3(4)	ENISA as an employer of choice	

2.1. HUMAN AND FINANCIAL RESOURCES – OUTLOOK FOR 2021–2023

2.1.1. Overview of the past and current situation

This section will briefly describes the development of the staff population, revenue and expenditure and the reasons for the changes.

With the enactment of the CSA both staff numbers and the financial resources of the agency have grown, reflecting the expanded tasks and mandate of the Agency. The Agency has historically found it very hard to recruit and retain the talent it needs to fulfil its mandate as the job market for cybersecurity skills is highly specialised and extremely competitive. This 'deficiency' was reflected in the average occupancy rate of the establishment plan, which was 88.3 % in 2017–2019. In turn, the unfulfilled posts have been a source of 'systemic surpluses' within the Agency's budget, requiring some amendments over the financial year to absorb the funds that were not used for staff salaries.

The occupancy rate of the establishment plan has also been a cause for concern in 2019 and 2020 for a number of reasons, including the mid-year enactment of the CSA in 2019, which put a stress on recruitment, and the outbreak of the COVID-19 pandemic, which delayed the launch and conduct of recruitment operations in 2020, as well as the change in senior manager, development of a new strategy for the Agency and launch of reorganisation, all of which have complicated the process of defining the competences and talent that the Agency requires to fulfil its new objectives and functions.

Table 3.

	2019	2020
Establishment plan posts	59	69
Occupancy rate (%)	87	75*

*As of July 2020; this rate is expected to grow significantly by the end of the year.

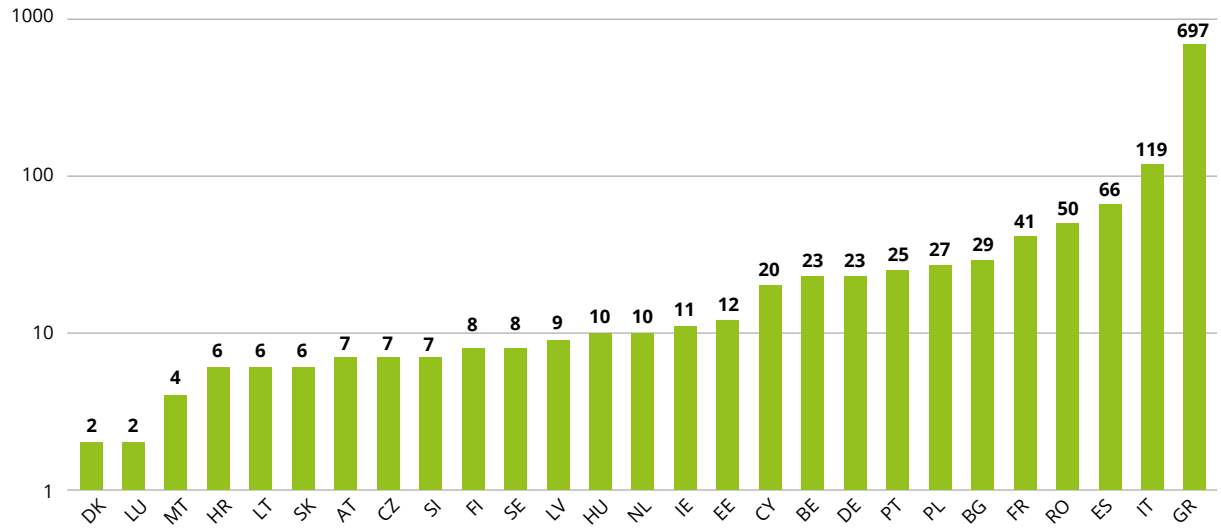
To overcome these challenges, at the beginning of 2020 the Agency embarked on a large-scale novel recruitment exercise with the aim of creating a sufficiently diverse and broad reserve shortlist of 75 candidates with more transversal competences and skills that could be used to recruit staff into grades AD6–AD8 and functions and thus fill the gaps in the current establishment plan, as well as serve as a pool of candidates for the establishment plan in 2021 and 2022 if necessary. The call, which was accompanied by a widespread promotion campaign, attracted 1 235 candidates (who submitted more than 1 600 applications) across all Member States (please see graph below), a result that is unprecedented in the history of the Agency. This has already resulted in a reserve shortlist of 69 candidates, from which

	Key performance indicator	Metrics
	Organisational performance culture	**1.** Proportion of key performance indicators reaching target levels **2.** Individual contribution to achieving the objectives of the Agency through a clear link to key performance indicators (career development plan report) **3.** Exceptions in the risk register **4.** Number of complaints filed against ENISA, including number of inquiries/complaints submitted to the European Ombudsman **5.** Results of the annual risk assessment exercise **6.** Observations from external audit bodies such as the European Court of Auditors (ECoA) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings)
	Staff commitment, motivation and satisfaction	**1.** Staff satisfaction survey (including attractiveness of ENISA as an employer, staff empowerment, organisational culture, opportunities for internal mobility, work space, work environment and work tools) **2.** Quality of ENISA training and career development activities organised for staff **3.** Reasons for staff departure (exit interviews) **4.** Staff retention / turnover rates **5.** Resilience and quality of ENISA information technology (IT) systems and services

recruitment has already been launched. This outcome needs to be added to the ongoing contracts agent call, which has attracted over 600 applications and is currently ongoing.

While the gender balance in the Agency follows trends in technology-dominated areas of the job market, the Agency proactively pursues gender balance with varying degrees of success. Agency staff citizenship is dominated by citizens of Member State of seat agreement, and to a lesser extent by citizens of neighbouring Member States; however, the diversity of candidates responding to the ongoing call might remedy this to some extent. Although geographical balance is a chronic issue, in the job market of the host Member State, ENISA represents a sound

Figure 1. Origin of candidates responding to the 2020 temporary agents call (AD6–AD8)



employer that has been proved to be reliable through a period of economic challenges in the EU. Overall, the situation of the Agency is not that dissimilar to the situation of other agencies.

Further information on appraisal of performance and reclassification/promotions, mobility policy, gender and geographical balance and schooling is provided in the annexes to this report.

2.1.2. Outlook for 2021–2023

In terms of the evolution of tasks, the CSA set out new levels of performance and cooperation that need to be met by the Agency's staff. In addition, and as noted in Section I, the expected political and legislative developments place a demand on the Agency to develop the necessary skills and expertise to cater for increasing needs in fulfilling its mandate in the field of operational cooperation, as well as international cooperation, both of which are relatively new tasks for the Agency.

The overarching need to grow the Agency's capabilities can be met by either (a) developing talent and measuring staff performance or (b) recruiting new staff who possess the competences required to meet the requirements of the CSA.

With regard to competence development, the Agency already has experience in learning and development that continuously produces outcomes in the areas of cybersecurity, project management, finance, etc. The area of performance management currently covers annual appraisals, reclassification and the linking of appraisals with training needs. There is a need, however, to develop more precise metrics for performance management and use information systems to this end, a process that has been kick-started with this SPD.

The shift in the profiles of newly recruited staff is also likely to lead to benefits for the Agency as it is expected that greater collaboration across agency verticals will be instigated. The push towards interdisciplinary and social science-based profiles is likely to support the areas that the Agency expects to develop in the years to come.

Better retention rates have lowered the impact of staff turnover on the Agency and, combined with the outcome of the 2020 temporary agents call, which has provided the agency with a sufficient number of shortlisted candidates to enable rapid recruitment, it is anticipated that in the next few years payroll expenditure will become more predictable, as the Agency has historically implemented the establishment plan as approved by the budgetary authority. The Agency has provided significant, albeit not always balanced, opportunities for reclassification to its staff.

While mobility in the Agency has been a continuing concern of management, several readjustments of its resources have taken effect over the past few years in an effort to seek the right balance between tasks and performance. The Agency will have have adapted its resources to the new environment set up by the CSA by the end of 2020.

In contrast to the three initial management posts, in the past 8 years the Agency has relied on a high number of management posts, which has allowed for a broader distribution of tasks and possibly more targeted control at the various stages of processing of tasks. However, with the implementation of the new structure in 2021, the number of middle management posts is expected to decrease and stabilise, from eight to six. It is hereby affirmed that the executive director is the senior manager of the Agency.

2.1.3. Resource programming for 2021–2023

2.1.3.1. Financial resources

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

Table 4.

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

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

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

2.1.4. Strategy for achieving efficiency gains

ENISA is committed to continue to implement measures to obtain efficiency gains in all activities. The new structure of the organisation, adopted and endorsed by its management board in June 2020, has been developed to specifically achieve and follow the principles of sound budgetary management and build efficiencies in both executing its core mandate and fulfilling its corporate functions.

Within the domain of its operational activities, the Agency is revolutionising its approach by implementing its work programme in such a way as to ensure efficiencies and maximise its added value. In particular, it will seek to systematically use its statutory bodies (National Liaison Officers (NLO) Network, ENISA Advisory Group), as well as other statutory groups that it is involved in (Stakeholder Cybersecurity Certification Group (SCCG), as set out in CSA Article 22, NIS Cooperation Group (NIS CG) and its workstreams, expert groups created under EU law) and its own ad hoc expert groups, where appropriate, to peer review the scope and direction of actions undertaken to achieve outputs, as well as validate the results. In 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 take into consideration existing Member State expertise. Hence, all activities listed in Sections 3.1 and 3.2 of this SPD include an indication of how specific deliverables and other actions undertaken to achieve the outputs will be validated and peer reviewed or consulted as per the legal framework in the area of certification.

The Agency is also setting up a framework for structured cooperation with CERT-EU to utilise synergies and avoid the duplication of activities in executing its tasks in the field of operational cooperation (Article 7 of the CSA). In addition, the establishment of a local office in Brussels should enable the Agency to create further collaborations with other EU institutions, agencies and bodies with regard to these and other activities. The Agency is also pursuing cooperation with relevant EU bodies (Joint Research Centre) and will embark on creating synergies with the Cybersecurity Competence Centre and Network once it is established to enable collaboration 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 benchmark its activities against 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 (with the European Union Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA), European Union Intellectual Property Office (EUIPO)) and in 2020 the Agency signed a service-level agreement with the European Centre for the Development of Vocational Training (Cedefop), which is also located in Greece, to enable further collaboration. This will include the setting up of a joint compliance function and the sharing of procurement procedures.

Prompted by the COVID-19 crisis, the Agency is reviewing its digital and tele-working framework and will embark on actively seeking efficiency gains through the digitalisation of its functions in all endeavours. It is already using EU tools such as accrual-based accounting (ABAC), ABAC assets, procurement and e-invoicing. Furthermore, in 2020, the Agency deployed Sysper and it is examining the migration of its services to other tools, such as Mission Processing System (MIPS) and eRecruitment. The Agency is using a basic workflow application called Paperless that makes handwritten signatures for internal approval redundant. Most administrative tasks are already supported by Paperless and other applications, which has enabled significant steps to be taken towards the aim of implementing 100% e-administration.

E-training is also encouraged internally with the aim, among other things, of reducing the associated costs of 'classroom' training (e.g. travelling costs). However, in view of the COVID-19 pandemic the Agency will also review the training, conferences and seminars provided for external parties and upgrade its capabilities to use secure digital conferencing across the field, providing further opportunities for efficiency gains, as well as expanding the scale and scope of its activities.

PART III

WORK PROGRAMME FOR 2021

This section describes the main body of the work programme, what the Agency aims to deliver in 2021 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 2021.

3.1. OPERATIONAL ACTIVITIES

Activity 1: Providing assistance on policy development

Overview of activity

This activity delivers assistance and advice to the EU and Member States in developing cybersecurity policy and sector-specific policy and law initiatives where matters related to cybersecurity are involved.

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 providing support in emerging policy areas (such as artificial intelligence, 5G and response to current and future crises), ENISA – in coordination with the European Commission and Member States – will also conduct policy scouting to support them to identify potential areas for policy development, as well as develop monitoring capabilities and tools to regularly and consistently be able to give advice on the effectiveness of existing EU policy and law.

The added value of this activity is to support decision-makers in a timely manner with regard to developments at the technological, societal or economic market level that affect the cybersecurity policy framework (see also Activity 8). Given the cross-cutting nature of cybersecurity across the policy landscape, the activity will provide not only an up-to-date risk-based analysis of cybersecurity in the areas of critical infrastructure and sectors, but also 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)
- Provide EU policymakers and stakeholders with timely and tailor-made policy recommendations on future cybersecurity challenges and opportunities
- Regularly inform EU policymakers about the effectiveness of the existing framework

Results	Link to strategic objective (ENISA strategy)
Where relevant, support the European Commission in ensuring that EU and national policies take into account cybersecurity aspects	• Cybersecurity as an integral part of EU policies • Empowered and engaged communities across the cybersecurity ecosystem
Outputs	**Key performance indicator**
1.1. Issue reports, studies and analysis on the effectiveness of the current cybersecurity policy framework in a requested area and the relevant best practices **1.2.** Support the European Commission and Member States by providing tailor-made advice and recommendations on new policy initiatives that tackle emerging technological, societal and economic trends **1.3.** Assist the Commission in reviewing the NIS directive	**Indicator:** ENISA's added value to EU institutions, bodies and Member States in providing support for policymaking (ex ante) **Metrics:** **1.1.** Number of relevant contributions to EU and national policies and legislative initiatives[6] **1.2.** Number of references to ENISA reports, analysis and/or studies in EU and national policy documents **1.3.** Satisfaction with ENISA added value and weight of contributions (survey) **Frequency:** Annual (1.1 and 1.2), biennial (1.3)
Validation	**Target groups and beneficiaries**
• NIS Cooperation Group (outputs 1.1 and 1.2) • ENISA ad hoc working groups[7] (output 1.2) • NLO Network and ENISA Advisory Group (when necessary)	EU and national policymaking institutions; EU and national experts (NIS Cooperation Group), relevant/ competent EU or Member State organisations/bodies)
Resources planned	
Human resources (FTEs)	Financial resources (EUR)
Total 6	**Total 280 000**

6 Targets TBD in 2021

7 Created under Article 20(4) of the CSA.

Activity 2: Supporting implementation of Union policy and law

Overview of activity

This activity provides support to Member States and EU Institutions in the implementation of European cybersecurity policy and legal frameworks and advice on specific cybersecurity aspects related to the NIS directive, telecom security and the security of electronic communications, data protection, privacy, electronic identification (eID) and trust services, incident notification and the general availability or integrity of the public core of the open internet. It further supports initiatives related to implementation of policy frameworks on novel digital technologies such as artificial intelligence, machine learning and the internet of things and networking technologies such as 5G (e.g. 5G security toolbox) and assists with the work of the NIS Cooperation Group and its sectorial workstreams. Contribution by ENISA in the European Commission's regular monitoring of the implementation of specific EU policies is envisaged that considers relevant indicators and could result in a contribution being made to a potential index for capturing the maturity of relevant cybersecurity policies.

The activity helps to avoid fragmentation and supports the coherent implementation of the digital single market across Member States.

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

Objectives

- Align horizontal cybersecurity policies with sectorial polices to avoid implementation inconsistencies
- Contribute to the efficient and effective monitoring of EU cybersecurity policy implementation in Member States
- Contribute to the effective implementation of cybersecurity policy across the EU and approximation of Member State laws, regulations and administrative provisions related to cybersecurity
- Improve cybersecurity practices taking on board lesson learned from incident reports

Results	Link to strategic objective (ENISA strategy)
• Consistent implementation of EU policy and law in the area of cybersecurity • EU cybersecurity policy implementation reflects sectorial specificities and needs • Exchange of good practice	• Cybersecurity as an integral part of EU policies • Empowered and engaged communities across the cybersecurity ecosystem
Outputs	**Key performance indicator**
2.1. Support the NIS Cooperation Group (NIS CG) and sectorial workstreams in accordance with the NIS CG work programme **2.2.** Support Member States and the European Commission in the implementation of the 5G security toolbox and its individual actions **2.3.** Recommendations, technical guidelines and other activities to assist with and support the implementation of policies within the NIS directive sectors, in the area of trust services and eID, under the European Electronic Communications Code and its implementing acts, and in the field of privacy and data protection and artificial intelligence **2.4.** Assist in establishing and implementing vulnerability disclosure policies **2.5.** Analyse and report on incidents as required by Article 5(6) of the CSA	**Indicator:** Contribution to policy implementation and implementation monitoring at EU and national levels (ex post) **Metrics:** **2.1.** Number of EU policies and regulations implemented at national level supported by ENISA **2.2.** Number of ENISA reports, analyses and/or studies referred to at EU and national levels (survey) **2.3.** Satisfaction with ENISA added value and weight of support (survey) **Frequency:** Annual (2.1), biennial (2.2 and 2.3)
Validation	**Target groups and beneficiaries**
• Article 13a expert group (for related activities under output 2.3) • Article 19 expert group (for related activities under output 2.3) • NIS Cooperation Group and established sectorial workstreams (outputs 2.1 and 2.2) • NLO Network (as necessary)	• Article 13a expert group, Article 19 expert group • Citizens • Conformity assessment bodies • Data protection authorities • European Commission, EU institutions/bodies (e.g. Body of European Regulators for Electronic Communications (BEREC)) • European Information Sharing and Analysis Centres (ISACs) • Member State cybersecurity authorities (NIS CG members) • Supervisory authorities • Trust service providers

Resources planned	
Human resources (FTEs)	Financial resources (EUR)
Total 14	**Total** 985 000

Activity 3: Building capacity

Overview of activity

This activity seeks to improve and develop the capability of Member States and EU institutions, bodies and agencies, as well as various sectors, to respond to cyberthreats and incidents, raise resilience and increase preparedness across the EU. Actions to support this activity include organising large-scale exercises, sectorial exercises and training, including computer security incidence response team (CSIRT) training. In addition, the activity seeks to develop and increase CSIRT capabilities, support information sharing within the cybersecurity ecosystem and assist in reviewing and developing national and EU-level cybersecurity strategies, including cross-border strategies.

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

Objectives

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

Results	Link to strategic objective (ENISA strategy)
• Enhanced capabilities across the community • Increased cooperation between communities	• Cutting-edge competences and capabilities in cybersecurity across the EU • Empowered and engaged communities across the cybersecurity ecosystem

Outputs	Key performance indicator
3.1. Assist Member States to develop national cybersecurity strategies **3.2.** Organise large-scale biannual exercises and sectorial exercises (including Cyber Europe, BlueOLEx, CyberSOPEx) **3.3.** Organise training and other activities to support and develop the maturity and skills of CSIRTs (including NIS directive sectorial CSIRTs) and other communities **3.4.** Develop coordinated and interoperable risk management frameworks **3.5.** Support the capacity-building activities of the NIS Cooperation Group and sectorial workstreams in accordance with the NIS CG work programme **3.6.** Support the establishment, development and cooperation of European information-sharing schemes based on ISACs, public–private partnerships and other existing mechanisms **3.7.** Organise the European Cyber Security Challenge (ECSC) **3.8.** Report on cybersecurity skill needs and gaps, and support skills development, maintenance and implementation (including the Digital Education Action Plan and a report on higher education programmes)	**Indicator:** Increased resilience against cybersecurity risks and preparedness to respond to cyber incidents **Metrics:** **3.1.** Increase/decrease in maturity indicators **3.2.** Outreach, uptake and application of lessons learned from capability-building activities **3.3.** Number of cybersecurity programmes (courses) and participation rates **3.4.** Stakeholder assessment of the usefulness, added value and relevance of ENISA capacity-building activities (survey) **Frequency:** Annual (3.1, 3.2 and 3.3), biennial (3.4)

Validation	Target groups and beneficiaries
• NLO Network (as necessary) • CSIRTs Network (output 3.3) • NIS Cooperation Group (output 3.6)	• CSIRTs Network • Cybersecurity professionals • EU institutions • European ISACs • Operational communities • Private industry sectors (health, transport, etc.)

Resources planned

Human resources (FTEs)		Financial resources (EUR)	
Total	**15**	**Total**	**1 400 000**

Activity 4: Enabling operational cooperation

Overview of activity

This activity supports operational cooperation among Member States and EU institutions, bodies, offices and agencies and between operational activities. Actions include establishing synergies with national and EU actors, including CERT-EU, with the view to exchange know-how and 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 for ex post technical inquiries regarding incidents.

Under this activity ENISA is supporting operational communities by helping to develop and maintain networks / IT platforms and communication channels.

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

Objectives

- Enhance and improve incident response capabilities across the EU
- Enable effective incident response and cooperation among Member States and EU institutions (including through the Blueprint)
- Improve the maturity and capacities of operational communities (including the CSIRTs Network, CyCLONe group)

Results	Link to strategic objective (ENISA strategy)
• All communities (EU institutions and Member States) use a rationalised set of SOPs • An agreed CSIRTs Network approach for selecting, operating and decommissioning tools • Coherent SOPs for cyber crisis management • Efficient framework, tools and methodologies for effective cyber crisis management	• Effective cooperation among operational actors within the EU in case of massive cyber incidents • Empowered and engaged communities across the cybersecurity ecosystem
Outputs	**Key performance indicator**
4.1. Support the functioning and operations of the CSIRTs Network (including through MeliCERTes) and CyCLONe group and cyber crisis management in the EU **4.2.** Activities to support the development, implementation and evolution of memoranda of understanding (MoUs) between ENISA, Europol, CERT-EU and the European Defence Agency (EDA) **4.3.** Develop SOPs, procedures, methodologies and tools for cyber crisis management	**Indicator:** Effective use of ENISA's tools and platforms and take-up of SOPs in operational cooperation **Metrics:** **4.1.** Number of users, both new and recurring, and usage per platform/tool/SOP provided by ENISA **4.2.** Uptake of platforms/tools/SOPs during massive cyber incidents **4.3.** Stakeholder satisfaction with the relevance and added value of platforms/tools/SOPs provided by ENISA (survey) **Frequency:** Annual (4.1 and 4.2), biennial (4.3)
Validation	**Target groups and beneficiaries**
• Management board (output 4.2) • NLO Network (as necessary) • CSIRTs Network and CyCLONe group (output 4.1)	• Blueprint stakeholders • EU decision-makers, institutions, agencies and bodies • Member State CSIRTs Network members • NIS Cooperation Group • Operators of essential services and digital service providers
Resources planned	
Human resources (FTEs)	Financial resources (EUR)
Total **8**	**Total** **1 110 000**

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

Overview of activity

This activity contributes to developing a cooperative response at EU and Member State levels to large-scale cross-border incidents or crises related to cybersecurity by aggregating and analysing reports to establish a common situational awareness, ensuring information flow and escalation measures between the CISRTs Network and technical, operational and political decision-makers at EU level.

In addition, at the request of Member States, the activity facilitates the handling of incidents or crises, public communication related to such incidents or crises and the testing of cooperation plans for such incidents or crises, as well as supporting EU institutions, bodies, offices and agencies with public communication related to incidents and crises. The activity also supports Member States with respect to operational cooperation within the CSIRTs Network by providing advice on specfic cyberthreats, assisting in the assessment of incidents, faciliting the technical handling of incidents, supporting cross-border information sharing and analysing vulnerabilities. Moreover, the activity seeks to engage with CERT-EU in structured cooperation.

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

Objectives

- Develop an effective incident response and cooperation among Member States and EU institutions, including cooperation between technical and political actors during incidents or crises
- Establish a common awareness of cyber incidents and crises across the EU
- Facilitate information exchange and cooperation, both cross-layer and cross-border, between Member States as well as with EU institutions

Results	**Link to strategic objective (ENISA strategy)**
• Member States and institutions cooperating effectively during large-scale cross-border incidents or crises • Public informed on a regular basis of important cybersecurity developments • Stakeholders aware of the current cybersecurity situation	• Effective operational cooperation within the EU in case of massive cyber incidents • Empowered and engaged communities across the cybersecurity ecosystem
Outputs	**Key performance indicator**
5.1. Generate and consolidate information (including for the general public) on cyber situational awareness, technical situational reports, incident reports and information on threats and support the consolidation and exchange of information at strategic, tactical and technical levels **5.2.** Support technical and operational cooperation, incident response coordination during crises and activities with the CSIRT Network, and CERT-EU, EC3, EEAS and EDA EU-wide crisis communication planning **5.3.** Provide assistance and support on the basis of Article 7(4) and 7(7) of the CSA	**Indicator:** ENISA ability to support the response to massive cyber incidents **Metrics:** **5.1.** Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents that ENISA contributes to mitigation efforts (survey) **5.2.** Stakeholder satisfaction with ENISA's ability to provide operational support (survey) **Frequency:** Biennial (5.1 and 5.2)
Validation	**Target groups and beneficiaries**
• Blueprint actors	• EU Member States (including CSIRTs Network members) • EU institutions, bodies and agencies • Other types of CSIRTs and product security incident response teams (PSIRTs)
Resources planned	
Human resources (FTEs)	Financial resources (EUR)
Total **8**	**Total** **1 200 000**

Activity 6: Development and maintenance of EU cybersecurity certification framework

Overview of activity

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

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

Objectives

- Trusted ICT products, services and processes
- Increased use and uptake of European cybersecurity certification

Results	Link to strategic objective (ENISA strategy)
• Support for schemes chosen to run under the European cybersecurity certification framework • Certified ICT products, services and processes are preferred by consumers and, where relevant, operators of essential services and digital service providers	• High level of trust in secure digital solutions • Empowered and engaged communities across the cybersecurity ecosystem
Outputs	**Key performance indicator**
6.1. Draft candidate cybersecurity certification schemes and contribute to the establishment of the schemes **6.2.** Implementation and maintenance of the established schemes including evaluation of adopted schemes and participation in peer review **6.3.** Support statutory bodies in discharging their duties with respect to governance roles and tasks **6.4.** Development and maintenance of necessary tools for an efficient and effective EU cybersecurity certification framework (including a certification website and collaboration platform)	**Indicators:** **1.** Uptake of the European cybersecurity certification framework and schemes as an enabler for secure digital solutions. **2.** Effective preparation of candidate certification schemes prepared by ENISA **Metric:** **6.1.** Number of stakeholders (governments or commercial solution providers) on the EU market using the cybersecurity certification framework for their digital solutions **6.2.** Citizens' trust in digital solutions (survey) **6.3.** Satisfaction with ENISA's support for the preparation of candidate schemes (survey) **Frequency:** Annual (6.1), biennial (6.2 and 6.3)
Validation	**Target groups and beneficiaries**
• Ad hoc certification expert groups (output 6.1) • European Cybersecurity Certification Group (ECCG) (outputs 6.1 and 6.2) • European Commission (outputs 6.1–6.3) • Stakeholder Cybersecurity Certification Group (SCCG) (outputs 6.3. and 6.4)	• Accreditation bodies at Member State and EU levels, certification supervisory authorities, conformity assessment bodies • European Commission and other institutions, agencies and competent authorities (e.g. European Data Protection Board (EDPB)), public authorities in the Member States, members of the European Cybersecurity Certification Group (ECCG) and Stakeholder Cybersecurity Certification Group (SCCG) • Product manufacturers and service providers who have an interest in EU schemes for the certification of ICT products and services (industry)
Resources planned	
Human resources (FTEs)	Financial resources (EUR)
Total **12**	**Total** **870 000**

Activity 7: Supporting the European cybersecurity market and industry

Overview of activity

This activity seeks to foster the cybersecurity market in the EU and the development of the cybersecurity industry, in particular small and medium-sized enterprises (SMEs) and start-ups, to reduce dependence on bodies outside the EU and to reinforce supply chains inside the EU. It involves actions to promote and implement 'security by design' and 'security by default' measures for ICT products, services and processes, including through standardisation. Actions to support this activity include compiling guidelines and good practices on cybersecurity requirements, facilitating the establishment and take-up of European and international standards for risk management and performance of regular analysis of cybersecurity market trends on both the demand and the supply sides and monitoring, and collecting and identifying dependencies or vulnerabilities used or integrated into ICT products or services.

In addition, this activity supports cybersecurity certification by monitoring developments in standards to be applied in the evaluation of certification schemes and recommending appropriate technical specifications for use in the development of certification schemes where standards are not available.

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

Objectives

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

Results	Link to strategic objective (ENISA strategy)
• Where relevant, contributions towards a more competitive European cybersecurity industry, SMEs and start-ups	• High level of trust in secure digital solutions • Empowered and engaged communities across the cybersecurity ecosystem
Outputs	**Key performance indicator**
7.1. Market analysis of the main trends in the cybersecurity market on both the demand and the supply side **7.2.** Monitoring developments in related areas of standardisation, analysis of standardisation gaps and establishment and take-up of European and international standards for risk management **7.3.** Guidelines and good practices on cybersecurity certification requirements for ICT products, services and processes **7.4.** Monitoring and documenting the dependencies and vulnerabilities of ICT products and services	**Indicator:** Recognition of ENISA's supporting role for participants in the European cybersecurity market **Metrics:** **7.1.** Number of market analyses, guidelines and good practices issued by ENISA **7.2.** Uptake of lessons learned / recommendations from ENISA reports **7.3.** Stakeholder satisfaction with the added value and quality of ENISA's work (survey) **Frequency:** Annual (7.1 and 7.2), biennial (7.3)
Validation	**Target groups and beneficiaries**
• Stakeholder Cybersecurity Certification Group (SCCG) (outputs 7.2 and 7.3) • ENISA Advisory Group (output 7.1) • NLO Network (as necessary)	• European ICT industry, SMEs, start-ups, product manufacturers and service providers • European standardisation organisations (European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC) and ETSI), as well as international and industry standardisation organisations

Resources planned

Human resources (FTEs)		Financial resources (EUR)	
Total	**9**	**Total**	**490 000**

Activity 8: Knowledge on emerging cybersecurity challenges and opportunities

Overview of activity

This activity aims to provide strategic long-term analysis, guidance and advice on emerging technologies (such as in the areas of artifitial intelligence, quantum distributed ledgers, cloud computing, edge computing, software development), cyberthreats and threat landscapes, vulnerabilities and risks, and provide topic-specific as well as general assessments on the expected societal, legal, economic and regulatory impacts, as well as targeted recommendations to Member States and EU institutions, bodies, offices and agencies. The activity also seeks to identify and give advice on research and innovation needs and priorities in the field of cybersecurity, and contribute to strategic agenda setting for cybersecurity research and innovation. To this end, as part of this activity relevant EU programmes will be assessed (e.g. Horizon Europe).

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

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

Objectives

- Identify and understand future cybersecurity challenges and opportunities and assess the interlinks between cybersecurity and relevant disrupting technologies in the current and future digital transformation
- Increase Member States' and the EU's resilience and preparedness in handling future cybersecurity challenges and opportunities
- Increase knowledge and information for specialised cybersecurity communities

Results	Link to strategic objective (ENISA strategy)
• Decisions about cybersecurity are future-proof and take account of the trends, developments and knowledge across the ecosystem • Stakeholders receive relevant and timely information for policymaking and decision-making	• Foresight on emerging and future cybersecurity challenges • Efficient and effective cybersecurity information and knowledge management for Europe • Empowered and engaged communities across the cybersecurity ecosystem
Outputs	**Key performance indicator**
8.1. Identification, collection and analysis of present and emerging challenges (e.g. technological, economic or societal) in cybersecurity (including developing and maintaining a European Cybersecurity Index) **8.2.** Provide targeted as well as general reports, recommendations, analysis and other actions in relation to future cybersecurity scenarios and threat landscapes (incident response landscape mapping for NIS directive sectors). **8.3.** Develop and maintain a portal (information hub), a one-stop shop for organising and making available to the public information on cybersecurity, and establishment of a procedural framework to support knowledge management activities **8.4.** Support EU research and development programmes and activities of European competences centres, including the four EU pilot projects for the European Cybersecurity Competence Centre and Network of National Coordination Centers	**Indicator:** ENISA's ability to contribute to Europe's cyber resilience through the provision of timely and effective information and knowledge **Metrics:** **8.1.** Number of users and frequency of use of a dedicated portal (observatory) **8.2.** Number of recommendations, analyses and challenges identified and analysed **8.3.** Stakeholder satisfaction with the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges and opportunities, including in research (survey) **Frequency:** Annual (8.1 and 8.2), biennial (8.3)
Validation	**Target groups and beneficiaries**
• NLO Network • ENISA Advisory Group (as necessary) • ENISA ad hoc working group (as necessary) • The forthcoming European Cybersecurity Competence Centre and Network of National Coordination Centers	• EU and national decision-making bodies and authorities • European Cybersecurity Competence Centre and Network of National Coordination Centers • General public • Industry, research and academic institutions and bodies

Resources planned

Human resources (FTEs)		Financial resources (EUR)	
Total	**9**	**Total**	**1 155 000**

Activity 9: Outreach and education

Overview of activity

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

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

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

The legal basis for this activity is Articles 10, 12 and 42 of the CSA.

Objectives

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

Results	**Link to strategic objective (ENISA strategy)**
• Greater understanding of cybersecurity risks and practices • Stronger European cybersecurity through higher global resilience	• Empowered and engaged communities across the cybersecurity ecosystem
Outputs	**Key performance indicator**
9.1. Develop an ENISA stakeholder strategy and undertake actions for its implementation **9.2.** Develop an ENISA international strategy and outreach activities **9.3.** Organise the European Cybersecurity Month (ECSM) **9.4.** Organise the International Cybersecurity Challenge **9.5.** Activities to promote and ensure the uptake of information on good cybersecurity practices (including on EU strategies, security by design and privacy by design at EU level, cybersecurity certification schemes) by different target groups.	**Indicator:** Level of awareness of cybersecurity, cyber hygiene and cyber literacy across the EU **Metrics:** **9.1.** Number of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics **9.2.** Level of awareness of cybersecurity across the EU / general public (e.g. EU barometer) **Frequency:** Annual (9.1), biennial (9.2)
Validation	**Target groups and beneficiaries**
• Management board (outputs 9.1 and 9.2) • Stakeholder Cybersecurity Certification Group (SCCG) (for certification-related issues under output 9.5) • NLO Network • ENISA Advisory Group (outputs 9.1 and 9.5)	• International partners • Member States and EU institutions, bodies and agencies • Public, businesses and organisations
Resources planned	
Human resources (FTEs)	Financial resources (EUR)
Total 6	**Total** 1 010 000

3.2. CORPORATE ACTIVITIES

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

Activity 10: Performance and risk management

Overview of activity

This activity seeks to achieve requirements set out in Article 4(1) of the CSA that set 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 hand in hand with the imposition of the new organisational set-up.

Under this activity ENISA will continue to enhance key objectives of the reorganisation, as described in management board decision 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 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. The actions undertaken will ensure that the Agency's outputs add real value, by making performance and ex post and ex ante evaluation integral to the work programme througout its lifecycle, including through rigorous quality assurance by carrying out proper project management, internal peer review and independent audits and validations.

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

Objectives

- For the performance of ENISA to be fully compliant with legal and financial frameworks (build a culture of compliance)
- Increased effectiveness and efficiency in achieving the Agency's objectives
- Protect the Agency's assets and reputation, while reducing risks

Results	Link to strategic objective (ENISA strategy)
• Maximise value for money provided to stakeholders and citizens • Build lasting credibility and trust	Sound resource and risk management
Outputs	**Key performance indicator**
10.1. Roll-out of an Agency-wide performance management framework and systems across its functions **10.2.** Develop, establish and implement a risk management plan and systems, including an anti-fraud strategy, a conflict of interest policy, a whistleblowing policy, an information security policy, an anti-harassment policy and an intellectual property rights (IPR) policy **10.3.** Develop and implement an Agency-wide IT strategy **10.4.** Carry out relevant training and develop guidelines for staff	**Indicator:** Organisational performance culture **Metrics:** **10.1.** Proportion of key performance indicators reaching targets **10.2.** Individual contributions to achieving the objectives of the Agency through clear links to key performance indicators (CDR report) **10.3.** Exceptions in the risk register **10.4.** Number of complaints filed against ENISA, including number of inquiries/complaints submitted to the European Ombudsman **10.5.** Results of the annual risk assessment exercise **10.6.** Observations from external audit bodies (e.g. ECoA) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings) **Frequency:** Annual
Validation	**Target groups and beneficiaries**
• Budget management committee • ENISA ethics committee • IPR management committee • IT management committee • Management team • Staff committee	• All stakeholders of the Agency • Citizens

Activity 11: Staff development and working environment

Overview of activity

This activity seeks to support ENISA aspirations as stipulated in Article 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'.

Moreover, since the start of the COVID-19 pandemic, the number of organisations that have announced permanent teleworking options has grown globally. This must accelerate a review of employer–employee relationships in the Agency, with a view to introducing a more flexible (50/50) framework while maintaining and enhancing employee motivation, efficiency and development, an option that was supported by 87 % of respondents to the staff survey conducted in June 2020.

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

Objectives

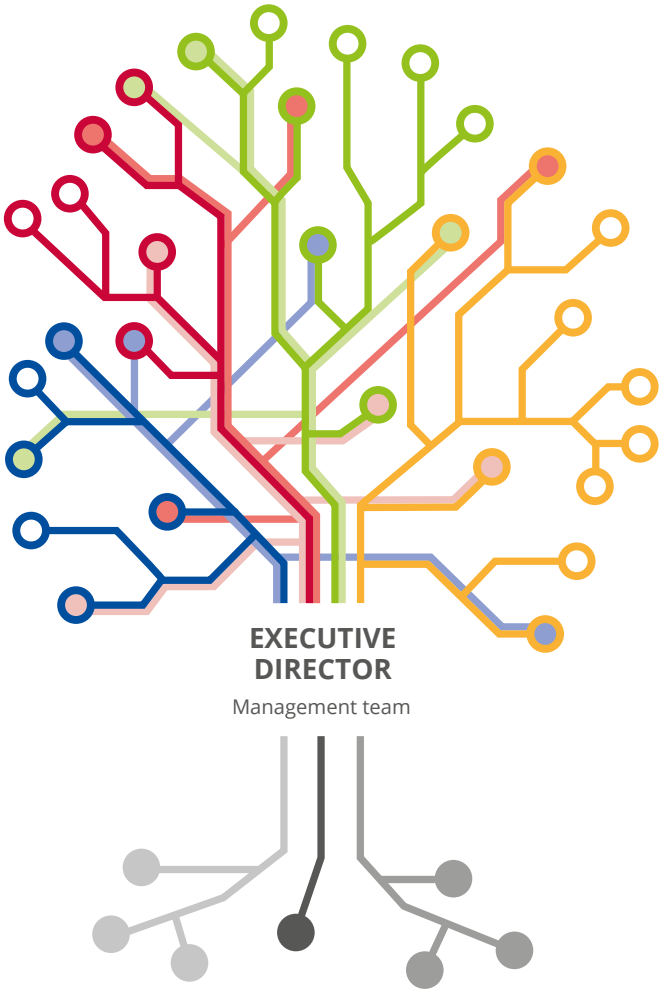
- Engaged staff who are committed and motivated to deliver and who are empowered to use fully their talents, skills and competences
- Digitally enabled workplace and environment (including home workspace) that cultivates and nourishes performance and enhances social and environmental responsibility

Results	**Link to strategic objective (ENISA strategy)**
ENISA as an employer of choice	Build an agile organisation focused on people
Outputs	**Key performance indicator**
11.1. Implementation of the competence framework (including the training strategy, CDR report, internal competitions, exit interviews) **11.2.** Actions to develop and nourish talent (in line with output 11.1) **11.3.** Undertake actions to support a digital working environment and develop necessary tools and services in line with objective 10.3 **11.4.** Planning and preparation and completion of the establishment of the Agency's headquarters to its new premises in line with the objectives of the activity	**Indicator:** Staff commitment, motivation and satisfaction **Metrics:** **11.1.** Staff satisfaction survey (including the attractiveness of ENISA as an employer, staff empowerment, organisational culture, opportunities for internal mobility, workspace, work environment and work tools) **11.2.** Quality of ENISA training and career development activities organised for staff **11.3.** Reasons for staff departure (exit interviews) **11.4.** Staff retention/turnover rates **11.5.** Resilience and quality of ENISA IT systems and services **Frequency:** Annual (or ad hoc for 11.3)
Validation	**Target groups and beneficiaries**
• Management team • Joint reclassification committee • IT management committee • Task force on relocation of the Agency • Staff committee	• ENISA staff members and employees

A

ANNEX 1

ORGANISATION CHART AS OF 1 JANUARY 2021



POLICY DEVELOPMENT AND IMPLEMENTATION UNIT

MARKET, CERTIFICATION AND STANDARDISATION UNIT

CAPACITY BUILDING UNIT

OPERATIONAL COOPERATION UNIT

- Research & Innovation team
- Awareness & Education team
- Knowledge & Information team
- International Cooperation team

ACCOUNTANT

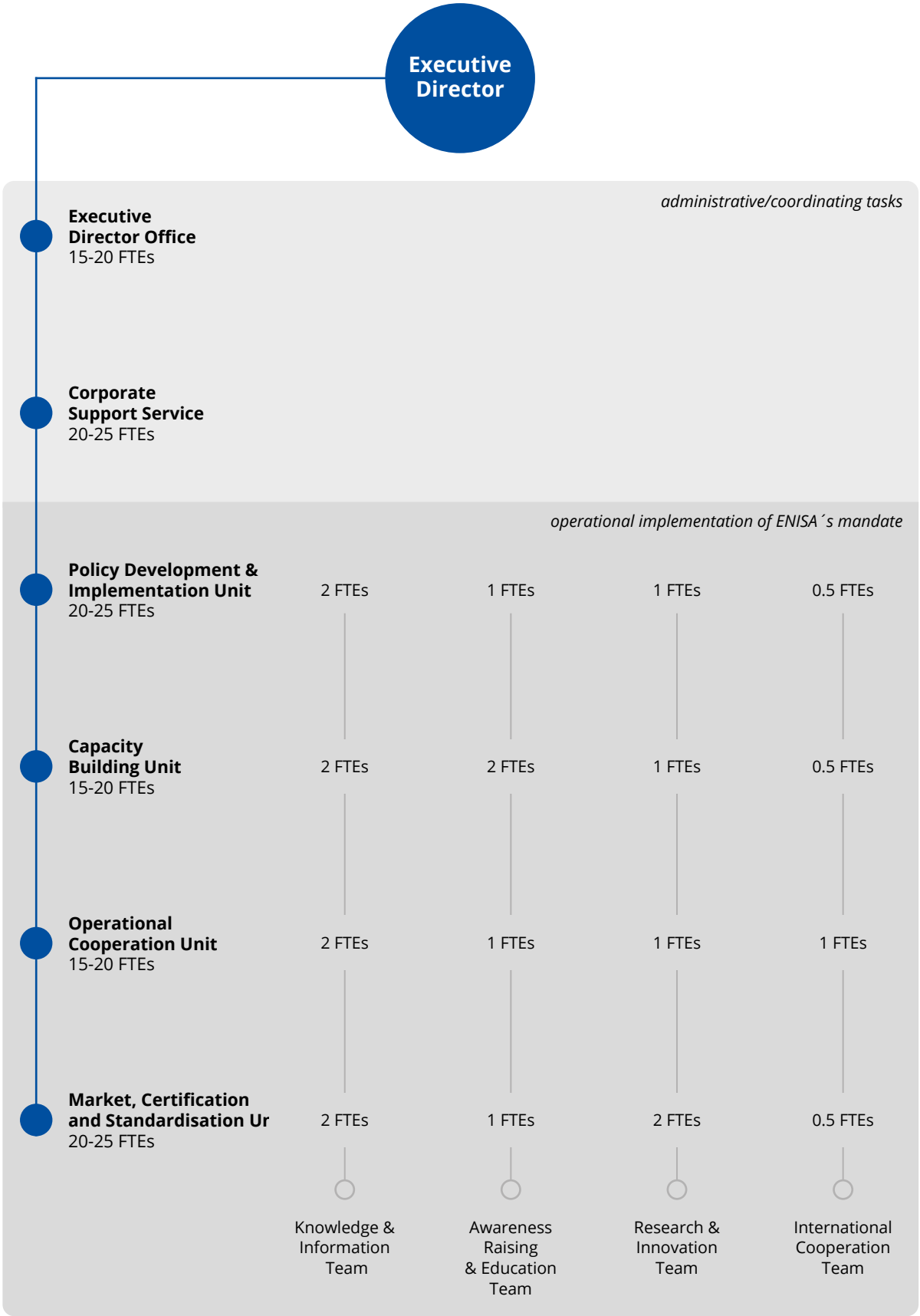
EXECUTIVE DIRECTOR'S OFFICE

Communication
Coordination
Internal Control & Compliance
Administration

CORPORATE SUPPORT SERVICES

Human Resources
Finance
Procurement
IT services

Administrative Organigramme



* ENISA establishement plan for 2021 foresees 118 FTEs. Exact number of FTEs per unit will be determined on the basis of the WP2021
** Organigramme shows the minimum number of FTEs the Units would be required to reserve for the performance of the tasks of the Teams

ANNEX 2
RESOURCE ALLOCATION PER ACTIVITY 2021–2023

The allocation of financial and human resources for 2021 for the operational and corporate activities described in Section III is presented in table 5 below. The allocation was determined according to the direct budget and number of full-time equivalents (FTEs) indicated for each activity, with the indirect budget being assigned based on causal relationships.

The following assumptions are used in the simplified activity-based budgeting methodology.

- The direct budget is the cost estimate for each of the nine operational activities described in Section III (and carried out under Articles 5–12) in terms of goods and services to be procured.
- The indirect budget is the cost estimate for salaries and allowances, mission costs, buildings, IT, equipment and miscellaneous operating costs attributable to each activity. The indirect budget is allocated to activities based on different drivers. The main driver for cost allocation was the estimated number of FTEs required for each operational activity in 2021.
- For the purpose of the allocation of human and financial resources, an Executive Director's Office activity (budget and FTEs), which includes coordination, compliance, communication and administration executed by 15 FTEs, was allocated for all of the Agency's activities.
- For the purpose of the allocation of human and financial resources, Corporate Support Service activity, including human resources, IT services, procurement and finance, facilities and logistics activity, was created.

Table 5.

		2021	
Allocation of human and financial resources	**Activity as described in Section 3.1**	**Full budget allocation (EUR)**	**Full FTE allocation**
Providing assistance on policy development	Activity 1	1 309 867.31	8.14
Supporting implementation of Union policy and law	Activity 2	3 388 023.72	18.99
Building capacity	Activity 3	3 974 668.28	20.34
Enabling operational cooperation	Activity 4	2 483 156.41	10.85
Contribute to cooperative response at Union and Member States level	Activity 5	2 573 156.41	10.85
Development and maintenance of EU cybersecurity certification framework	Activity 6	2 929 734.62	16.28
Supporting the European cybersecurity market and industry	Activity 7	2 034 800.97	12.21
Knowledge on emerging cybersecurity challenges and opportunities	Activity 8	2 699 800.97	12.21
Outreach and education	Activity 9	2 039 867.31	8.14
Total		**23 433 076.00**	**118.00**

	2022		2023	
	Full budget allocation (EUR)	Full FTE allocation	Full budget allocation (EUR)	Full FTE allocation
	1 636 062.06	8.96	1 636 062.06	8.96
	3 874 144.81	20.91	3 874 144.81	20.91
	5 015 155.16	22.41	5 015 155.16	22.41
	1 555 051.72	7.47	1 555 051.72	7.47
	2 414 093.09	13.44	2 414 093.09	13.44
	3 572 124.13	17.93	3 572 124.13	17.93
	1 908 187.71	8.96	1 908 187.71	8.96
	2 137 072.41	10.46	2 137 072.41	10.46
	2 115 172.41	10.46	2 115 172.41	10.46
	24 227 063.50	**121.00**	**24 227 063.50**	**121.00**

ANNEX 3
FINANCIAL RESOURCES 2021–2023

(Tables 6–8 as well as budget allocation per activity areas depend on the new Multiannual Financial Framework which is not yet adopted therefore changes might apply after MFF is adopted and internal needs clarified)

Table 6. Revenue

Revenues	Revenue estimated by the Agency	
	2020*	2021
EU contribution	20 646 000	22 248 000
Other revenue	1 036 884	1 185 076
Total revenue	**21 682 884**	**23 433 076**

* As adopted in the amending budget 1/2020 (management board decision MB/2020/18).

Table 7.

Revenue	2019 executed budget	2020 revenue estimated by the Agency*	2021 revenue as requested by the Agency	Variance 2021/2020	Envisaged 2022	Envisaged 2023
1. Revenue from fees and charges						
2. EU contribution	15 400 829	20 646 000	22 248 000	8 %	23 023 000	23 023 000
– of which assigned revenue deriving from previous years' surpluses**	–85 534.89	–110 505.47	–579 112.99	524 %		
3. Third countries contribution (including European Economic Area (EEA)/EFTA and candidate countries)	370 696	503 120	545 076	8 %	564 064	564 064
– of which EEA/EFTA (excluding Switzerland)	370 696	503 120	545 076	8 %	564 064	564 064
– of which candidate countries						
4. Other contributions	435 844	533 764	640 000	0 %	640 000	640 000
5. Administrative operations						
– of which interest generated by funds paid by the Commission by way of EU contributions (Framework Financial Regulation Article 58)						
6. Revenues from services rendered against payment						
7. Correction of budgetary imbalances						
Total revenue	**16 207 370**	**21 682 884**	**23 433 076**	**8 %**	**24 227 064**	**24 227 064**

* As adopted in the amending budget 1/2020 (management board decision MB/2020/18).
** The 2019 surplus (as indicated under column '2021 revenue as requested by the agency) has increased by more than five times the value of the previous year (+524 %), which can partially be explained by the late adoption in June 2019 of ENISA's new mandate (the CSA), resulting in a delay to the 2019 implementation of deliverables, which had a negative impact on the 2020 budget because of a domino effect. Furthermore, with its renewed mandate, ENISA was given greater competences but also greater financial resources, increasing its budget by almost a factor of two in less than 3 years.

Table 8. For ENISA to review again

Expenditure (EUR)	2020*		2021	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1	11 203 334	11 203 334	10 775 409	10 775 409
Title 2	3 150 568	3 150 568	3 507 667	3 507 667
Title 3	7 328 981	7 328 981	9 150 000	9 150 000
Total expenditure	**21 682 884**	**21 682 884**	**23 433 076**	**23 433 076**

* As adopted in the amending budget 1/2020 (management board decision MB/2020/18).

Table 9.

Expenditure (EUR)	Commitment and payment appropriations*					
	2019 executed budget	2020 budget**	2021 budget as requested by the Agency	VAR 2021/2020	Envisaged 2022	Envisaged 2023
Title 1. Staff expenditure	**7 458 310**	**11 203 334**	**10 775 409**	**–4 %**	**11 245 821**	**11 245 821**
11 Staff in active employment	5 627 276	7 126 084	8 810 319	24 %	9 107 970	9 107 970
12 Recruitment expenditure	254 762	704 686	410 087	–42 %	423 982	423 982
13 Socio-medical services and training	222 200	375 738	1 084 064	189 %	1 120 796	1 120 796
14 Temporary assistance	1 354 073	2 996 826	470 939	–84 %	593 073	593 073
Title 2. Building, equipment and miscellaneous expenditure	**4 346 742**	**3 150 568**	**3 507 667**	**11 %**	**3 013 739**	**3 013 739**
20 Building and associated costs	783 366	929 820	1 364 624	47 %	1 867 710	1 867 710
21 Movable property and associated costs	45 391	54 074	99 000	83 %	151 981	151 981
22 Current corporate expenditure	81 829	98 702	798 696	709 %	129 235	129 235
23 ICT	3 436 156	2 067 972	1 245 347	–40 %	864 813	864 813
Title 3. Operational expenditure	**4 402 318**	**7 328 981**	**9 150 000**	**25 %**	**9 967 504**	**9 967 504**
30 Activities related to meetings and missions	910 929	628 966	650 000	3 %	51 694	51 694
32 Horizontal operational activities	524 689	1 517 962	0	–100 %	992 528	992 528
36/37 Core operational activities	2 966 700	5 182 053	8 500 000	64 %	8 923 282	8 923 282
Total expenditure	**16 207 370**	**21 682 884**	**23 433 076**	**8 %**	**24 227 064**	**24 227 064**

* ENISA operates with non-differential appropriations; therefore, commitment appropriations equal payment appropriations.
** As adopted in the amending budget 1/2020 (management board decision MB/2020/18).

Table 10. Budget out-turn and cancellation of appropriations

Budget out-turn (EUR)	2017	2018	2019
Revenue actually received (+)	11 223 387	11 572 995	16 740 086
Payments made (–)	–9 901 545	–10 345 736	–11 980 352
Carry-over of appropriations (–)	–1 376 730	–1 348 657	–4 357 734
Cancellation of appropriations carried over (+)	90 916	108 302	62 522
Adjustment for carry-over of assigned revenue appropriations carried over (+)	49 519	124 290	116 393
Exchange rate difference (+/–)	–12	–689	–1 802
Adjustment for negative balance from previous year (–)	–	–	–
Total	**85 535**	**110 505**	**579 113**

* As adopted in the amending budget 1/2020 (management board decision MB/2020/18).

CANCELLATION OF APPROPRIATIONS

- Cancellation of commitment appropriations. In 2019 commitment appropriations were cancelled for an amount of EUR 521 426, representing 3 % of the total budget. ENISA demonstrated a commitment rate of 97 % of C1 appropriations (appropriations for the respective year) at the year-end (31 December 2019). The consumption of the 2019 budget at year-end shows the capacity of the Agency to fully implement its annual appropriations. The payment rate reached 70 % and the amount carried forward to 2020 was EUR 4 347 332, representing 27 % of the total C1 appropriations in 2019.
- Cancellation of payment appropriations for the year. No payment appropriations were cancelled during 2019.
- Cancellation of payment appropriations carried over (fund source C8 – appropriations carried over automatically from 2018 to 2019). The appropriations for 2018 carried over to 2019 were utilised at a rate of 95 % (automatic carry-overs), which indicates a satisfactory estimation of needs. Of the EUR 1 232 263 carried forward, an amount of EUR 62 522 was cancelled because the estimated expenditure deviated from the actual paid amount. This cancellation represents 0.4 % of the total budget for 2019.

ANNEX 4
HUMAN RESOURCES – QUANTITATIVE

Overview of all categories of staff and their development: staff policy plan for 2021–2023

Table 11. Staff population and development: overview of all categories

Statutory staff and seconded national experts

Staff	2019			2020	2021	2022	2023
Establishment plan posts	**Authorised budget**	**Actually filled as of 31 December 2019**	**Occupancy rate (%)**	**Authorised staff**	**Envisaged staff**	**Envisaged staff**	**Envisaged staff**
Administrators (ADs)	43	37	86	51	57	60	60
Assistants (ASTs)	16	14	88	18	19	19	19
Assistants/ secretaries (ASTs/SCs)							
Total establishment plan posts	59	51	87	69	76	79	79
External staff	**FTEs corresponding to the authorised budget**	**Executed FTEs as of 31 December 2019**	**Execution rate (%)**	**Headcount as of 31 December 2020**	**FTEs corresponding to the authorised budget**	**Envisaged FTEs**	**Envisaged FTEs**
Contract agents	30	26	87	26	30	30	30
Seconded national experts	9	4	44	4	12	12	12
Total external staff	5	12	100	12	5	5	5
Total	44	42	95	42	47	47	47
Total staff (excludinig external staff)	**103**	**93**	**90**	**111**	**118**	**121**	**121**

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

Table 12.

Human resources	2020	2021	2022	2023
	Envisaged FTEs	Envisaged FTEs	Envisaged FTEs	Envisaged FTEs
Contract agents	n/a	n/a	n/a	n/a
Seconded national experts	n/a	n/a	n/a	n/a
Total	**n/a**	**n/a**	**n/a**	**n/a**

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

Table 13. Other human resources

Structural service providers.

	Actually in place as of 31 December 2019
Security	4
IT	

Interim workers.

	Actually in place as of 31 December 2019
Number	30

Table 14. Multiannual staff policy plan for 2019, 2020, 2021, 2022 and 2023

Function group and grade	2019				2020		2021		2022		2023	
	Authorised budget		Actually filled as of 31 December 2019		Authorised budget		Envisaged		Envisaged		Envisaged	
	PP	TP	PP	TP	PP	TP	PP	TP	PP	TP	PP	TP
AD 16												
AD 15		1				1		1		1		1
AD 14				1								
AD 13								1		2		2
AD 12		6		6		6		5		4		4
AD 11								2		2		2
AD 10		5		3		5		3		4		4
AD 9		12		4		12		12		11		11
AD8		19		10		21		21		22		22
AD 7				6		3		8		8		8
AD 6				6		3		4		6		6
AD 5				1								
AD total		**43**		**37**		**51**		**57**		**60**		**60**
AST 11												
AST 10												
AST 9												
AST 8								1		2		2
AST 7		3		2		4		4		3		3
AST 6		7		2		8		8		8		8
AST 5		5		4		5		5		5		5
AST 4		1		4		1		1		1		1
AST 3				1								
AST 2				1								
AST 1												
AST total		**16**		**14**		**18**		**19**		**19**		**19**
AST/SC 6												
AST/SC 5												
AST/SC 4												
AST/SC 3												
AST/SC 2												
AST/SC 1												
AST/SC total												
Total		**59**		**51**		**69**		**76**		**79**		**79**
Overall total	**59**		**51**		**69**		**76**		**79**		**79**	

PP: Permanent Posts, TP: Temporary posts

Table 15. External personnel

Contract agents

Contract agents	FTEs corresponding to the authorised budget 2019	Executed FTEs as of 31 December 2019	Headcount as of 31 December 2019	FTEs corresponding to the authorised budget 2020	FTEs corresponding to the authorised budget 2021	FTEs corresponding to the authorised budget 2022	FTEs corresponding to the authorised budget 2023
Function group IV	28	17	17	28	28	28	28
Function group III	2	8	8	2	2	2	2
Function group II	0	0	0	0	0	0	0
Function group I	0	1	1	0	0	0	0
Total	**30**	**26**	**26**	**30**	**30**	**30**	**30**

Seconded national experts

Seconded national experts	FTEs corresponding to the authorised budget 2019	Executed FTEs as of 31 December 2019	Headcount as of 31 December 2019	FTEs corresponding to the authorised budget 2020	FTEs corresponding to the authorised budget 2021	FTEs corresponding to the authorised budget 2022	FTEs corresponding to the authorised budget 2023
Total	**9**	**4**	**4**	**12**	**12**	**12**	**12**

Table 16. Recruitment forecasts for 2021 following retirement/mobility or new requested posts (indicative table)

Job title in the agency	Type of contract (official, temporary agent or contract agent)		Temporary agents/officials		Contract agents
	Due to foreseen retirement/ mobility	New post requested because of additional tasks	Internal (brackets)	External (brackets)	Recruitment function group (I, II, III and IV)
Safety, security and facilities officer	Retirement in 2021	n/a	n/a	n/a	n/a
Experts		6 AD posts	n/a	n/a	n/a
Assistant		1 AST post	n/a	n/a	n/a

ANNEX 5
HUMAN RESOURCES – QUALITATIVE

A. RECRUITMENT POLICY

Implementing rules in place.

		Yes	No	If no, which other implementing rules are in place
Engagement of contract agents	Model decision C(2019)3016	x		
Engagement of temporary agents	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 temporary agents	Model decision C(2015)9560	x		
Reclassification of contract agents	Model decision C(2015)9561	x		

Table 17. Reclassification of temporary agents/promotion of officials

Average seniority for each grade among reclassified staff

Grades	2016	2017	2018	2019	2020	Actual average over 5 years	Average over 5 years according to decision C(2015)9563
AD05	–	–	–	–	–	–	2.8
AD06	1	1	2	3	-	3.7	2.8
AD07	1	–	–	–	–	4	2.8
AD08	1	–	1	1	–	5.7	3
AD09	–	–	–	1	–	10	4
AD10	–	–	–	–	–	–	4
AD11	–	1	–	–	–	3	4
AD12	–	–	–	–	–	–	6.7
AD13	–	–	–	–	–	–	6.7
AST1	–	–	–	–	–	–	3
AST2	–	–	–	–	–	–	3
AST3	2	1	1	1	–	4.4	3
AST4	–	1	1	1	–	5.6	3
AST5	1	–	1	–	–	5.5	4
AST6	1	–	–	–	–	4	4
AST7	–	–	–	–	–	–	4
AST8	–	–	–	–	–	–	4
AST9	–	–	–	–	–	–	n/a
AST10 (senior assistant)	–	–	–	–	–	–	5
There are no AST/SCs at ENISA: n/a							
AST/SC1							4
AST/SC2							5
AST/SC3							5.9
AST/SC4							6.7
AST/SC5							8.3

Table 18. Reclassification of contract staff

Contract agents	Grade	Staff activity as of 1 January 2018	Staff members reclassified in 2019	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
Function group IV	17	–	–	–	Between 6 and 10 years
	16	1	–	–	Between 5 and 7 years
	15	1	–	–	Between 4 and 6 years
	14	11	–	–	Between 3 and 5 years
	13	3	–	–	Between 3 and 5 years
Function group III	11	1	–	–	Between 6 and 10 years
	10	2	–	–	Between 5 and 7 years
	9	7	3	5.7	Between 4 and 6 years
	8	2	1	4.8	Between 3 and 5 years
Function group II	6	–	–	–	Between 6 and 10 years
	5	–	–	–	Between 5 and 7 years
	4	–	–	–	Between 3 and 5 years
Function group I	3	1	–	–	n/a
	2	–	–	–	Between 6 and 10 years
	1	–	–	–	Between 3 and 5 years

C. GENDER REPRESENTATION

Table 19. Data as of 31 December 2019 for statutory staff only (officials, temporary agents and contract agents)

		Officials		Temporary agents		Contract agents		Total	
		Number	%	Number	%	Number	%	Number	%
Female	Administrator level	–	–	10	–	15	–	–	–
	Assistant level (AST and AST/SC)	–	–	8	–	–	–	–	–
	Total	–	–	18	54.5	15	45.5	33	45
Male	Administrator level	–	–	24	–	11	–	–	–
	Assistant level (AST and AST/SC)	–	–	5	–	–	–	–	–
	Total	–	–	29	72.5	11	27.5	40	55
Overall total		**–**	**–**	**47**	**64**	**26**	**36**	**73**	**100**

Table 20. Data on gender ratios in 2015 and 2019 for middle and senior management

	2015		2019	
	Number	%	Number	%
Female managers	0	0	2	20
Male managers	10	100	8	80

The focus of the Agency on cybersecurity may be one reason for the gender imbalance in management in the Agency. Nevertheless, an improvement has been noted over the past 5 years. Continuous efforts to encourage female involvement in this area have been successful; however, further efforts should be made in order to achieve a higher percentage of female middle and senior managers at ENISA in the coming years.

D. GEOGRAPHICAL BALANCE

Table 21. Data as of 31 December 2019 for statutory staff only (officials, temporary agents and contract agents)

Nationality	AD and CA FG IV		AST/SC, AST and CA FG I/CA FG II/CA FG III		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	3	6	2	8	5	6.8
BG	2	4	–	–	2	2.7
CY	–	–	1	4	1	1.4
CZ	1	2	–	–	1	1.4
DE	1	2	–	–	1	1.4
Double*	4	8	3	12.5	7	9.6
EE	1	2	–	–	1	1.4
ES	2	4	1	4	3	4.1
FR	3	6	1	4	4	5.5
GR	19	38.8	10	41	29	39.7
IT	2	4	–	–	2	2.7
LT	–	–	1	4	1	1.4
LV	2	4	–	–	2	2.7
NL	2	4	–	–	2	2.7
PL	1	2	1	4	2	2.7
PT	3	6	1	4	4	5.5
RO	2	4	2	8	4	5.5
SE	1	2	–	–	1	1.4
SK	–	–	1	4	1	1.4
Total	**49**	**67.1**	**24**	**32.9**	**73**	**100**

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

Table 22. Growth over 5 years of the most represented nationality in the Agency

Most represented nationality	2015		2019	
	Number	%	Number	%
Greek	18 (out of 63)	28.6	29 (out of 73)	39.7

The imbalance in the most represented nationality at ENISA is related to several factors, such as the level of posts and related salaries, which may be perceived as less appealing for job seekers from relatively more advanced Member State economies; the fact that ENISA is considered to offer better working conditions than the average conditions offered in the Greek job market; the small job market in Greece for cybersecurity professionals; and historical decisions taken by previous appointing authority powers delegated to the Executive Director (AIPNs). Other reasons that may be cited are the need for stability during the start-up phase of the Agency, with staff members from the hosting Member State (Greece) being less likely to resign (resulting in lower turnover), which, because of the relatively young age of the Agency, is still having an impact; the relatively better academic profile of Greek candidates applying for lower level posts; the relatively smaller payroll cost for Greek staff who are better qualified than average and who do not require an expatriation allowance; and the general tendency for people to remain in lower level positions in the home country.

E. SCHOOLING

Agreement in place with the European School of Heraklion	
Contribution agreements signed with the European Commission on type I European schools	No
Contribution agreements signed with the European Commission on type II European schools	Yes
Number of service contracts in place with international schools	For the school year 2019–2020, 12 service-level agreements are in place

ANNEX 6
ENVIRONMENT MANAGEMENT

While ENISA has not yet adopted a formal environment management policy, it has nevertheless implemented several greening measures such as the recycling of office materials, a reduction in electricity usage for lighting and heating/cooling, the use of videoconferencing equipment instead of physical meetings involving travel, the use of teleworking, the provision of bicycle racks to promote the use of public transport, and implementing green public procurement.

All of these measures were taken within the scope of the agency's activities and to the extent possible given its infrastructure and location.

ENISA presently occupies part of a leased building in Athens. This unfortunately does not allow the Agency to control the heating/cooling system or to access autonomous electricity meters. The Agency is therefore unable to directly monitor these systems and assess the impact of the greening measures implemented.

Therefore, ENISA has not been able to obtain Eco-Management and Audit Scheme (EMAS) certification for its main office building considering the leasing restrictions. However, it is envisaged that this certification will be obtained for the new premises to be provided by the Hellenic Authorities. In anticipation of this, the Agency plans to conduct an environmental audit of its activities, as well as pursue options to offset its carbon emissions (including those produced through its missions).

ANNEX 7
BUILDING POLICY

As in the existing Seat Agreement between ENISA and the Greek government, which entered into force on 4 October 2019, the Agency will continue to have premises in Athens and Heraklion. The permanent seat of the Agency is in Athens, where the majority of its staff are based, with a support office located in Heraklion.

At the time of this document the ENISA premises in Athens are privately owned and rented by the Agency; in Heraklion the ENISA premises are located in a public building made available by the Hellenic Authorities. The rent for the premises in Athens and Heraklion is covered by the Hellenic Authorities, who provide up to EUR 640 000 per year.

The current building in Athens will not be able to accommodate all of the new staff who will be joining the Agency in light of the new mandate, with an additional challenge being that the current rental contract expires on 31 December 2021 with no possibility of extension. ENISA has asked the Hellenic Authorities to find suitable premises to accommodate the Agency in Athens. The Ministry of Digital Governance, representing the Hellenic Authorities, is in charge of this dossier and has expressed a commitment to find adequate long-term premises for the Agency. The selection of the new premises in Athens will need to be completed by Q3 2020 to allow a smooth transition.

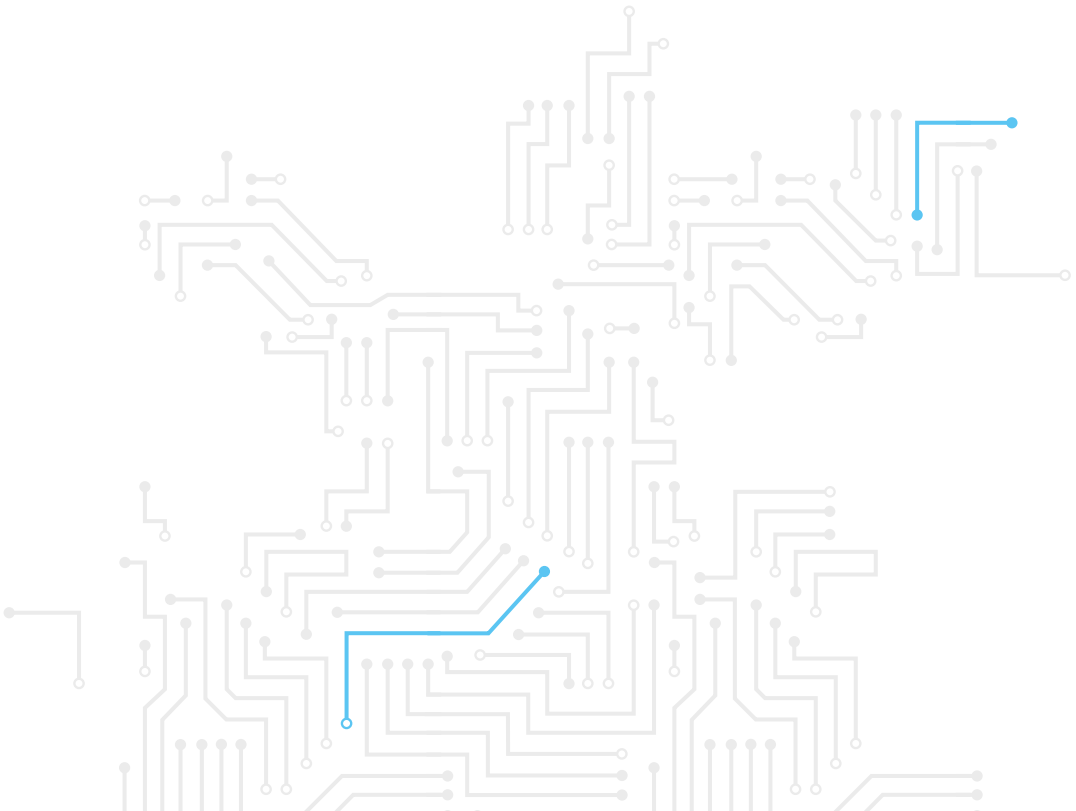
ANNEX 8
PRIVILEGES AND IMMUNITIES

Agency privileges	Privileges granted to staff	
	Protocol of privileges and immunities/ diplomatic status	Education/day care
In accordance with Article 23 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019, protocol no 7 on the privileges and immunities of the European Union, annexed to the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU), applies to the Agency and its staff. The Greek government and ENISA signed a Seat Agreement on 13 November 2018, which was ratified by Greek Law 4627/2019 on 25 September 2019 and entered into force on 4 October 2019 and is applicable to ENISA and its staff.	In accordance with Article 35 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019, the protocol no 7 on the privileges and immunities of the European Union, annexed to the TEU and the TFEU, applies to the Agency and its staff. The Greek government and ENISA signed a Seat Agreement on 13 November 2018, which was ratified by Greek Law 4627/2019 on 25 September 2019 and entered into force on 4 October 2019 and is applicable to ENISA and its staff.	A public school of European education of type 2 was founded in 2005 by the Greek government in Heraklion, Crete, for the children of the staff of ENISA. There is no European school operating in Athens.

ANNEX 9
EVALUATIONS

External consultants are contracted to carry out annual ex post evaluations of operational activities. The overall aim of the annual evaluations is to evaluate effectiveness, efficiency, added value, utility, coordination and coherence.

ENISA uses an internal monitoring system that is intended to support the project management function, which includes project delivery and allocation of resources. This is used for regular reporting and managerial purposes by the ENISA management team. Moreover, ENISA has implemented a mid-term review procedure and regular monthly management team meetings. ENISA expects to undertake a study to upgrade the use of an electronic tool for internal project management and overall delivery of the Agency's work programme.



ANNEX 10

STRATEGY FOR ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS

The Agency's strategy for effective internal control is based on best international practices and on the internal control framework (COSO framework's international standards).

The control environment is a set of standards for conduct, processes and structures that provides the basis for effective internal control across ENISA. The management team sets the tone at the top with respect to the importance of internal control, including expected standards of conduct.

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

The control activities ensure the mitigation of risks related to the achievement of policy, operational and internal control objectives. They are performed at all levels of the organisation, at various stages of business processes and across the technology environment. They may be preventative 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 respect external and internal communication need to be considered. External communication provides the specific Agency stakeholders and, globally, EU citizens with information on ENISA's policies, objectives, actions and achievements. Internal communication provides ENISA staff with the information required to support the achievement of objectives and to enable awareness for day-to-day controls.

Continuous and specific assessments are used to ascertain whether or not 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 their success. In order to implement this approach, the European Anti-Fraud Office (OLAF) has recommended that each agency should adopt an anti-fraud strategy that is proportionate to its fraud risks. Rules for the prevention and management of conflicts of interests are part of the anti-fraud strategy of the Agency.

ANNEX 11

GRANTS, CONTRIBUTIONS AND SERVICE-LEVEL AGREEMENTS

ENISA does not receive any form of grants.

As part of the host country agreement an annual contribution is received from the Hellenic Authorities to cover leasing expenditures for the Agency's offices (as per the Seat Agreement – Greek Law 4627/2019). The 2019 contribution was EUR 435 844.

ENISA has signed a service-level agreement (SLA) with EU-LISA, an EU agency, for the purposes of sharing its knowledge and resources related to the organisation of EU-LISA's security exercises in 2019 and 2020, as well as making available its online exercise platform. The income generated amounts to EUR 97 920 per year to cover staff costs and overheads (two FTEs, equivalent to contract agent posts, are allocated to these tasks). The amounts established in the agreement are based on a cost recovery policy, rather than on generating any additional financial value for the parties involved.

The table below provides a summary of the SLAs and agreements of the Agency, including the contracted amounts where necessary.

Table 23.

Title	Type	Contractor	Contracted amount (EUR)
SLA with EU-LISA – cyber exercise (new)	SLA	EU-LISA	
SLA with Cedefop	SLA	Cedefop	
10th amendment of the SLA with CERT-EU-001-00	SLA	European Commission	24 000.00
SLA and service delivery agreement with the Directorate-General for Budget and usage of the ABAC system	SLA	DG BUDG	
SLA for the 'issuance process of the laissez-passer' with the European Commission	SLA	European Commission	
Collaboration between the Directorate-General for Human Resources and ENISA – SYSPER services	SLA	DG HR	
SLA with the Directorate-General for HR	SLA	DG HR	
Global SLA with the Directorate-General for Informatic	SLA	European Commission	
SLA with the Office for Official Publications of the European Communities	SLA	Office for OPEC	
SLA for the ABAC system with the Directorate-General for Budget	SLA	DG BUDG	
SLA with the European Administrative School	SLA	EAS	
Agreement for provision of ICCA services with BEREC	SLA	BEREC Office	15 000.00
SLA for provision of electronic data back-up services with BEREC	SLA	BEREC Office	
SLA with EASA – Permanent Secretariat	SLA	European Aviation Safety Agency (EASA)	
SLA for European Union Agencies Network (EUAN) shared support office (SSO)	SLA	European Food Safety Authority (EFSA)	2 459.00
SLA with Veritas School	SLA	Veritas Educatio – Educação E Serviços, SA	
SLA with Leonteios School	SLA	Leonteio Lykeio Patision AEE	
SLA with American Community Schools of Athens	SLA	ACS Athens Inc.	
SLA with Douka School	SLA	Douka Ekpaideftiria AE	
SLA with Neue Schule 2019/2020	SLA	Neue Schule AE	
SLA with Trianemi School 2019/2020	SLA	Trianemi School	
SLA with Platon School 2019/2020	SLA	Platon School	
SLA with Lycée Franco-Hellénique 2019/2020	SLA	Lycée Franco-Hellénique Eugène Delacroix	
SLA with Arsakeio School 2019/2020	SLA	H EN Athinais Filekpaideftiki Etairia (Arsakeio)	
SLA with Campion School 2019/2020	SLA	Campion School Inc.	
SLA with Ionios School	SLA	Ionios Sxoli SA Training Company	
SLA with St Catherine's British School 2019/2020	SLA	St Catherines British School	
SLA with Papakosmas Datatechnica No 2020/003, P7EM-100, 1452152	SLA	Papakosmas Ntatatechnika EPE	

Title	Type	Contractor	Contracted amount (EUR)
SLA with Papakosmas Datatechnica No 2020/004, P7EM-075, 1452165	SLA	Papakosmas Ntatatechnika EPE	
Amendment 3 of the SLA implementation and usage of the ABAC system	SLA		
Amendment to the SLA between ENISA and BEREC	SLA	BEREC Office	
SLA with Paymaster Office (PMO)	SLA		
SLA with European Personnel Selection Office and European Administrative School (updated)	SLA	EPSO	
Cooperation between EDA and ENISA	Agreement	EDA	
Agreement with the Hellenic Ministry of Infrastructure, Transport and Networks	Agreement	Hellenic Ministry of Infrastructure, Transport and Networks	
ABAC data warehouse extraction and transfer for ENISA's needs	Agreement		27 000.00
Mandate and service agreement for a 'type 2 European school' with the European Commission	Agreement		
Administrative arrangement with Directorate General Human Resources and Security; Security Directorate	Agreement		
Agreement with the Translation Centre for the Bodies of the EU	Agreement		
Provision of a water fountain and water bottles for the Athens office	Agreement		
Collaboration agreement with CEN and CENELEC	Agreement		
Austrian signature scheme for e-cards and mobile signatures	Agreement	A-Trust Gesellschaft fur Sicherheitssysteme im Elektronischen Datenverkehr GMBH	
Agreement for courier services	Agreement	TNT Skypak Hellas EPE	
Mission Charter of the Internal Audit Service of the European Commission	Agreement		
Agreement on strategic cooperation with Europol	Agreement	Europol	
Agreement with Edenred (Ticket Restaurant meal vouchers)	Agreement	Vouchers Services SA	
Joint ENISA–Europol/EC3 working group on security and safety online	Agreement	Europol	
Non-disclosure agreement CT1607860 – confidential and proprietary document between 12 parties	Agreement		
Working arrangement agreement with EU-LISA (MoU)	Agreement	EU-LISA	
Lease agreement Athens office (main building)	Agreement	Athenian Properties Ltd	
Lease agreement Athens office (east wing)	Agreement	Athenian Properties Ltd	
Agreement with Hellenic Postal Services AE – Athens office	Agreement	Ellinika Tachydromeia AE	
Inter-agencies cost-sharing agreement (EUAN)	Agreement	EFSA	982.00
Agreement for courier services	Agreement	DHL International SA	
Mission Charter of the Internal Audit Service – revised	Agreement		

ANNEX 12

STRATEGY FOR COOPERATION WITH THIRD COUNTRIES AND/ OR INTERNATIONAL ORGANISATIONS

The strategy for cooperation with third countries and/or international organisations was approved by the management board in 2017. Following the entry into force of the CSA in 2019, it is expected that during 2021 the Agency will prepare a new international strategy.

NOTES

TPAH-21-001-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

Publications Office

ISBN 978-92-9204-460-2