EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA SINGLE PROGRAMMING DOCUMENT 2022–2024

Condensed work programme 2022

JANUARY 2021

CONTACT

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

LEGAL NOTICE

This publication presents the European Union Agency for Cybersecurity (ENISA) Single Programming Document 2022–2024 (Condensed Work Programme 2022) as approved by the Management Board in Decision No MB/2010/17. The Management Board may amend the Work Programme 2022–2024 at any time. ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source. Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

Luxembourg: Publications Office of the European Union, 2022

Print	ISBN 978-92-9204-566-1	doi: 10.2824/654851	TP-09-22-075-EN-C
PDF	ISBN 978-92-9204-567-8	doi: 10.2824/79403	TP-09-22-075-EN-N

ENISA SINGLE PROGRAMMING DOCUMENT 2022–2024

Condensed work programme 2022

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TABLE OF CONTENTS

FOREWORD

Europe's digital decade has started with a wide range of important, ambitious and pioneering EU policy initiatives that will already have changed the digital landscape by the time we implement this 2022–2024 European Union Agency for Cybersecurity (ENISA) single programming document.

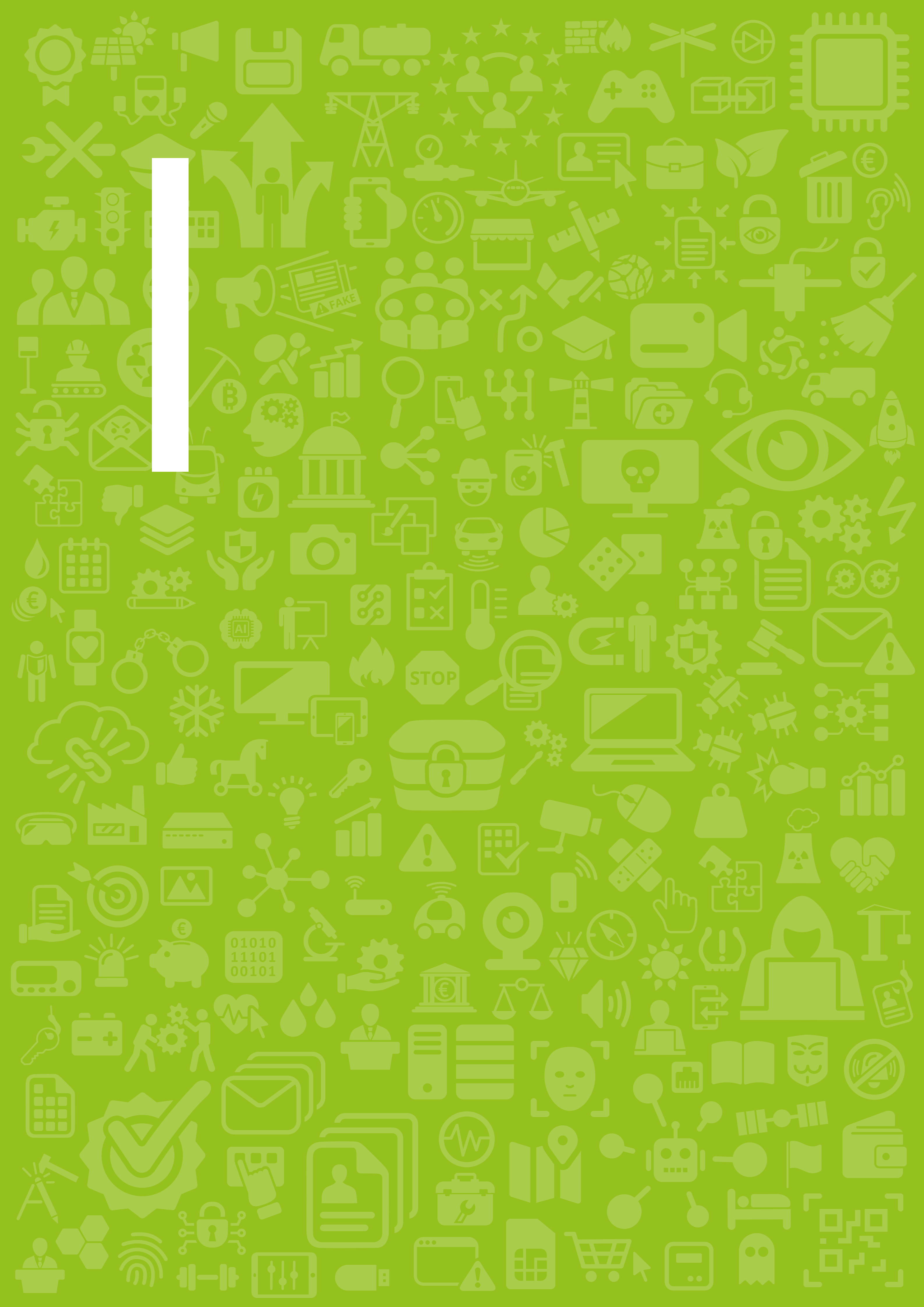
A great many of these initiatives either directly or indirectly integrate cybersecurity concerns, challenges and solutions, and they were introduced in December 2020 in the EU's new cybersecurity strategy. ENISA is ready and indeed very proud to contribute to making these initiatives and their implementation a success, whether by promoting the uptake of the EU's first cybersecurity certification schemes, revising the network and information security (NIS) directive and the electronic identification and trust services (eIDAS) regulation, supporting the full implementation of the EU's 5G Cybersecurity Toolbox or fulfilling its roles in the European Cybersecurity Competence Centre, the Network of National Coordination Centres and the new Joint Cyber Unit. ENISA will use its new mandate, the expanded tasks and the fresh resources given to it by the 2019 Cybersecurity Act to make sure that it remains a key and reliable player and partner within the EU's cybersecurity ecosystem, able to tackle the ever-moving target of cybersecurity. Furthermore, it will make sure that the need for future resources is understood and that resources remain tailored to the EU's cybersecurity prerogatives.

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

I am particularly proud that we – the Agency's staff and Management Board together – have laid solid foundations to make ENISA more agile, more connected and more performance-orientated, and this is reflected in the new organisational structure of ENISA, operational since 1 January 2021, and in the way we work. This has been enshrined in the 2020 ENISA strategy A Trusted and Cyber Secure Europe. And the effects are showing: we are increasingly able to attract cybersecurity talent from all over the EU to help us make a difference. In addition, with the generous support of our Greek host authorities, we have moved to larger premises in Athens, and we are expanding our networks throughout the EU, specifically through the imminent opening of a local office in Brussels.

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

Juhan Lepassaar
Executive Director



PART I
GENERAL CONTEXT

The year 2020 was characterised by the increased prioritisation of EU digital policies, through initiatives such as the Digital Services Act, the proposals for cybersecurity-specific revisions to the NIS directive, and many other digital initiatives, such as the European digital identity. The EU's ambition in this area were encapsulated in the phrase 'making 2020–2030 "Europe's Digital Decade"', used by Commission President Ursula von der Leyen in her State of the Union address[1] in September 2020. Where cybersecurity is concerned, these ambitions were made more concrete in the EU's cybersecurity strategy[2] for the digital decade, released in December 2020, and also in the context of ensuring the EU's technological autonomy. This prioritisation continued in 2021[3] and beyond.

ENISA welcomes the EU's new cybersecurity strategy. The strategy proposes, among many things, a review of the NIS directive, a new critical entities resilience directive, a network of security operations centres (SOCs), new measures to strengthen the EU Cyber Diplomacy Toolbox and the further implementation of the 5G Cybersecurity Toolbox. The Agency is ready to fully utilise its mandate and tasks to act in the areas outlined by the strategy that are covered by its mandate over the period of the 2022–2024 single programming document (SPD).

The COVID-19 pandemic has not only brought healthcare challenges; it has also had an impact on the process of digitalisation in Europe, worldwide and across sectors, increased technological complexities and exposed the need to boost technology skill sets. These effects in turn have accelerated exposure to a wide range of cybersecurity threats and threat actors, as documented by ENISA in 2021, on the one hand, and have increased the need for cybersecurity knowledge, awareness, resilience, cooperation and solutions on the other. This affects all aspects of ENISA's work and the cybersecurity ecosystem that the EU is building up.

ENISA's eighth edition of its annual threat landscape report[4] confirmed current and future trends of cyberattacks becoming ever-more sophisticated, targeted, widespread and undetected. Malware was again voted the EU's number one cyber threat in a poll of intelligence experts, and changes were observed in phishing, identity theft and ransomware that moved them to higher-ranking positions. Monetisation remains cybercriminals' top motivation, and the COVID-19 environment fuelled attacks on homes, businesses, governments and critical infrastructure in 2020 and early 2021. Industries and governments alike continue to be hit by cyberespionage attacks. The number of data breach incidents continues to be very high, and

[1] https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

[2] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

[3] And has been fortified by the most recent State of the Union address (15 September 2021), which highlighted the concepts of cooperation, resilience and situational awareness (https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701).

[4] https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

the amount of stolen financial information and user credentials is growing. Unfortunately, we are getting used to hearing terms like 'Bad Rabbit ransomware', 'Winnti', 'Magecart' and 'watering hole attacks'. In December 2020, the European Medicines Agency was a victim of a cyberattack resulting in the leak of documents relating to the evaluation processes for COVID-19 vaccines. In the same month, another cyberattack on the software company SolarWinds through its supply chain resulted in a back-door infiltration into its commercial software application. The list has grown in 2021, with further supply chain attacks with global implications, such as the Kaseya and SITA attacks. The current escalation and the threat landscape status require the continual introduction of new methods and different approaches for Europe to become cybersecure.

The adoption and implementation of policy frameworks is one key area where the EU is making a difference. Indeed, the policies and initiatives that will be put in place in the coming years will determine how the EU faces the cybersecurity challenges of today and tomorrow. In this context, ENISA will determine and adapt the support that it provides, particularly in the following areas.

THE NIS2 DIRECTIVE AND THE JOINT CYBER UNIT

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

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

ENISA is already invested in the above areas, with its resilience, cooperation and capacity-building work, and will be building up its own capacities to support the outcome of the proposal in the coming years using existing resources and building on these wherever necessary. This will also apply to increased cooperation under the potential Joint Cyber Unit (JCU) umbrella. ENISA will contribute to the implementation of the Commission's recommendation on 'building the Joint Cyber Unit', with a view to contributing to the establishment of an EU crisis management framework. This includes fostering cooperation among cybersecurity communities, among relevant EU institutions, bodies and agencies, and within (and between) civilian cooperation networks (i.e. the Cyber Crisis Liaison Organisation Network (CyCLONe), the CSIRTs Network and, to the extent needed, Cooperation Group).

IMPLEMENTATION OF THE EU CYBERSECURITY CERTIFICATION FRAMEWORK

ENISA is playing a central role in supporting the implementation of the European cybersecurity certification framework by preparing and maintaining the candidate schemes with the support of area experts and in collaboration with public authorities in Member States. It is expected that the draft candidate cybersecurity certifications schemes proposed by ENISA will be adopted as Commission implementing regulations. A conformity assessment of digital products, services and processes in the digital single market will be enabled under the adopted schemes, therefore improving their cybersecurity. At the time of writing, ENISA has prepared a candidate scheme on common criteria (common criteria based European candidate cybersecurity certification scheme) and is advancing its work on cloud services (European cybersecurity certification scheme for cloud services) and 5G (EU5G).

Finalising the candidate schemes for the more specialised product categories under the common criteria and for cloud services is just the first step and should start bringing initial benefits in terms of EU-wide certification processes and higher consumer and user trust during 2022–2024.

RESEARCH AND INNOVATION

The EU is extending its support for and investments in the wealth of expertise and experience in cybersecurity research and technological and industrial development that exists in the EU by prioritising cybersecurity in its research and innovation support efforts, and in particular through its Horizon Europe and Digital Europe programmes. It is also pooling resources and expertise by setting up the European Cybersecurity Competence Centre and the Network of National

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

Coordination Centres[6]. ENISA is ready to contribute to this essential area in the coming years within the role given to it by the regulation establishing the European Cybersecurity Competence Centre and the Network of National Coordination Centres and by the mandate of the Cybersecurity Act (CSA). Some of this work is anticipated to take place in 2022–2024, and the particular tasks required will become clearer as the Cybersecurity Competence Centre becomes operational.

ARTIFICIAL INTELLIGENCE

With the EU's artificial intelligence (AI) agenda advancing rapidly following the European Commission proposal on AI[7] and 2021 coordinated plan on AI[8], the EU is addressing the major technological, ethical, legal and socioeconomic challenges that must be met to put AI at the service of European citizens and the economy, for instance by considering linking high-risk AI systems to mandatory trustworthiness requirements. One of these challenges is understanding the interplay between cybersecurity and AI and how this can affect the availability, safety and resilience of future AI services and applications.

Building on ENISA's AI threat landscape report[9] of December 2020 and with the guidance of its Ad Hoc Expert Group on AI[10], the Agency can continue its open dialogue with EU institutions in support of the legislative initiatives reaching into 2022–2024. In this way, ENISA can continue to support the Commission and Member States by providing good security practices and guidelines.

THE EUROPEAN DIGITAL IDENTITY FRAMEWORK

The EU's eIDAS regulation provides a framework for interoperability of national electronic identification (eID) schemes and sets up an EU-wide market of electronic trust services. eID schemes and trust services are crucial for the EU digital market because they allow citizens and businesses to carry out transactions online in a safe and trusted way. In 2020, the Commission reviewed the eIDAS regulation and identified several gaps. In June 2021, the Commission adopted a proposal for a revised legal framework establishing a European digital identity[11] that can be used by all EU citizens and by EU businesses when carrying out online transactions. In 2022–2024, ENISA will support Member States and the Commission in the implementation and development of the toolbox and the European digital identity framework as set out in the Commission's recommendation of 3 June 2021[12] in addition to promoting the exchange of good practices and capacity building of relevant stakeholders.

FURTHER DEVELOPMENTS

In 2020, ENISA put forward a proposal to open a local office in Brussels in accordance with Article 20(5) of the CSA. This will strengthen ENISA's position in the digital ecosystem of the EU and in particular its role in establishing synergies with EU institutions, bodies, offices and agencies in the field of operational cooperation at EU level. Moreover, the local office in Brussels will aim to ensure regular and systematic cooperation with EU institutions, bodies and agencies and other competent bodies involved in cybersecurity. Indeed, it will support the delivery of tasks mandated to ENISA under Article 7 of the CSA, in particular that of establishing and maintaining structured cooperation with the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU). A detailed and annual cooperation plan is being integrated into ENISA's SPD and is part of the memorandum of understanding (MoU) signed in early 2021. This will enable both organisations to benefit from synergies provided by proximity and daily contact and to avoid any duplication of activities.

In 2021, ENISA established a cooperation agreement[13] with the European Telecommunications Standards Institute (ETSI). ETSI and ENISA have the common objective of collaborating on, contributing to and promoting regional and international standardisation. There is mutual interest in avoiding any duplication of technical work, and in adopting an aligned and complementary approach to the standardisation process in specific domains.

[6] Regulation (EU) 2021/887 of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

[7] Proposal for Regulation (EU) 2021/206 of 21 April 2021 laying down harmonised rules on AI (Artificial Intelligence Act) and amending certain Union legislative acts.

[8] https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review

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

[10] https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/artificial_intelligence/ad-hoc-working-group

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281

[12] Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common union toolbox for a coordinated approach towards a European digital identity framework.

[13] Signature pending.

II

PART II
WORK PROGRAMME 2022

This is the main body of the work programme, describing, as per operational and corporate activity, what the Agency aims to deliver in the respective year in terms of 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 2022.

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

ACTIVITY 1: Providing assistance in 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, and on the basis of the new 2020 EU cybersecurity strategy. Aspects such as privacy and personal data protection are taken into consideration (including encryption).

This activity seeks to bolster policy initiatives on novel/emerging technology areas by providing technical, fact-driven and tailor-made cybersecurity advice and recommendations. In addition to support in emerging policy areas (such as AI, 5G, EU eID, quantum computing, blockchain, big data, digital resilience and response to current and future crises), ENISA – in coordination with the Commission and Member States – will also conduct policy scouting to support the Commission and Member States in identifying potential areas of 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 in accordance with the EU's institutional competencies in this area.

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

Objectives

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

Link to strategic objective (ENISA strategy)

- Cybersecurity as an integral part of EU policies

Results

Cybersecurity aspects are considered and embedded across EU and national policies

Outputs

1.1. Issue reports, studies and analyses on the effectiveness of the current cybersecurity policy frameworks.

1.2. Carry out preparatory work and provide the Commission and Member States with tailor-made advice and recommendations on new policy initiatives in emerging technological, societal and economic trends, such as AI, 5G, eID, digital operational resilience in the finance sector, cyber insurance and other potential initiatives (e.g. The Once Only Technical Solution).

1.3. Assist the Commission in reviewing existing policy initiatives.

Key performance indicator

Indicator:

ENISA's added value to EU institutions, bodies and Member States in providing support to policymaking (ex ante).

Metrics:

1.1. Number of relevant contributions to EU and national policies and legislative initiatives[14].

1.2. Number of references to ENISA reports, analysis in EU and/or national policy documents.

1.3. Satisfaction with the added value of ENISA's contributions (survey).

Frequency: Annual (1.1 and 1.2), biennial (1.3)

Validation

- NIS Cooperation Group (NIS CG) and other formally established groups (outputs 1.1 and 1.2).
- ENISA ad hoc working groups[15] (output 1.2).
- NLO Network, ENISA Advisory Group and other formally established expert groups (when necessary).

Target groups and beneficiaries

EU and national policymaking institutions, EU and national experts (NIS CG, relevant/competent EU or Member State organisations/bodies) and electronic communications services.

Resources planned

Total Human resources (FTEs)	**6[16]**	**Total Financial resources (EUR)**	**363 000**

[14] Baselines for these metrics should be known by the end of 2021. Therefore, targets linked to these baselines will be developed in 2022 for the 2023 work programme.

[15] Created under Article 20(4) of the CSA.

[16] Allocation of an additional five FTEs from the NIS proposal will take place in due course according to the final agreement of regulators and once the tasks have been finalised.

ACTIVITY 2: Supporting implementation of Union policy and law

Overview of activity

This activity provides support to Member State and EU institutions in the implementation of European cybersecurity policy and the legal framework and advice on specific cybersecurity aspects related to the EU's 2020 cybersecurity strategy, the NIS directive, telecom and electronic communications security, data protection, privacy, eID (including the European digital identity framework and trust services), incident notification and the general availability or integrity of the public core of the open internet.

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

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

This activity helps to avoid fragmentation and supports a coherent implementation of the digital single market across Member States, following a consistent approach to cybersecurity, privacy and data protection.

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

Objectives

- Consistent development of sectoral Union policies with horizontal Union policy to avoid implementation inconsistencies.
- Contribute to the efficient and effective monitoring of EU cybersecurity policy implementation in Member States.
- Effective implementation of cybersecurity policy across the EU and aim to support consistency of Member State laws, regulations and administrative provisions related to cybersecurity.
- Improved cybersecurity practices, taking on board lessons learnt from incident reports.

Link to strategic objective (ENISA strategy)

- Cybersecurity as an integral part of EU policies.
- Empowered and engaged communities across the cybersecurity ecosystem.

Results

- Consistent implementation of EU policy and law in the area of cybersecurity.
- EU cybersecurity policy implementation reflects sectoral specificities and needs.
- Wider adoption and implementation of good practices.

Outputs

2.1. Support the NIS Cooperation Group and work streams as per the NIS CG work programme and sectors under NISD.

2.2. Support Member States and the Commission in the implementation and monitoring of the 5G Cybersecurity Toolbox and its individual actions.

2.3. Provide advice, issue technical guidelines and facilitate exchange of good practices to support Member States and the Commission on the implementation of cybersecurity policies, in particular eID and the trust services framework, European Electronic Communications Code and its implementing acts, and security measures for data protection and privacy.

2.4. Assisting in establishing and implementing vulnerability disclosure policies considering also the NIS2 proposal.

Key performance indicator

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 added value of ENISA's support (survey).

Frequency: Annual (2.1), biennial (2.2 and 2.3).

Validation

- NIS Cooperation Group or established work streams (outputs 2.1 and 2.2).
- Article 13a Expert Group and Article 19 Expert Group (output 2.3).
- Formally established bodies and expert groups as necessary (outputs 2.3 and 2.4).
- NLO Network (as necessary).

Target groups and beneficiaries

- Member State cybersecurity authorities (NISD CG members), national supervisory authorities, data protection authorities and national accreditation bodies.
- The Commission, EU institutions/bodies (e.g. Body of European Regulators for Electronic Communications (BEREC), European Data Protection Supervisor, European Data Protection Board, European Union Agency for Railways (ERA), European Maritime Safety Agency (EMSA), sectoral EU agencies (e.g. European Union Agency for the Cooperation of Energy Regulators (ACER) and Interinstitutional committees (e.g. ICT Advisory Committee (ICTAC), Interinstitutional committee for digital transformation (ICDT).
- Article 13a Expert Group and Article 19 Expert Group members.
- EU citizens.
- Conformity assessment bodies and trust service providers.
- Operators of essential services, including their associations and networks.

Resources planned

Total Human resources (FTEs)	**12**	**Total Financial resources (EUR)**	**798 475**

ACTIVITY 3:
Building capacity

Overview of activity

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

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

Objectives

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

Link to strategic objective (ENISA strategy)

- Cutting-edge competences and capabilities in cybersecurity across the EU.
- Empowered and engaged communities across the cybersecurity ecosystem.

Results

- Enhanced capabilities across the community.
- Increased cooperation between communities.

Outputs

3.1. Assist Member States to develop national cybersecurity strategies.

3.2. Organise large-scale biennial exercises and sectoral exercises (Cyber Europe, Blue OLEx, CyberSOPex, etc.) including through cyber ranges.

3.3. Organise training and other activities to support and develop maturity and skills of

Key performance indicator

Indicator:

Increased resilience to cybersecurity risks and preparedness to respond to cyber incidents.

Metrics:

3.1. Increase/decrease of maturity indicators.

3.2. Outreach, uptake and application of lessons learnt from capability-building activities.

Outputs

CSIRTs (including the NIS sectoral CSIRT) 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 work streams as per the NIS CG work programme.

3.6. Support European information-sharing communities through information-sharing and analysis centres (ISACs) based on the core service platform of the Connecting Europe Facility, as well as other collaboration mechanisms such as public-private partnerships. Support the reinforcement of SOCs as well as their collaboration, assisting Commission and Member State initiatives in this area in line with the objectives of the EU cybersecurity strategy in the building and improving of SOCs[17].

3.7. Organise and support cybersecurity challenges including the European Cybersecurity Challenge.

3.8. Report on cybersecurity skills needs and gaps, and support skills development, maintenance and implementation (including a digital education action plan and a report on higher education programmes).

Validation

- NLO Network (as necessary).
- CSIRTs Network (output 3.3).
- CyCLONe members (as necessary).
- NIS Cooperation Group (outputs 3.5 and 3.6).
- Ad hoc working group on SOCs (output 3.6).

Key performance indicator

3.3. Number of cybersecurity programmes (courses) and participation rates.

3.4. Number of exercises executed annually.

3.5. Stakeholder assessment of usefulness, added value and relevance of ENISA capacity-building activities (survey).

Frequency: Annual (3.1, 3.2, 3.3 and 3.4), biennial (3.5).

Target groups and beneficiaries

- Cybersecurity professionals.
- EU institutions and bodies.
- Private industry sectors (operators of essential services such as health and transport).
- CSIRTs Network and related operational communities.
- European information-sharing and analysis centres.
- CyCLONe members.

Resources planned

Total Human resources (FTEs)	13	Total Financial resources (EUR)	1 921 265

[17] In particular, continue developing and updating the mapping of the current landscape of SOCs in the EU, including public and private, provide in-house or as a service, and main operators of SOCs services in the EU, and provide other relevant support to the Commission in implementing the SOCs-related objectives of the EU cybersecurity strategy (e.g. support for the design of calls for expressions of interest, procurements, etc., liaison with stakeholders and research activities).

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, in particular by establishing a local office in Brussels. Actions include establshing synergies with the different national cybersecurity communities (including civilian, law enforcement, cyber diplomacy and cyber defence) and EU actors – notably CERT-EU – with the view to exchange know-how and best practices, provide advice and issue guidance.

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

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

In view of Commission Recommendation (EU) 2021/1086 and the Council conclusions of the 20 October 2021 (ST 13048 2021) 'Exploring the potential of the Joint Cyber Unit (JCU) initiative – Complementing the EU coordinated response to large-scale cybersecurity incidents and crises', ENISA will engage in the development of the JCU, along the lines and the roles defined according to ongoing discussions among Member State and EU operational actors.

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

Objectives

- Enhance and improve incident response capabilities across the EU.
- Enable effective European cybersecurity crisis management by continuously improving the cyber crisis management framework.
- Ensure coordination in cybersecurity crisis management among relevant EU institutions, bodies and agencies (e.g. CERT-EU, European External Action Service, European Union Agency for Law Enforcement Cooperation (Europol)).
- Improve maturity and capacities of operational communities (including CSIRTs Network, CyCLONe group).
- Contribute to preparedness, shared situational awareness, and coordinated response to and recovery from large-scale cyber incidents and crises across different communities.

Link to strategic objective (ENISA strategy)

- Effective cooperation among operational actors within the EU in case of massive cyber incidents.
- Empowered and engaged communities across the cybersecurity ecosystem.

Results

- All communities (EU institutions and Member States) use a rationalised and coherent set of SOPs for cyber crisis management.
- Efficient framework, tools (secure and high availability) and methodologies for effective cyber crisis management.

Outputs

4.1. Support the functioning and operations of the CSIRTs Network (also through MeliCERTes), CyCLONe, JCU, SOCs Network[18] and cyber crisis management in the EU, including cooperation with relevant Blueprint stakeholders (e.g. Europol, CERT-EU, European External Action Service and European Defence Agency).

4.2. Develop and enhance standard operating policies, procedures, methodologies and tools for cyber crisis management (also related to a future JCU).

4.3. Deploy and maintain operational cooperation platforms and tools (MeliCERTes, CyCLONe, MoUs, etc.), including preparations for a secure virtual platform for a future JCU.

Key performance indicator

Indicator:

Effective use of ENISA's tools, platforms and take-up of SOPs in operational cooperation.

Metrics:

4.1. Number of users, both new and recurring, and usage per platform/tool/SOPs provided by ENISA.

4.2. Uptake of the platform/tool/SOPs during massive cyber incidents.

4.3. Stakeholder satisfaction with the relevance and added value of the platforms/tools/SOPs provided by ENISA (survey).

Frequency: Annual (4.1 and 4.2) and biennial (4.3).

Validation

- NLO Network (as necessary).
- CSIRTs Network and CyCLONe (output 4.1).
- Blueprint actors.

Target groups and beneficiaries

- Blueprint stakeholders.
- EU decision-makers, institutions, agencies and bodies.
- Member State CSIRTs Network members.
- NISD Cooperation Group.
- Operators of essential services (OESs) and digital service providers (DSPs).

Resources planned

Total Human resources (FTEs)	**10**	**Total Financial resources (EUR)**	**1 703 350**

[18] Provide support for the design and development of cross-border platforms for pooling of CTI data at EU level (including definition of a blueprint architecture, data infrastructure requirements, data processing and analytics tools, data sharing protocols), CTI exchange initiatives already under way, legal aspects, interoperability, etc.

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

Overview of activity

This activity contributes to the development of a cooperative response at EU and Member States 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 CSIRTs Network and technical, operational and political decision-makers at EU level.

In addition, this activity can include, at the request of Member States, facilitating the handling of incidents or crises, public communication related to such incidents or crisis and testing cooperation plans for such incidents or crises. It can also include supporting EU institutions, bodies, offices and agencies with public communication regarding such incidents and crises. This activity also supports Member States with respect to operational cooperation within the CSIRTs Network by providing advice on a specfic cyber threat, assisting in the assessment of incidents, facilitating technical handling of incidents, supporting cross-border information sharing and analysing vulnerabilities.

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

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

Objectives

- Effective incident response and cooperation among Member States and EU institutions, including cooperation of technical and political actors during incidents or crises.
- Common situational awareness of cyber incidents and crises across the EU.
- Information exchange and cooperation, cross layer and cross border between Member States and as well as with EU institutions.

Link to strategic objective (ENISA strategy)

- Effective operational cooperation within the Union in case of massive (large-scale, cross-border) cyber incidents.
- Empowered and engaged communities across the cybersecurity ecosystem.

Results

- Member States and institutions cooperating effectively during large-scale, cross-border incidents or crises.
- Public informed of important cybersecurity developments.
- Stakeholders aware of current cybersecurity situation.

Outputs

5.1. Generate and consolidate information (including to the general public) on common cyber situational awareness, technical situational reports, incident reports, threats and support consolidation and exchange of information on strategic, operational and technical levels.

5.2. Support technical (including through MeliCERTes) and operational cooperation, incident response coordination and EU-wide crisis communication during large-scale, cross-border incidents or crises.

5.3. Initiate the development of a trusted network of vendors/suppliers.

Key performance indicator

Indicator:

ENISA's ability and preparedness 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 ENISA contributes to the mitigation of (survey).

5.2. Stakeholders' satisfaction with ENISA's preparedness and ability to provide operational support (survey).

5.3. Number of relevant incident responses ENISA contributed to as per Article 7 of the CSA.

Frequency: Biennial (5.1 and 5.2), annual (5.3).

Validation

- Blueprint actors.

Target groups and beneficiaries

- EU Member States (including CSIRTs Network members and CyCLONe).
- EU institutions, bodies and agencies.
- Other type of CSIRTs and product security incident response teams.

Resources planned

Total Human resources (FTEs)	8	Total Financial resources (EUR)	824 500

ACTIVITY 6: Development and maintenance of EU cybersecurity certification framework

Overview of activity

This activity emcompasses actions to establish a European cybersecurity schemes by preparing and reviewing candidate European cybersecurity certification schemes in accordance with Article 49 of the CSA, at the request of the Commission or on the basis of the EU's rolling work programme. Actions also include evaluating adopted certification schemes and participating in peer reviews. In addition, this activity assists the Commission in providing secretariat of the European Cybersecurity Certification Group (ECCG) and providing secretariat of the Stakeholder Cybersecurity Certification Group (SCCG). ENISA also makes available and maintains a dedicated European cybersecurity certification website, as per Article 50 of the CSA.

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

Objectives

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

Link to strategic objective (ENISA strategy)

- High level of trust in secure digital solutions.
- Empowered and engaged communities across the cybersecurity ecosystem.

Results

- Certified ICT products, services and processes are preferred by consumers and businesses.

Outputs

6.1. Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes.

6.2. Implementation and maintenance of the established schemes, including evaluation of adopted schemes and participation in peer review.

6.3. Support the statutory bodies in carrying out their duties with respect to governance roles and tasks.

6.4. Development and maintenance of necessary tools for making effective use of the EU's cybersecurity certification framework (including the certification website, the core service platform (Connecting Europe

Key performance indicator

Indicators:

1. Uptake of the European cybersecurity certification framework and schemes as an enabler of secure digital solutions.
2. ENISA's effective preparation of candidate certification schemes.

Metrics:

6.1. Number of stakeholders (public authorities and/or commercial solution providers) on the EU market using the cybersecurity certification framework for their digital solutions.

6.2. Stakeholders' trust in digital solutions of certification schemes (citizens, public sector and businesses) (survey).

Outputs

Facility) for collaboration, and publication and promotion of the implementation of the cybersecurity certification framework).

Key performance indicator

6.3. Uptake of certified digital solutions (products, services and processes) using certification schemes under the CSA framework.

6.4. Number of candidate certification schemes prepared by ENISA.

6.5. Number of people/organisations engaged in the preparation of certification schemes.

6.6. Satisfaction with ENISA's support in the preparation of candidate schemes (survey).

Frequency: Annual (6.1, 6.4 and 6.5), biennial (6.2, 6.3 and 6.6).

Validation

- Ad hoc certification expert groups (output 6.1).
- ECCG (outputs 6.1 and 6.2).
- European Commission (outputs 6.1–6.3).
- SCCG (outputs 6.3 and 6.4).

Target groups and beneficiaries

- Public authorities, accreditation bodies at Member State and EU levels, certification supervisory authorities, conformity assessment bodies.
- Product manufacturers and service providers who have an interest in EU schemes for the certification of ICT products and services (industry).
- The European Commission; other EU institutions, agencies and competent authorities (e.g. European Data Protection Board); public authorities in the Member States; and members of the ECCG and SCCG.

Resources planned

Total Human resources (FTEs)	11	Total Financial resources (EUR)	1 025 750

ACTIVITY 7: Supporting the European cybersecurity market and industry

Overview of activity

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

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

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

Objectives

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

Link to strategic objective (ENISA strategy)

- High level of trust in secure digital solutions.
- Empowered and engaged communities across the cybersecurity ecosystem.

Results

- Contribution towards understanding market dynamics.
- A more competitive European cybersecurity industry, SMEs and start-ups.

Outputs

7.1. Market analysis on the main trends in the cybersecurity market on both the demand side and the supply side.

7.2. Monitoring developments in related areas of standardisation, analysis on standardisation gaps and establishment and take-up of European and international standards for risk management in relation to certification.

7.3. Guidelines on and examples of good practices in cybersecurity certification requirements for ICT products, services and processes.

7.4. Monitoring and documenting the dependencies and vulnerabilities of ICT products and services.

Key performance indicator

Indicator:

Effectiveness 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 learnt / 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

- SCCG (outputs 7.2 and 7.3).
- ENISA Advisory Group (output 7.1).
- NLO (as necessary).
- ECCG (output 7.4).

Target groups and beneficiaries

- European ICT industry, SMEs, start-ups, product manufacturers and service providers.
- European standardisation organisations (European Committee for Standardization, European Committee for Electrotechnical Standardization and ETSI) and international and industry standardisation organisations.

Resources planned

Total Human resources (FTEs)	8	Total Financial resources (EUR)	373 800

ACTIVITY 8:
Knowledge on emerging cybersecurity challenges and opportunities

Overview of activity

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

A key new component of this activity will be the contribution to the work of the European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Coordination Centres ("Competence Centre and Network"). This will include contributing to the development of a comprehensive and sustainable Cybersecurity Industrial, Technology and Research Agenda, and the respective work programmes.

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

The legal basis for this activity is Article 9 ,Article 11 and Article 5(6) of the CSA.

Objectives

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

Link to strategic objective (ENISA strategy)

- 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

Results

- 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.
- The research and innovation agenda is tied to cybersecurity needs and requirements.

Outputs

8.1. Develop and maintain an EU cybersecurity index.

8.2. Collect and analyse information to report on the cyber threat landscapes.

8.3. Analyse and report on incidents as required by Article 5(6) of the CSA.

8.4. Develop and maintain a portal (information hub), a one-stop shop to organise and make available to the public information on cybersecurity, and establish a procedural framework to support knowledge management activities maximising synergies with the European Cybersecurity Atlas.

8.5. Foresight on emerging and future cybersecurity challenges and recommendations.

8.6. Contribute to the EU's strategic research and innovation agenda and programmes in the field of cybersecurity (annual report).

8.7. Advise on potential investment priorities (e.g. capacity building and market and industry) and emergent cyber technologies, in particular supporting the activities of the Competence Centre and the Network.

Key performance indicator

Indicator:

ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge, including its contribution to the research and innovation agenda.

Metrics:

8.1. Number of users and frequency of usage of the dedicated portal (observatory).

8.2. Number of recommendations, analyses and challenges identified and analysed.

8.3. Number of requests from Member States and EU research and innovation entities to contribute, provide advice or participate in activities.

8.4. Stakeholder satisfaction with the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges and opportunities, including in research (survey).

Frequency: Annual (8.1–8.3), biennial (8.4).

Validation

- NLO Network (as necessary).
- ENISA Advisory Group (as necessary).
- ENISA ad hoc working group (as necessary).
- Formally established bodies and expert groups as necessary (output 8.3).
- The European Cybersecurity Competence Centre and Network of National Coordination Centres and Competence Centre Governing Board (outputs 8.6 and 8.7).

Target groups and beneficiaries

- General public.
- Industry, research and academic institutions and bodies.
- Article 13a Expert Group and Article 19 Expert Group members
- EU and national decision-making bodies and authorities.
- European Cybersecurity Competence Centre and Network.

Resources planned

Total Human resources (FTEs)	**10**	**Total Financial resources (EUR)**	**1 051 950**

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 risks 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 support coordination across Member States on awareness and education.

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

This 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

- Advance cybersecure behaviour by essential service providers in critical sectors.
- Elevate the understanding of cybersecurity risks and practices across the EU and globally.
- Foster EU cybersecurity values and priorities.

Link to strategic objective (ENISA strategy)

- Empowered and engaged communities across the cybersecurity ecosystem.

Results

- Greater understanding of cybersecurity risks and practices.
- Stronger European cybersecurity through higher global resilience.

Outputs

9.1. Develop activities to enhance behavioural change by essential service providers in critical sectors (as defined by the NISD).

9.2. Promote cybersecurity topics, education and good practices on the basis of the ENISA stakeholders' strategy.

9.3. Implement ENISA international strategy and outreach

9.4. Organise European Cybersecurity Month and related activities.

Key performance indicator

Indicator:

1. Level of awareness of cybersecurity, cyber hygiene and cyber literacy across the EU.

2. Level of outreach.

Metrics:

9.1. Number of cybersecurity incidents reported having human error as a root cause.

9.2. Number of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics.

9.3. Geographical and community coverage of outreach in the EU.

9.4. Level of awareness of cybersecurity across the EU / general public (e.g. Eurobarometer and other surveys).

Frequency: Annual (9.1–9.3), biennial (9.4).

Validation

- Management Board (outputs 9.1 and 9.3), SCCG (for certification-related issues under output 9.2).
- NLO Network.
- ENISA Advisory Group (outputs 9.1 and 9.2).

Target groups and beneficiaries

- General public, businesses and organisations.
- Member States and EU institutions, bodies and agencies.
- International partners.

Resources planned

Total Human resources (FTEs)	**5**	**Total Financial resources (EUR)**	**439 900**

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, which sets an objective for the Agency to 'be a centre of expertise on cybersecurity by virtue of its **independence**, the scientific and technical **quality of the advice and assistance it delivers**, the information it provides, the **transparency of its operating procedures**, the **methods of operation**, and its **diligence in carrying out its tasks**.' This objective requires an efficient performance and risk management framework, which should be developed and implemented Agency wide.

Under this activity, ENISA will continue to enhance key objectives of its reorganisation, as described in the Management Board Decision MB/2020/5, including the need to address 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. Actions undertaken will ensure that the Agency's outputs add real value, through making performance and ex post and ex ante evaluations integral to the work programme througout its life cycle, including by rigorous quality assurance through proper project management, internal peer reviews and independent audits and validations. Gaps in skills and training as well as resource planning will be reviewed and mitigated. The Agency will carry out a risk assessment of its organisational activities and IT systems and propose mitigation measures. The Agency will link its main business processes with information systems that serve these processes and will produce a single registry of corporate processes (SOPs).

The legal basis for this activity is 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 stakeholders.

Objectives

- Increased effectiveness and efficiency in achieving Agency objectives.
- Fully comply with legal and financial frameworks in performance (i.e. build a culture of compliance).
- Protect the Agency's assets and reputation, while reducing risks.
- Achieve full climate neutrality of all operations by 2030.

Link to strategic objective (ENISA strategy)

- Sound resource and risk management.

Results

- Maximised quality and value provided to stakeholders and citizens.
- Building lasting credibility and trust.

Outputs

10.1. Implementation of a performance management framework.

10.2. Implementation of a communications strategy.

10.3. Develop and implement risk management plans (including cybersecurity risk assessment of IT systems and a quality management framework) and relevant policies and processes.

10.4. Develop and monitor the implementation of Agency-wide budgetary and IT management processes.

10.5. Implement single administrative practices across the Agency.

10.6. Carry out an overarching audit on the CO_2 impact of all operations of the Agency and develop and implement a targeted action plan.

Key performance indicator

Indicator:

1. Organisational performance culture.

2. Trust in ENISA.

Metrics:

10.1. Proportion of key performance indicators reaching targets.

10.2. Individual staff contribution to achieving the objectives of the Agency through clear links to key performance indicators (CDR report).

10.3. Exceptions in risk register.

10.4. Number of complaints filed against ENISA, including number of inquiries/complaints of the European Ombudsman.

10.5. Number of complaints addressed in a timely manner and in accordance with relevant procedures.

10.6. Results of the annual risk assessment exercise.

10.7. Observations from external audit bodies (e.g. European Court of Auditors) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings and number of observations successfully completed and closed).

10.8. Level of trust in ENISA (survey).

Frequency: Annual (10.1–10.7), biennial (10.8).

Validation

- Management Team.
- Budget Management Committee.
- IT Management Committee.
- Intellectual Property Rights Management Committee.
- Staff Committee.
- ENISA Ethics Committee.

Target groups and beneficiaries

- Citizens.
- All stakeholders of the Agency.

ACTIVITY 11:
Staff development and working environment

Overview of activity

This activity seeks to support ENISA's 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, the impact of the pandemic has shed new light on remote working and the Agency operates a flexible (50/50) office / home working arrangements to better balance work requirements in a pragmatic manner.

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 as an agile and knowledge-based organisation in which staff can evolve personally and professionaly, keeping staff engaged, motivated and with a sense of belonging. This 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 platfoms), delivering state-of-the-art services and supporting ENISA's business owners and stakeholders in line with the Agency's objectives.

Objectives

- Ensure that staff are engaged, committed and motivated to deliver, and empowered to fully use their talent, skills and competences.
- Digitally enabled workplace and working environment (including home workspace) that promote performance and balance social and environmental responsibility.

Link to strategic objective (ENISA strategy)

- Build an agile organisation focused on people.

Results

- ENISA as an employer of choice.

Outputs

11.1. Maintain and implement the competence framework into all HR processes (including into training strategy, CDR, internal competitions and exit interviews).

11.2. Develop a HR strategy with an emphasis on talent development, growth and innovation.

11.3. Undertake actions to develop and nourish talent and conduct necessary management development activities.

11.4. Develop and maintain a user-friendly and service-oriented teleworking and office environment (including digital tools and services).

11.5. Set up service provisions standards and provide quality support and services for ENISA staff, employees, corporate partners and visitors.

Key performance indicator

Indicator:

Staff commitment, motivation and satisfaction.

Metrics:

11.1. Staff satisfaction survey (including attractiveness of ENISA as an employer, staff empowerment, organisational culture, opportunities for internal mobility, workspace, work environment and work tools).

11.2. Quantity and quality of ENISA's training and career development activities organised for staff.

11.3. Reasons for staff departure (exit interviews).

11.4. Staff retention/turnover rate.

11.5. Resilience and quality of ENISA's IT systems and services (including ability to consistently increase satisfaction with IT services and tools).

Frequency: Annual (or ad hoc for metric 11.3).

Validation

- Management Team.
- Joint Reclassification Committee.
- IT Management Committee.
- Task Force on Relocation of the Agency.
- Staff Committee.

Target groups and beneficiaries

- ENISA staff members and employees.

TP-09-22-075-EN-C

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
Agamemnonos 14
Chalandri 15231, Attiki, Greece

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

enisa.europa.eu

Publications Office
of the European Union

ISBN 978-92-9204-566-1