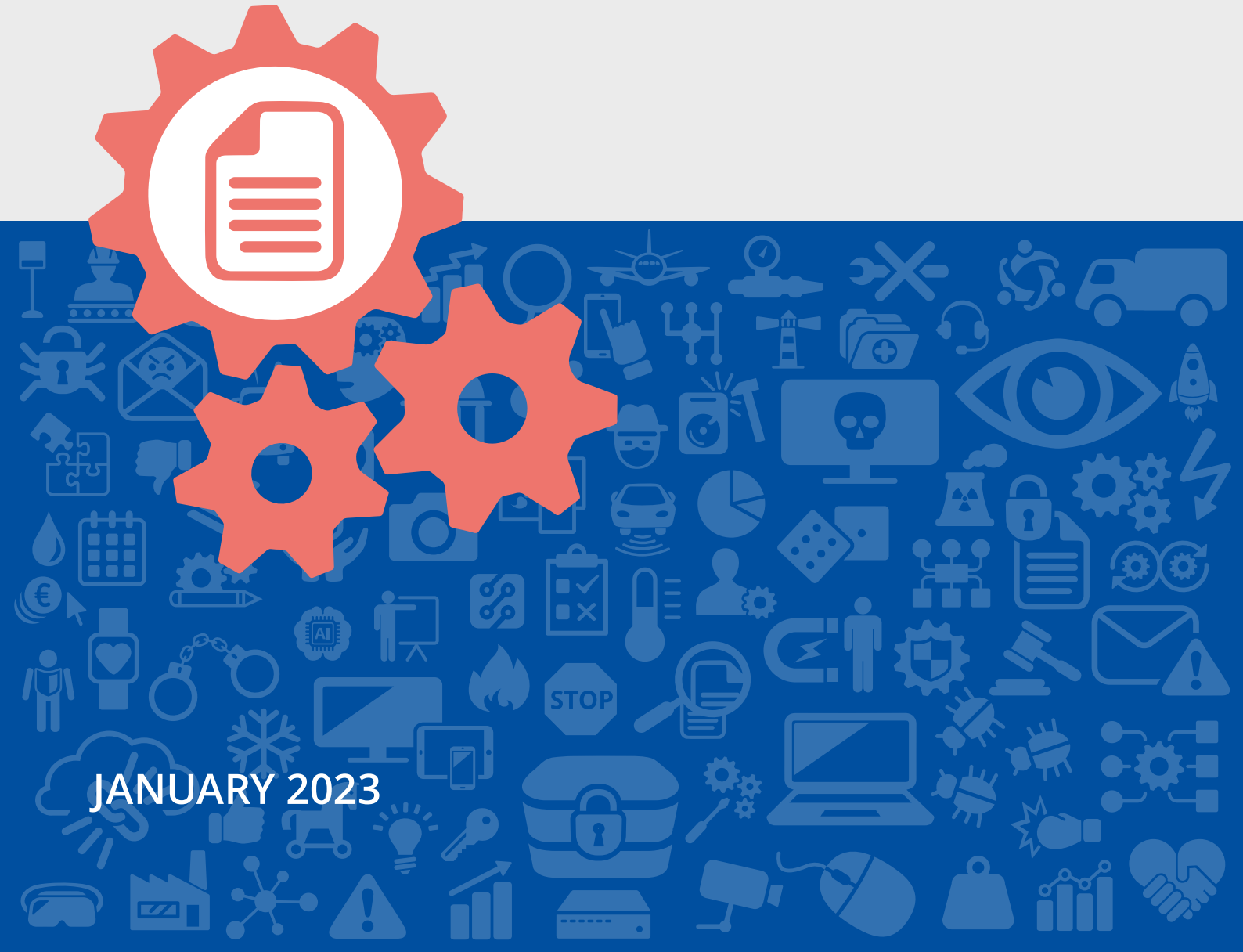
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA SINGLE PROGRAMMING DOCUMENT 2023–2025

Condensed work programme 2023



JANUARY 2023

CONTACT

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

LEGAL NOTICE

COPYRIGHT NOTICE

Luxembourg: Publications Office of the European Union, 2022

Print	ISBN 978-92-9204-631-6	ISSN 2467-4397	doi: 10.2824/892841	TP-AH-23-002-EN-C
PDF	ISBN 978-92-9204-630-9	ISSN 2467-4176	doi: 10.2824/107843	TP-AH-23-002-EN-N

ENISA SINGLE PROGRAMMING DOCUMENT 2023–2025

Condensed work programme 2023

EUROPEAN UNION AGENCY
FOR CYBERSECURITY


FAKE
STOP
AI
01010
11101
00101

TABLE OF CONTENTS

FOREWORD

The strong cyber dimension of the Russian war of aggression against Ukraine and its reflections in the cybersecurity threat landscape have once again emphasised the role of cybersecurity as a cornerstone of a digital and connected Europe. Despite the spill-overs and direct attacks, by-and-large the EU has been able to deal with the cyber threats posed by the Russian aggression through the resilience of its Member States and across Europe, as well as forging support and cooperation with Ukraine and other allies and partners.

Within this context, ENISA's challenge is both to keep pace and set the pace in supporting the Union in achieving a high common level of cybersecurity across Europe. This Single Programming Document (SPD) for the years 2023-2025 represents another step in bringing this about.

Firstly, it puts emphasis on strengthening the resilience of Member States and EU institutions, bodies and agencies. In 2023, approximately half of ENISA's operational resources, both budget and human resources, will be dedicated to enhancing operational cooperation and building capacity. Together with the one-off support of up to 15 million EUR, which the European Commission allocated to ENISA in Autumn 2022, the Agency will be able to massively scale up and expand its ex-ante and ex-post services to Member States in 2023.

Secondly, building on the outcomes of strategic discussions within its Management Board throughout 2022, the Agency has developed service packages in key areas of its mandate. They integrate ENISA's various outputs across different activities, help the agency to prioritise its actions, build and make use of internal synergies, and ensure that adequate resources are reserved across the Agency in a transparent manner.

Thirdly, through this work-programme ENISA will endeavour to help Member States to prepare for the transposition of the reviewed NIS Directive, as well as to prepare the ground for the roll-out and implementation of the EU cybersecurity certification schemes.

Finally, recognising the growing need to bring together the EU's activities and resources across the cybersecurity communities, this SPD establishes a new activity in the area of research and innovation to structure the Agency's cooperation and collaboration with the European Cybersecurity Competence Centre (ECCC) and its emerging networks.

All those areas also accentuate the resource constraints under which the Agency now operates. The foreseen budget increase for the 2023 work programme has been fully absorbed by the increase in staff expenditure and inflation. Due to a shortfall of over 3 million EUR, the Agency has had to reduce the scope of some of its operational activities, limiting the number of exercises and training it rolls-out or postponing its actions in countering ransomware.

Such reductions mean drawbacks in certain areas and might become a real obstacle if new tasks should be added to the Agency without a parallel increase in its resources. Thus, though ENISA welcomes the pioneering set of cybersecurity initiatives being put forward in 2022 and relishes the different and varied roles they imply for the Agency, it needs to have the right level of human and financial resourcing to match those aims and ambitions.

The EU has been mastering cybersecurity initiatives and structures not least through a unique general consensus across parties and across Member States as its prime driving force. This consensus should now also include the resourcing of the Agency. This would give the Union the ability it needs to steer cybersecurity developments in the years to come.

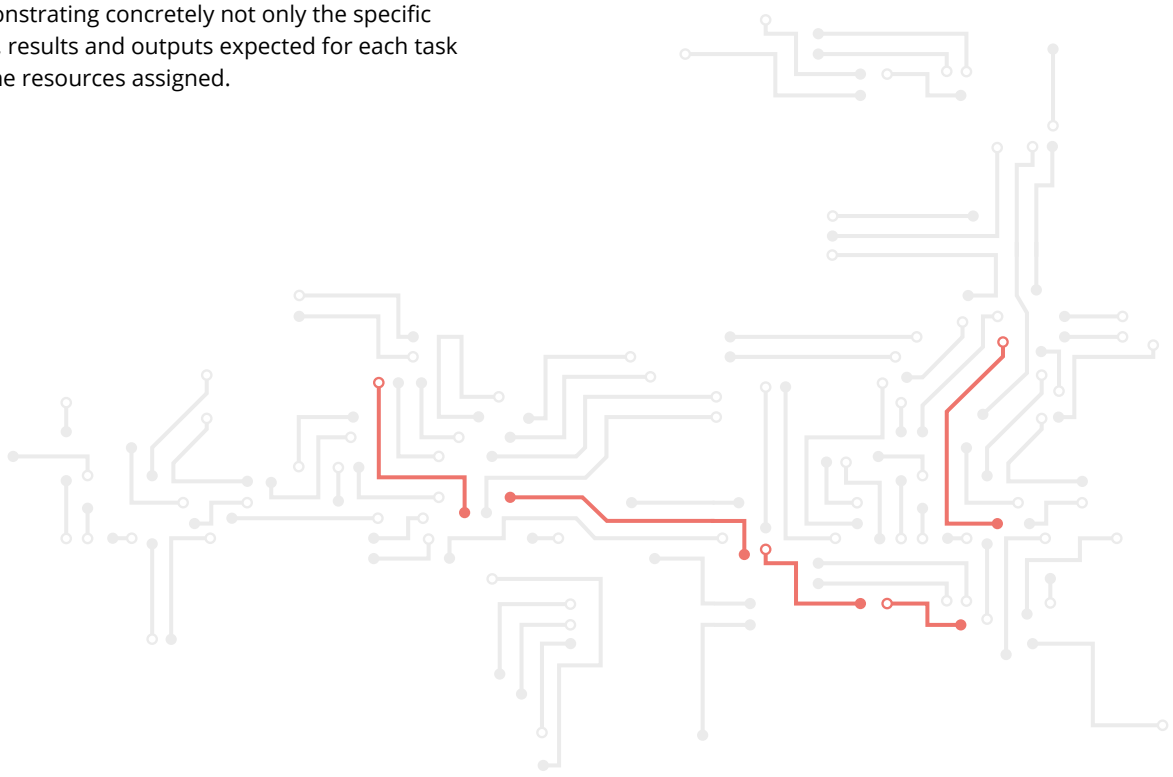
Juhan Lepassaar
Executive Director


FAKE
AI
STOP
01010
11101
00101

WORK PROGRAMME 2023

This is the main body of the Work Programme describing, in terms of its operational and corporate activities, what the Agency aims to deliver in the year 2023 towards achieving its strategy and the expected results. Ten operational activities and two corporate activities in total have been identified to support the implementation of ENISA's mandate in 2023.

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



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 legislative initiatives on matters related to cybersecurity and on the basis of the 2020 EU Cybersecurity Strategy. Aspects such as privacy and personal data protection are taken into consideration (including encryption).

The activity seeks to bolster policy initiatives on novel or emerging technology areas by providing technical, fact-driven and tailor-made cybersecurity advice and recommendations. ENISA will support the EC and MSs on new policy initiatives[1] through evidence-based inputs into the process of policy development. ENISA, in coordination with the EC and Member States will also conduct policy scouting to support them in identifying potential areas for policy development based on technological, societal and economic trends as well as in developing monitoring capabilities and tools to regularly and consistently be able to provide advice on the effectiveness of existing Union policy and law in accordance with the EU's institutional competencies in the area.

This activity also contributes to the service package INDEX by providing data used in the cybersecurity index (Activity 8), by providing input that can be used for future certification schemes (CERTI service package) and by providing findings and recommendations for the service packages offered to critical NIS sectors (Activity 2).

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

Objectives

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

1 Policy initiatives such as the forthcoming Cyber Resilience Act and initiatives on Artificial Intelligence (AI), 5G, quantum computing, blockchain, big data, data spaces, digital resilience and response to current and future crises

Results

Cybersecurity aspects are considered and embedded across EU and national policies

Link to strategic objective (ENISA strategy)

Cybersecurity as an integral part of EU policies

Empowered and engaged communities across the cybersecurity ecosystem

Outputs

1.1. Assist and advise the EC and Member States in reviewing the effectiveness of current cybersecurity policy frameworks

1.2 Assist and advise the EC and MS on new policy developments, as well as carrying out preparatory work

1.3 Support policy monitoring of existing and emerging policy areas and maintain a catalogue of all relevant cybersecurity legislations and policies at the EU level

Validation

- NIS Cooperation Group (NIS CG) and other formally established Groups (outputs 1.1, 1.2 and 1.3)
- ENISA ad hoc working groups[2] (outputs 1.1, 1.2, and 1.3)
- National Liaison Officers Network, ENISA Advisory Group and other formally established expert groups (when necessary)

Stakeholders and levels of engagement[3]

Partners

DG Connect, NIS Cooperation Group, National Competent Authorities, other formally established groups, European Commission Directorate General's Office and Agencies – depending on policy area (e.g. DG GROW, European Insurance and Occupational Pensions Authority)

Involve / Engage

ENISA National Liaison Officers, operators of essential services, digital service providers and industry associations or representatives.

2 in accordance with Art 20(4) of CSA

3 Stakeholders and levels of engagement stem from the implementation of the ENISA stakeholder strategy

Key performance indicators

ENISA's added value to EU institutions, bodies and Member States in providing support for policymaking (ex ante)	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
1.1. Number of relevant contributions to EU and national policies and legislative initiatives	Number	Annual	Manual collection from staff members	193	215
1.2. Number of references to ENISA reports, analyses and/or studies in EU policy documents	Number	Biennial	Survey[4]	N/A	Baseline to be established in 2023
1.3. Satisfaction with added value of ENISA's contributions		Biennial	Survey	N/A	Baseline to be established in 2023
1.4. Number of EU policy files under development and supported by ENISA	Number	Annual	Report	N/A	Baseline to be established in 2023

Resource forecast

Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
1.1	INDEX, SITAW, NIS, CERTI	1.45	246,712	0.00	11,387	0.10	0	1.55	258,099
1.2	NIS, CERTI	1.30	28,086	0.60	27,150	0.10	0	2.00	55,237
1.3	NIS, CERTI	0.95	9,404	0.25	7,523	0.00	0	1.20	16,926
Activity total				**FTE**		**4.75**	**Budget**		**330,262**

4 Biennial surveys for each activity will be conducted in Q1 2023 for reference year 2022. Results will be recorded in annual activity report 2022 and single programming document 2024-2026.

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 the legal framework and technical advice on specific cybersecurity aspects of the implementation of the NIS2[5] and other legislations. The activity seeks to avoid fragmentation and supports a coherent implementation of the Digital Single Market across Member States, following a consistent approach between cybersecurity, privacy and data protection.

Under this activity ENISA provides support to the NIS Cooperation Group, its work streams, and the implementation of its biannual Work Programme including, for example, the implementation of the 5G toolbox, but also new tasks under the NIS2 such as the EU register for operators of digital infrastructure.

It further includes horizontal outputs, which address sector-agnostic cross-cutting issues[6], and sectorial outputs, which are sector-specific and are addressed via targeted service packages for the critical (NIS) sectors. In addition, this work contributes, with relevant sectorial intelligence, to other SPD activities such as exercises and training (Activity 3), situational awareness (Activity 5), knowledge and information (Activity 8), and awareness raising (Activity 9).

Furthermore, Activity 2 provides support to MSs on cybersecurity aspects of policy implementation in the areas of digital identity and wallets (eID), once-only technical solutions (OOTS), technical aspects of privacy and data protection and to the Union's policy initiatives on the security and resilience of the public core of the open internet (e.g. DNS4EU). Overall support is provided for the implementation of the 2020 EU Cybersecurity strategy.

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

Objectives

- Consistent development of sectorial Union policies with horizontal Union policy to avoid implementation inconsistencies
- Contribute to the efficient and effective monitoring of the implementation of EU cybersecurity policy in Member States
- Effective implementation of cybersecurity policy across the Union and consistency between sectorial and horizontal cybersecurity policies
- Improved cybersecurity practices taking on board lessons learned from incident reports

5 The NIS2 covers a) critical operators such as telecoms and trust service providers, which were not covered by the NIS1 but by other legislation (EECC and eIDAS), b) sectors which were already covered by the NIS1 such as energy, finance, health and c) new sectors, such as space and public administration.

6 Such cross-cutting issues include namely security measures, technical aspect of cybersecurity, supply chain risk management, and vulnerability disclosure policies.

Results

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

Link to strategic objective (ENISA strategy)

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

Outputs

2.1. Support the activities of the NIS Cooperation Group including its work programme

2.2. Support Member States and the EC in the implementation of horizontal aspects of the NIS directive

2.3. Support Member States and the EC with the security and resilience of the NIS sectors via targeted service package identified in the ENISA NIS strategy

2.4. Provide advice, issue technical guidelines and facilitate the exchange of good practices to support Member States and the EC on the implementation of cybersecurity aspects of transversal EU policies[7]

Validation

- NIS Cooperation Group and/or established work streams (Outputs 2.1, 2.2, 2.3)
- Telecoms working group (ECASEC) and trust services working group (Outputs 2.3, 2.4)
- eID Cooperation network, ENISA Ad Hoc Working Group on data protection engineering (Output 2.4)
- ENISA National Liaison Officers' Network (as necessary)

Stakeholders and levels of engagement

Partners

National cybersecurity agencies and national authorities for cybersecurity in the EU Member States (NIS CG plenary and work streams), National Regulatory Authorities (ECASEC), National Supervisory bodies (ECATS), Conformity Assessment Bodies (CABs), and informal groups of authorities (e.g. FESA, informal working group of financial authorities), EC, EU Institutions or bodies (e.g. Body of European Regulators for Electronic Communications (BEREC), European Data Protection Supervisor (EDPS), European Data Protection Board (EDPB), European Railway Agency (ERA), European Maritime Safety Agency (EMSA), other sectorial EU Agencies (e.g. ACER, EASA, ESA, ECB, EBA) and institutional industry bodies (e.g. ICANN, RIPE-NCC, ENTSO-E, ENTSO-G, EU.DSO entity)

Involve / Engage

ENISA National Liaison Officers, operators of essential services, digital service providers, trust service providers, data protection authorities, Information Sharing and Analysis Centres (ISACs), research and academia, and industry associations or representatives.

7 Including DORA, Electricity Code, privacy and eIDAS.

Key performance indicators

Contribution to policy implementation and implementation monitoring at EU and national levels (ex post)	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
2.1. Number of EU policies and regulations implemented at national level supported by ENISA	Number	Annual	Manual collection from staff members	5	5
2.2. Number of ENISA reports, analyses and/or studies referenced at EU and NIS CG documents (survey)	Number	Biennial	Survey	N/A	Baseline to be established in 2023
2.3. Satisfaction with added-value of ENISA of support (survey)		Biennial	Survey	N/A	Baseline to be established in 2023
2.4. Number of critical sectors with high level of cybersecurity maturity (NIS sector 360)	Number	Annual	Internal analysis (NIS sector 360)	N/A	Baseline to be established in 2023

Resource forecast

Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
2.1	SITAW, NIS, TREX	6.2	336,846	0	-	0.25	-	6.45	336,846
2.2	SITAW, NIS, CERTI, TREX	4.45	422,402	0		0.3	-	4.75	422,402
2.3	SITAW, NIS, CERTI	-	-	3	214,155	0.3		3.3	214,155
Activity total				**FTE:**		**14.5**	**Budget:**		**973,404**

ACTIVITY 3:
Building capacity

Overview of activity

This activity seeks to improve and develop the capabilities of Member States, Union institutions, bodies and agencies as well as various sectors to respond to cyber threats and incidents, raise resilience and increase preparedness across the Union. This is achieved through the development of frameworks (Risk management, strategies, etc.) that are based on lessons learnt from MSs through the implementation and development of their National Cybersecurity Strategies.

Actions to support this activity include the organisation of large-scale exercises, sectorial exercises, training and others.[23]

In addition, the activity seeks to develop and raise CSIRT capabilities, support information sharing within the cybersecurity ecosystem including cross-border, and assist in reviewing and developing national and Union level cybersecurity strategies.

This activity leads the service package TREX and contributes to NIS and INDEX service packages.

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

Objectives

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

Results

- Enhanced capabilities across the community
- Increased cooperation between communities

Link to strategic objective (ENISA strategy)

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

23 CSIRT training and Capture the Flag (CTF) and Attach Defence (AD) competitions.

Outputs

2.1. Assist MSs to develop, implement and assess National Cybersecurity Strategies

3.2. Organise large-scale biennial exercises and sectorial exercises[8]

3.3. Organise training and other activities to support and develop maturity and skills of CSIRTs (including NIS sectorial CSIRT), NIS cooperation group (NIS CG) and work streams, information sharing and analysis centres (ISACs) and other communities

3.4. ~~Develop coordinated and interoperable risk management frameworks~~[9]

3.5. Support the reinforcement of Security Operational Centres (SOCs) as well as their collaboration, assisting initiatives of the Commission and Member States in this area in line with the objectives of the EU Cybersecurity Strategy in the building and improving of SOCs[10]

3.6. Organise and support cybersecurity challenges including the European Cyber Security Challenge (ECSC)[11]

Validation

- NLO Network (as necessary)
- CSIRTs Network (output 3.3)
- CyCLONe members (as necessary)
- NIS Cooperation Group (output 3.2 and 3.3)
- EU ISACs (output 3.3)
- Ad-hoc WG on SOCs (output 3.5)

Stakeholders and levels of engagement

Involve / Engage

Cybersecurity professionals, private industry sectors (operators of essential services such as health, transport etc.), EU Institutions and bodies, CSIRTs Network and related operational communities, European ISACs, CyCLONe members, NISD Cooperation Group, ISACs Blueprint stakeholders

Key performance indicators

Increased resilience against cybersecurity risks and preparedness to respond to cyber incidents	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
3.1. Increase/decrease in indicators of maturity					
Maturity of national cybersecurity strategies					
Number of Member States that rate the overall maturity of their cybersecurity strategy					
High maturity	Number	Annual	Survey	3	5
Medium maturity	Number	Annual	Survey	4	5
Low maturity	Number	Annual	Survey	3	2

8 (Including Cyber Europe, Blueprint operational level exercise (BlueOLEx), Cyber Exercise to test SOPs (CyberSOPEx etc) and through cyber ranges. NIS cooperation group exercise postponed due to resource constraints.

9 Output is supressed in 2023 work programme due to insufficient resources.

10 Would be priority output for the consideration of consuming any surplus budget in 2023.

11 In the context of this output ENISA is also preparing a few Service Levels Agreements with key EU Agencies with advanced requirements for capacity building activities (e.g. eu LISA).

Increased resilience against cybersecurity risks and preparedness to respond to cyber incidents	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
Number of Member States planning to use ENISA's framework to measure the maturity of their national cybersecurity capabilities					
Already using	Number	Annual	Survey	3	5
Not set but planning to use	Number	Annual	Survey	4	5
Don't know or have not set KPIs currently and will not set KPIs	Number	Annual	Survey	3	3
The frequency with which Member States update their strategies to adapt to technological advancements and new threats					
Every 2–3 years	Number	Annual	Survey	2	3
Every 4–5 years	Number	Annual	Survey	6	8
More than 6 years or don't know	Number	Annual	Survey	2	2
Total maturity of ISACs (self-assessment)	%	Annual	Report	63%	65%
3.2. Outreach, uptake and application of lessons learned from capability-building activities					
CySOPEx 2021 (number of improvements proposed by participants)	Number	Per exercise	Report	5	3[12]
3.4 The number of exercises executed annually	Number	Annual	Report	5[13]	5
3.5 Stakeholder assessment of the usefulness, added value and relevance of ENISA capacity-building activities (survey)					
Usefulness low	%	Biennial of capacity building activities	Survey	9%	Maximum 5%
Usefulness medium	%	Average of capacity building activities	Survey	71%	25% to 50%
Usefulness high	%	Average of capacity building activities	Survey	20%	Minimum 45%

12 Average number of improvements across all exercises.

13 Relates to 2022 exercises executed as of October 2022.

Increased resilience against cybersecurity risks and preparedness to respond to cyber incidents	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
Relevance low	%	Average of capacity building activities	Survey	4%	Maximum 5%
Relevance medium	%	Average of capacity building activities	Survey	53%	25% to 50%
Relevance high	%	Average of capacity building activities	Survey	43%	Minimum 45%
3.5 ISACs maturity					
Number of Exercises organised by EU ISACs	%[14]	Biennial	Report	N/A	Minimum 30%
Number of Training sessions organised by EU ISACs	%	Biennial	Report	N/A	Minimum 30%

Resource forecast

Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
3.1	TREX, INDEX	2.00	108,919	0.00	0	0.00	0	2.00	108,919
3.2	TREX, NIS	4.25	584,153	0.00	0	0.00	0	4.25	584,153
3.3	TREX	4.00	635,580	0.00	0	0.00	0	4.00	635,580
3.4[15]									–
3.5	TREX	0.50	28,544	0.00	0	0.00	0	0.50	28,544
3.6	TREX	3.00	352,043	0.00	0	0.00	0	3.00	352,043
Activity total				**FTE:**	**13.75**	**Budget:**		**1,709,239**	

14 The % out of a total of 10 EU ISACs (as per NIS and NIS2).

15 Output to be suppressed in 2023 given resource constraints.

ACTIVITY 4:
Enabling operational cooperation

Overview of activity

The activity supports operational cooperation among Member States, Union institutions, bodies, offices and agencies and between operational activities in particular through its local office in Brussels, Belgium. Actions include establishing synergies with and between the various national cybersecurity communities (including the civilian, law enforcement, cyber diplomacy and cyber defence) and EU actors notably CERT-EU with a view to exchanging know-how, best practices, providing advice and issuing guidance.

In addition, inline with NIS2 requirements ENISA will continue to support Member States in the CSIRTs Network in respect of operational cooperation. Moreover with the formal establishement of the EU CyCLONe (Cyber Crisis Liason Organization Network) in NISD2, ENISA will support tthe coordination of cyber crises by advising and assisting both networks.

Under this activity ENISA is supporting operational communities through helping to develop and maintain secure and highly available networks and IT platforms and communication channels to ensure, in particular, the maintenance, deployment and uptake of the MeliCERTes platform[16]. Furthemore, in view of the implementation of the NIS2 Directive, this activity supports coordinated vulnerability disclosure by designated CSIRTs in the CSIRTs Network and the implementation of a European vulnerability database.

In view of the EC Recommendation 4520 (2021) and Council Conclusions of the 20 October 2021 (ST 13048 2021) on 'exploring the potential of the Joint Cyber Unit initiative – complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises', ENISA will engage in exploring the potential of the JCU, along the lines and the roles defined according to ongoing discussions amongst MSs and relevant EU institutions, bodies and agencies. In addition, this activity implements the ENISA Cybersecurity Support Action[17].

This activity underpins the Situational Awareness service package and contributes to INDEX and NIS service packages.

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

Objectives

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

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

17 the Agency will prepare where possible for the future Emergency Response Fund, providing that ENISA will be asked to support it and without pre-empting the outcome of the legislative process.

Results

- All communities (EU institutions and MSs) use a streamlined and coherent set of SOPs for management of cyber crises
- Efficient tools (secure and with high availability) and methodologies for effective management of cyber crises

Link to strategic objective (ENISA strategy)

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

Outputs

4.1. Support the functioning and operations of the operational networks and communities and cooperation with relevant stakeholders including blueprint actors[18].

4.2. Support coordinated vulnerability disclosure efforts by designing and deploying the EU Vulnerability Database.

4.3. Deploy, maintain and promote platforms for operational cooperation and tools including preparations for a secure virtual platform for CyCLONe

Validation

4.1. NLO Network (as necessary)

4.2. CSIRTs Network and EU CyCLONe

4.3. Blueprint actors

Stakeholders and levels of engagement

Partners

Blueprint actors, EU decision-makers, institutions, agencies and bodies, CSIRTs Network Members, EU CyCLONe Members, SOCs.

Involve / Engage

NISD Cooperation Group, OESs and DSPs, ISACs

18 CSIRTs Network, CyCLONe, SOCs network, potentially JCU.

Key performance indicators

Effective use of ENISA's tools and platforms and take-up of SOPs in operational cooperation	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
4.1 Number of users, both new and recurring, and usage per platform/tool/SOP provided by ENISA					
CSIRT Network					
Active users – increase from 2020	%	Annual	Platform	115%	110%
Number of exchanges/interactions – increase from 2020	%	Annual	Platform	291%	100%
EU CyCLONe					
Active users – increase from 2020	%	Annual	Platform	143%	100%
Number of exchanges/interactions – increase from 2020	%	Annual	Platform	1,011%	150%*
4.2 Uptake of platforms/tools/SOPs during massive cyber incidents[19]		Ad hoc		N/A	
4.3 Stakeholder satisfaction with the relevance and added value of platforms/ tools/SOPs including EU vulnerability database	N/A	Biennial	Survey	N/A	Baseline to be established in 2023

Resource forecast

Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
4.1	NIS, SITAW	4.30	44,567	3.70	412,895	0.35	0	8.35	457,462
4.2	NIS, SITAW	1.00	72,978	1.00	69,743	0.20	0	2.20	142,720
4.3	SITAW, NIS	3.00	636,908	3.00	885,440	0.00	0	6.00	1,522,348
Activity total				**FTE:**		**16.55**	**Budget:**		**2,122,530**

19 CSIRTs Network, CyCLONe, SOCs network, potentially JCU.

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

Overview of activity

This activity contributes to the development of cooperative preparedness and responses at the level of the Union and Member States to large-scale cross-border incidents or crises related to cybersecurity. ENISA is delivering this activity by aggregating and analysing reports to establish a common situational awareness, ensuring information flow between the CSIRTs network, CyCLONe, the Cyber Crisis Task Force and other technical, operational and political decision-makers at Union level and including cooperation with other services of EUIBAs such as CERT-EU and EC3 and the use of an information exchange with security vendors and non-EU cybersecurity entities. The activity includes the development of regular in-depth EU Cybersecurity Technical Situation Reports in accordance with CSA art 7(6).

In addition, the activity foresees, at the request of Member states, the facilitation of the handling of incidents or crises (including analyses and the exchange of technical information). The activity supports Union institutions, bodies, offices and agencies in the public communication of incidents and crises. The activity specfic cyber threats, assisting in the assessment of incidents, facilitating the technical handling of incidents, supporting cross-border information sharing and analysing vulnerabilities, including through the EU Vulnerability Database (under development in Output 4.2).

This activity supports operational cooperation, including mutual assistance and situational awareness in the framework of the proposed potential JCU. In addition, this activity implements the ENISA Cybersecurity Support Action[20].

Moreover the activity persues the further fostering and optimising of structured cooperation with CERT-EU (please see Annex XIII Annual Cooperation Plan 2023).

This activity leads the service package on situational awareness (SITAW) and contributes to the INDEX and NIS service packages.

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

Objectives

- Enhanced preparedness and effective incident response and cooperation amongst Member States and EU institutions, including cooperation of technical, operational and political actors during incidents or crises
- Common situational awareness before and during cyber incidents and crises across the Union
- Information exchange and cooperation, cross-layer and cross-border between Member States and as well as with EU institutions

20 The Agency will prepare where possible for the future Emergency Response Fund, provided ENISA will be asked to support it and without pre-empting the outcome of the legislative process.

Results

- Member States and institutions cooperating effectively during large-scale cross-border incidents or crises
- Stakeholders and public aware of current developments in cybersecurity

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

Outputs

5.1. Generate and consolidate information (including for the general public) on common cyber situational awareness, technical situational reports, incident reports, threats and support consolidation and exchange of information at strategic, operational and technical levels[21]

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. Maintain, develop and promote the trusted network of vendors or suppliers for information exchange and situational awareness

Validation

- Blueprint actors

Stakeholders and levels of engagement

Partners

EU Member States (including CSIRTs Network members and CyCLONe), EU Institutions, bodies and agencies, other technical and operational blueprint actors, partnership programme for 5.3 (with trusted vendors, suppliers and partners)

Involve / Engage

Other types of CSIRTs and PSIRTs

21 Advisory group proposal for standby emergency incident analysis team provisioned within output 5.1.

Key performance indicators

ENISA ability and preparedness to support response to massive cyber incidents	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
5.1 Number of relevant incident responses to which ENISA contributed in accordance with the CSA Art. 7	Number	Annual	Report	775[22]	TBD
5.2 Number of incidents analysed or curated	Number	Annual	OSINT report	775	
5.3 Number of high visibility incidents analysed	Number	Annual	Flash report	38	
5. 4 Number of large-scale cross-border incidents with high impact analysed	Number	Annual	Joint Rapid Report[23]	13	
5.5 Number of incidents to which ENISA contributed in response	Number	Annual	Cyber Assistance Mechanism	1	
5.6 Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents in which ENISA contributes efforts to mitigate	N/A	Biennial	Survey	N/A	Baseline to be established in 2023
5.7 Take up of ENISA support services	Number	Annual	Report	N/A	Baseline to be established in 2023
5.8 Number of trusted vendors	Number	Annual	Report	N/A	Baseline to be established in 2023
5.9 Stakeholder satisfaction with ENISA's ability to provide operational support	N/A	Biennial	Survey	N/A	Baseline to be established in 2023

22 As of October 2022 for the year 2022.

23 Structured cooperation with CERT-EU.

Resource forecast

Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
5.1	SITAW, INDEX	7.40	764,432	0.00	0	0.00	0	7.40	764,432
5.2	SITAW			1.4	97,701	0.00	0	1.40	97,701
5.3	SITAW	0.25	51,379	0.95	0	0.00	0	1.20	51,379
Activity total				**FTE:**	**10**	**Budget:**		**913,512**	

ACTIVITY 6:
Development and maintenance of EU cybersecurity certification framework

Overview of activity

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

The activity leads the CERTI service package and contributes to the NIS service package.

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
- Improve the management of the security posture of certified products, services and processes by applying continuous compliance monitoring for high level assurance

Results

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

Link to strategic objective (ENISA strategy)

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

Outputs

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

6.2. Implementing and maintaining established schemes including the evaluation of adopted schemes, participation in peer reviews etc.

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

6.4. Developing and maintaining the necessary provisions and tools and services concerning the Union's cybersecurity certification framework (including a certification website, supporting the Commission in relation to the core service platform of CEF (Connecting Europe Facility) for collaboration and publication, and promoting the implementation of the cybersecurity certification framework etc.

Validation

- Ad hoc working groups on certification (output 6.1 and 6.2.)
- ECCG (6.1.6.2, 6.3 and 6.4)
- European Commission (outputs 6.1, 6.2, 6.3, 6.4)
- SCCG (output 6.3. and 6.4.)

Stakeholders and levels of engagement

Partners

EU Member States (including National Cybersecurity Certification Authorities, ECCG), European Commission, EU institutions, bodies and agencies, Selected stakeholders as represented in the SCCG

Involve / Engage

Private sector stakeholders with an interest in cybersecurity certification, conformity assessment bodies, national accreditation bodies consumer organisations

Key performance 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	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
6.2 Stakeholders' level of trust in the digital solutions of certification schemes (citizens, public sector and businesses).		Biennial	Survey	N/A	Baseline to be established in 2023
6.3 Uptake of certified digital solutions (products, services and processes) using certification schemes under the CSA framework		Biennial	Survey	N/A	Baseline to be established in 2023

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	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
6.4 Number of candidate certification schemes prepared by ENISA[25]	Number	Annual	Report	N/A	Minimum 75% of schemes formally requested to be under ongoing development
6.5 Number of people or organisations engaged in the preparation of certification schemes[25]	Number	Annual	Report	N/A	Minimum: 10 organisations; 10 individual experts; 50% of EU MSs joining an AHWG; 30% of organisations to be an SME; 5% to be from a third country
6.6 Satisfaction with ENISA's support for the preparation of candidate schemes		Biennial	Survey	N/A	Baseline to be established in 2023

Resource forecast

Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
6.1	CERTI, NIS	4.65	565,936	0.70	945	0.00	0	5.35	566,881
6.2	CERTI	1.35	90,720	0.00	-	0.00	0	1.35	90,720
6.3	CERTI	1.05		0.00		0.00	0	1.05	–
6.4	CERTI	1.10	75,859	0.15	71,118	0.00	0	1.25	146,977
Activity total				**FTE:**		**9**	**Budget:**		**804,578**

24 Number of schemes formally requested by the Commission or given the go ahead on the basis of the Union Rolling Work Programme, and the number of cybersecurity certification schemes under development by ENISA.

25 Numerical value from ENISA records on a per scheme basis to produce number of: organisations, individual experts, EU Member States, percentage of SMEs, percentage of third country organisations involved that support the promulgation of a cybersecurity certification scheme.

ACTIVITY 7:
Supporting European cybersecurity market and industry

Overview of activity

This activity seeks to foster the cybersecurity market for products and services in the European Union along with the development of the cybersecurity industry and services, in particular SMEs and start-ups, to reduce dependence on outside sources and increase the capacity of the Union and to reinforce supply chains to the benefit of the internal market. It involves actions to promote and implement 'security by design' and 'security by default' measures in ICT products, services and processes, including through standardisation. Actions to support this activity include producing analyses and guidelines as well as good practices on cybersecurity requirements, facilitating the establishment and take up of European and international standards across applicable areas such as risk management as well as performing regular analyses of cybersecurity market trends on both the demand and supply side including monitoring, collecting and identifying dependencies among ICT products, services and processes and vulnerabilities present therein. It also involves creating platforms for collaboration among the cybersecurity market players, in order to improve the visibility of trustworthy and secure ICT solutions in the internal digital market.

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

This activity contributes to the CERTI and NIS service packages.

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

Objectives

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

Results

- Contributing towards an understanding of cybersecurity market dynamics
- A more competitive European cybersecurity industry, SMEs and start-ups

Link to strategic objective (ENISA strategy)

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

Outputs

7.1. Market analysis of the main trends in the cybersecurity market on both the demand and supply side, and evaluation of certified products, services and processes

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

7.3. Guidelines and good practices on cybersecurity for ICT products, services and processes and recommendations to the EC and the ECCC

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

Validation

- SCCG (outputs 7.2 & 7.3)
- ENISA Advisory Group (output 7.1)
- NLO (as necessary)
- ECCG (output 7.4)
- Ad hoc working groups cybersecurity market analysis (output 7.1)

Stakeholders and levels of engagement

Partners

EU Member States (including entities with an interest in cybersecurity market monitoring e.g. NCCA, National Standardisation Organisations), European Commission, EU institutions, bodies and agencies, European Standardisation Organisations (CEN, CENELEC, ETSI), Private sector or ad hoc standards setting organisations

Involve / Engage

Private sector stakeholders with an interest in cybersecurity market and/or standardisation, International Organisation for Standardisation / International Electrotechnical Committee, consumer organisations

Key performance indicators

Effectiveness of ENISA's supporting role for participants in the European cybersecurity market	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
7.1. Number of market analyses, guidelines and good practices issued by ENISA					
Cybersecurity market analysis framework	Number	Annual	Reports	2	1
7.2. Uptake of lessons learned or recommendations from ENISA reports (average of responses)	%	Annual	Survey	49%	60%
7.3. Stakeholder satisfaction with the added value and quality of ENISA's work	%	Biennial	Survey	N/A	Baseline to be established in 2023

Resource forecast

Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
7.1	CERTI, INDEX, CERTI	2.90	116,161	0.35	0	0.00	0	3.25	116,161
7.2	CERTI, NIS	1.60	112,132	0.20	0	0.00	0	1.80	112,132
7.3	CERTI	0.50	73,017	0.00	0	0.00	0	0.50	73,017
7.4	CERTI	0.50	54,716	0.00	0	0.00	0	0.50	54,716
Activity total				**FTE:**		**6**	**Budget:**		**356,027**

ACTIVITY 8:
Knowledge of emerging cybersecurity challenges and opportunities

Overview of activity

This activity delivers on ENISA's strategic objectives SO7 (efficient and effective management of cybersecurity knowledge for Europe) and supports SO6 (foresight on emerging and future cybersecurity challenges). In particular, work under this activity shall provide strategic long-term analyses, guidance and advice on emerging and future technologies, based on the results of regular cybersecurity foresight exercises. Typical examples may include artificial intelligence, quantum computing, space technology, etc

Moreover, on the basis of risk management principles and the consolidation of information and knowledge 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 the Union's institutions, bodies, offices and agencies. In doing so, the Agency will take into account work on incident reporting in accordance with relevant EU legislations. In this respect, the Agency will continue analysing and reporting on incidents as required by Art 5(6) of the CSA and will, upon request, support incident reporting and analysis in other legislative acts such as Art.10 of eIDAS Regulation, DORA, etc.

In terms of the management of knowledge, ENISA will work towards consolidating data, information and knowledge concerning the status of cybersecurity across MSs and the EU and continue its effforts in developing and maintaining the EU cybersecurity index. The Agency will also continue its efforts to organise and make available to the public information on cybersecurity by means of a dedicated infohub that will cater for the needs of different stakeholders.

These activities leverage the expertise on relevant legal, regulatory, economic and social trends and data by aggregating and analysing information. The strategic goal is to provide timely, reliable and useful information and knowledge (across the past-present-future timeline) to various target audiences in accordance with their needs and contribute to the improvement of the state of cybersecurity across the Union.

This activity leads ENISA's efforts towards delivering the cybersecurity index (INDEX) service package, while contributing in parallel to the delivery of the NIS, TREX and situational awareness (SITAW) service packages.

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

Objectives

- Identify and understand emerging and future cybersecurity challenges and opportunities and assess the interlinks between cybersecurity and relevant disrupting technologies in current and future digital transformation
- Increase the resilience and preparedness of Member States and the Union in handling future cybersecurity challenges and opportunities
- Increase knowledge and information for specialised cybersecurity communities
- Greater insight of the current state of cybersecurity across the Union

Results

- Decisions about cybersecurity are future proof and take account of the trends, developments and knowledge across the ecosystem
- MSs have the tools for assessing and understanding their cybersecurity maturity

Link to strategic objective (ENISA strategy)

- Foresight on emerging and future cybersecurity challenges
- Efficient and effective management of cybersecurity information and knowledge for Europe
- Empowered and engaged communities across the cybersecurity ecosystem

Outputs

8.1. Develop and maintain the EU cybersecurity index

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

8.3. Analyse and report incidents as required by Art 5(6) of the CSA as well as other sectorial legislation (e.g. DORA, eIDAS Art. 10, etc.)

8.4. Develop and maintain a portal (information hub), respectively identify appropriate tools for a one-stop-shop to organise and make available to the public information on cybersecurity, and the establishment of 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. ~~Building and exchanging knowledge on ransomware threat (incl. capacity building and awareness raising and education)~~[26]

Validation

- NLO Network (for Output 8.4 and 8.5, and as necessary for other outputs)
- ENISA Advisory Group (as necessary)
- ENISA ad hoc working groups (for Outputs 8.1, 8.2, 8.4 and 8.6 as necessary
- CSIRT Network (output 8.1 and 8.2)
- Formally established bodies and expert groups as necessary (output 8.3)
- NIS Directive Cooperation Group (output 8.1)

Stakeholders and levels of engagement

Partners

EU and national decision-making bodies and authorities, ECASEC and Art. 19 Expert Group members

Involve / Engage

Industry, research and academic institutions and bodies

26 Output supressed during the 2023 work programme due to insufficient resources.

Key performance indicators

ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge including foresight on emerging and future challenges	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
8.1 Number of users and frequency of use of a dedicated portal (observatory)	N/A[27]				
8.2. Number of recommendations, analyses and challenges identified and analysed (reports)	Number	Annual	ENISA reports and studies	288	300
8.3 Number of recommendations, analyses and challenges identified and analysed (reports)	Number	Biennial	Survey	N/A	
8.4 The influence of foresight on the development of ENISA's work programme	Number	Annual	SPD	N/A	Applicable as of 2023
8.5 Uptake of reports generated in activity 8	Number	Annual	Media monitoring report	N/A	Applicable as of 2023
8.6 Uptake of the cybersecurity index	Number	Annual	Index platform	N/A	Applicable as of 2023

Resource forecast

Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
8.1	INDEX	2.50	181,982	0.00		0.00		2.50	181,982
8.2	INDEX, SITAW, NIS	2.00	156,616	0.35		0.25	15,000	2.60	171,616
8.3	INDEX, SITAW, NIS	1.00	58,791	0.20		0.00	–	1.20	58,791
8.4	INDEX, TREX	1.00	152,235	0.00		0.00	–	1.00	152,235
8.5	INDEX	1.10	207,257			0.10	40,000	1.20	247,257
~~8.6~~[28]									
Activity total				**FTE:**	**8.50**	**Budget:**		**811,881**	

27 InfoHub is in the process of being developed.

28 Output suppressed in 2023 due to insufficient resources.

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, Union institutions, bodies, offices and agencies and the EU's international partners, it aims to build an empowered European community with an allied global community which can counter risks in line with the values of the Union. Under this activity the Agency will be organising regular outreach campaigns, providing guidance on best practices and supporting coordination across MSs on awareness and education. Moreover, the Agency will facilitate the exchange of best practices and information on cybersecurity in education between MSs.

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

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

This activity contributes to the NIS, CERTI and TREX service packages. The legal basis for this activity are Articles 10, 12 and 42 of the CSA.

Objectives

- Advance cyber-secure behaviour by essential service providers in critical sectors
- Elevate the understanding of cybersecurity risks and practices across the EU and globally
- Foster EU cybersecurity values and priorities
- Increase the supply of skilled professionals to meet market demand, and promote cybersecurity education

Results

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

Link to strategic objective (ENISA strategy)

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

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 strategy of ENISA's stakeholders

9.3 Implement ENISA's international strategy and outreach

9.4 Organise European cybersecurity month (ECSM) and related activities

9.5 Report on needs and gaps in cybersecurity skills, and support skills development, maintenance and implementation (including the Digital Education Action Plan and a report on higher-education programmes)

9.6 Implement the Cybersecurity in Education roadmap[29]

Validation

- Management Board (as necessary)
- SCCG (for certification related issues under output 9.2)
- NLO Network (as necessary)
- ENISA Advisory Group (outputs 9.1 and 9.2)
- AHWG on cybersecurity skills (output 9.5)

Stakeholders and levels of engagement

Partners

ECSM Coordination Group, National Competent Authorities through the NIS Cooperation Group Work Streams, AHWG on Awareness Raising and Education, Enterprise Security AHWG (SMEs), AHWG on Skills

Involve / Engage

ENISA National Liaison Officers (NLOs), DG CONNECT, NIS Operators of Essential services, European Cybersecurity Competence Centre, International partners (CISA, NIST etc)

29 Roadmap developed by ENISA during the course of 2022.

Key performance indicators

Level of awareness of cybersecurity, cyber hygiene and cyber literacy across the EU Level of outreach	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
9.1 Number of cybersecurity incidents reported having human error as a root cause	Number	Annual	Report	N/A	Baseline to be established in 2023
9.2 Number of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics					
Social media impressions	Average number	Annual	Social media (Facebook, LinkedIn, Twitter)	20,756,630	20,000,000
Social media engagement	Average number	Annual	Social media (Facebook, LinkedIn, Twitter)	117,720	150,000
Video views	Average number	Annual	Social media (Facebook, LinkedIn, Twitter)	2,021,129	3,000,000
Website visits	Average number	Annual	ENISA website	123,504	150,000
Participation in events	Average number	Annual	Media monitoring	5	10
References	Average number	Annual	Website announcements	40	50
9.3 Number of cybersecurity programmes (courses) and participation rates (a)					
Total number of students enrolled in the first year of academic programmes (2020)	Number	Annual	Report[30]	4,843	6,000
Number of male students	%	Annual	Report	80%	70%
Number of female students	%	Annual	Report	20%	30%
Total number of cybersecurity programmes (2020)	Number	Annual	Report	119	130

30 https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education.

Level of awareness of cybersecurity, cyber hygiene and cyber literacy across the EU Level of outreach	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
Number of postgraduate programmes	%	Annual	Report	6%	5%
Number of masters programmes	%	Annual	Report	77%	80%
Number of bachelors programmes	%	Annual	Report	17%	15%
9.4 Geographical and community coverage of outreach in the EU	Number	Annual			Baseline to be established in 2023
9.5 Level of awareness of cybersecurity across the EU / general public (e.g. EU barometer)		Biennial		N/A	Baseline to be established in 2023

Resource forecast

Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
9.1[31]	NIS	1.00	66,482	0.50	43,688	0.00	0.00	1.50	110,170
9.2	INDEX, CERTI	0.75	42,701	0.75	31,314	0.00	0.00	1.50	74,014
9.3	SITAW, TREX	0.75	–	0.75	26,544	0.00	0.00	1.50	26,544
9.4	TREX	0.10	–	0.90	95,147	0.00	0.00	1.00	95,147
9.5*	INDEX, TREX	0.40	47,441	0.60	59,775	0.00	0.00	1.00	107,216
9.6	INDEX	0.20	38,059	0.80	38,059	0.00	0.00	1.00	76,117
Activity total				**FTE:**		**7.50**	**Budget:**		**489,209**

31 Outputs 9.1 and 9.5 would be priority outputs for the consuming of any surplus budget in 2023.

ACTIVITY 10:
Advise on research and innovation needs and priorities

Overview of activity

This activity aims to provide advice to EU Member States (MSs), EU institutes, bodies and agencies (EUIBAs) on research needs and priorities in the field of cybersecurity, thereby contributing to the EU's strategic research and innovation agenda.

To prepare this strategic advice, ENISA will take full account of past and ongoing research, activities in development and technology assessment, and scan the horizon for emerging and future technological, societal and economic trends that may have an impact on cybersecurity.

ENISA will also conduct regular consultations with relevant user groups, projects (including EU funded projects), researchers, universities, institutes, industries, start-ups and digital innovation hubs to consolidate information and identify gaps, challenges and opportunities in research and innovation from the different quadrants of the community.

This activity contributes to the delivery of ENISA NIS service package.

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

Objectives

- Advance the response to current and emerging cyber risks and threats with the use of effective risk prevention technologies
- Ensure that the EU strategic research and innovation agenda in cybersecurity is aligned with the needs and priorities of the community
- Reduce dependence on cybersecurity products and services from outside the Union and to reinforce supply chains within the Union

Results

- Research and development of cybersecurity technology reflecting the needs and priorities of the Union
- Funding the development of cybersecurity technologies that meet the Union's ambition to become more resilient, autonomous and competitive

Link to strategic objective (ENISA strategy)

- Foresight on emerging and future cybersecurity challenges
- Empowered and engaged communities across the cybersecurity ecosystem

Outputs

10.1 Consolidated cybersecurity research and innovation roadmap across the EU

10.2 Collect and analyse information on new and emerging information and communications technologies in order to identify gaps, trends, opportunities and threats (research & innovation observatory)

10.3 Provide strategic advice to the EU agenda on cybersecurity research, innovation and deployment

Validation

- The European Cybersecurity Competence Centre and Network of National Coordination Centres and Competence Centre Governing Board (output 10.2 & 10.3)
- NLO as necessary

Stakeholders and levels of engagement

Partners

Member States (including the National Coordination Centres), EU-IBAs (Including the EC, ECCC and JRC)

Involve / Engage

Market actors – in particular the NIS sectors' stakeholders (e.g. OES), academia and research communities, cybersecurity industry as well as solution and service providers

Key performance indicators

Contributing to Europe's Strategic Research and Innovation Agenda in the field of cybersecurity.	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
10.1 Number of requests from the EU-IBAs (including the ECCC) and MSs to contribute, provide advice or participate in activities	Number	Annual	Report	N/A	Baseline to be established in 2023
10.2 Number of references to ENISA advice and recommendations in the EU Strategic Research and Innovation Agenda including Annual and Multiannual Work programmes	Number	Annual	Report	N/A	Baseline to be established in 2023
10.3 Stakeholder satisfaction on the usefulness, relevance and timeliness of ENISA's advice on cybersecurity research needs and funding priorities (Survey)		Biennial	Survey	N/A	Baseline to be established in 2023

Resource forecast

Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
10.1				1	41,428	0.00	0	1	41,428
10.2	NIS	0.10	0	0.90	123,453	0.00	0	1	123,453
10.3				1.8	25,490	0.20	5,000	2	30,490
Activity total				**FTE:**		**4**	**Budget:**		**195,371**

CORPORATE ACTIVITIES

Activities 11 to 12 encompass enabling actions that support the operational activities of the agency.

ACTIVITY 11: Performance and risk management

Overview of activity

This activity seeks to achieve the requirements set out in Art 4(1) of the CSA that sets an objective for the Agency to: 'be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks'. This objective requires an efficient performance and risk management framework, and the development of single administrative practices. It also includes building an internal capacity for contribution, e.g. via shared services, to the EU Agencies network and in key areas of the Agency's expertise (e.g. cybersecurity risk management).

Under this activity ENISA will confinue to enhance the key objectives of the renewed organisation, as described in the MB decision No MB/2020/5, including the need to address the gaps in the Agency's quality assessment framework, enhance proper and functioning internal controls and compliance checks. In terms of resource management the budget management committee ensures the Agency adheres to sound financial management.

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

Objectives

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

Results

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

Link to strategic objective (ENISA strategy)

- Sound resource and risk management

Outputs

11.1 Maintain the framework for performance management including through single administrative practices across the Agency

11.2 Develop and implement annual communications strategy

11.3 Develop and implement risk management plans including cybersecurity risk assessment for IT systems, including focus on quality management framework and business processes as well as relevant policies

11.4 Maintain and monitor the implementation of Agency wide processes for IT management and develop processes for budgetary management

11.5 Manage and provide secretariats for statutory bodies (EB, MB, NLO and AG)

11.6 Obtain and maintain the EU Eco-Management and Audit Scheme (EMAS) certificate through continuous overview of the impact of CO2 on all operations of the Agency in line with the applicable legal framework and publish a statement on the environment

Validation

- Management Team
- Chairs of statutory bodies (Output 10.5)
- Budget Management Committee
- IT Management Committee
- Intellectual Property Rights Management Committee
- Staff Committee
- ENISA Ethics Committee

Stakeholders and levels of engagement

Partners

Members of statutory bodies such as Management Board, Advisory Group and National Liaison Officers

Involve / Engage

All ENISA stakeholders

Key performance indicators

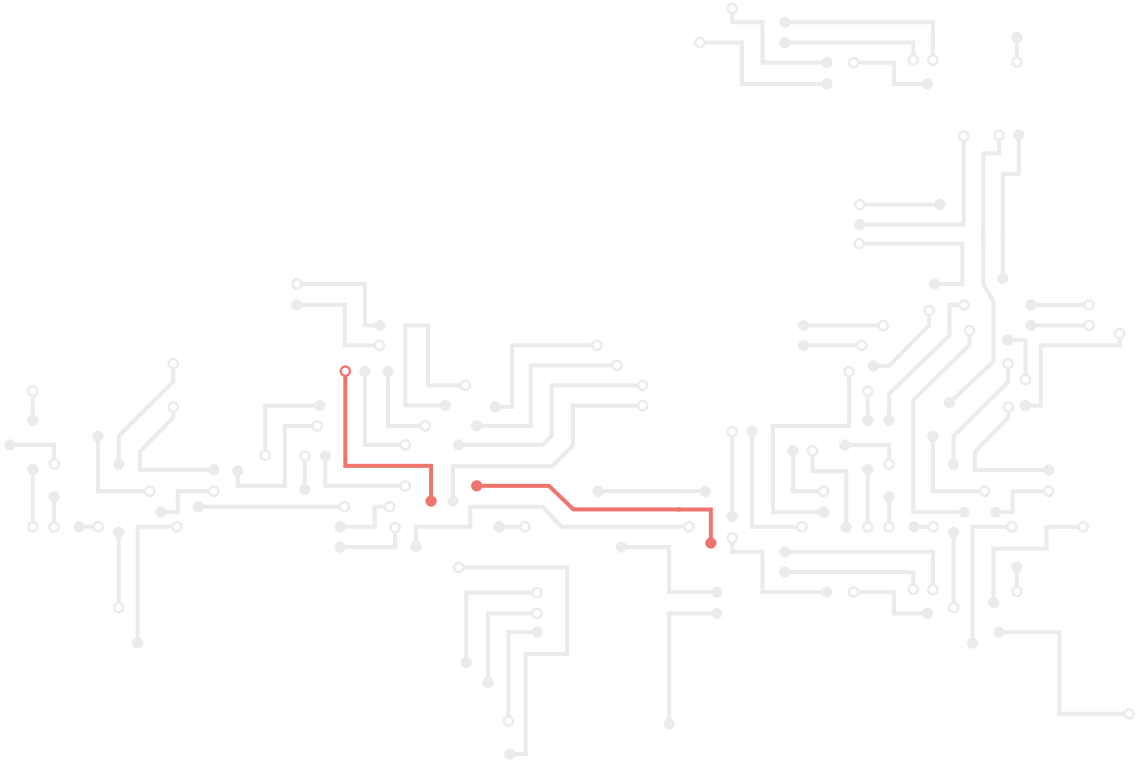
Organisational performance culture Trust in ENISA brand	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
11.1. Proportion of key performance indicators reaching targets	%	Annual	Report	N/A[32]	65%
11.2. Individual staff contribution to achieving the objectives of the agency via clear link to KPIs in staff career development report (CDR report) (all units aggregated)	%	Annual	Objectives 2021	60%	85%
11.3. Exceptions in the risk register	Number	Annual	Internal control	16	11
Deviation from financial regulations	Number	Annual	Internal control	14	10
Deviation from staff regulations	Number	Annual	Internal control	2	1
11.4. Number of complaints filed against ENISA, including number of inquiries or complaints submitted to the European Ombudsman	Number	Annual	Report	19	12
11.5 Number of complaints addressed in a timely manner and according to relevant procedures	Number	Annual	Internal control files	N/A	Baseline to be established in 2023
11.6 Number of high risks identified in annual risk assessment exercise	Number	Annual	Internal control files	N/A	Baseline to be established in 2023
11.7 Implementation of risk treatment plans	Number	Annual	Report	N/A	Baseline to be established in 2023
11.8 Number and types of activities at each level of engagement[33]	Number	Annual	Report	N/A	Baseline to be established in 2023
11.9. Observations from external audit bodies (e.g. European Court of Auditors ECoA) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings and number of observations successfully completed and closed	Number	Annual	Report	4	2
11.10 Level of trust in ENISA		Biennial	Survey	N/A	Baseline to be established in 2023

32 Baselines were available as of the 2021 annual activity report therefore proportion of metrics reaching targets will be assessed in the 2022 annual activity report.

33 Relates to the stakeholder strategy and its implementation, refers to activities such as conferences, workshops etc.

Resource forecast

Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)	
		FTE	EUR	FTE	EUR	FTE	EUR
11.1	All service packages	1		5.5	160,850		
11.2	All service packages	2		2	304,000		
11.3	All service packages	0.5		3	197,000		
11.4				1.5	0		
11.5				2	126,500		
11.6				0.5	61,500		
Activity total		**FTEs:**		**18**	**Budget:**		**849,000**



ACTIVITY 12:
Staff development and working environment

Overview of activity

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

The actions which will be pursued under this activity will focus on making sure that the Agency's HR resources fit the needs and objectives of ENISA, by attracting, retaining and developing talent and building ENISA's reputation as an agile and knowledge-based organisation where staff can evolve personally and professionaly, where staff are kept engaged, motivated and have a sense of belonging. Emphasis will be placed on the development of competency and ways to make ENISA an 'employer of choice' in order to support ENISA's objectives This activity will seek to build an attractive workspace by establishing an effective framework enabling teleworking outside the place of assignment, developing and maintaining excellent working conditions (premises, layout of office space) and implementing modern user-centric IT and teleconferencing tools delivering state-of-the-art corporate services and supporting ENISA's business owners and stakeholders in line with the Agency's objectives.

ENISA will strive to maximise the efficiency of its resources by maintaining its focus on developing a flexible, highly-skilled and fit-for-purpose workforce through strategic workforce planning in order to ensure the effective functioning of the Agency and to maintain high quality services in the administrative and operational areas. ENISA will further improve the support given to it in strategic planning and resource management, leading to a constant optimisation of resources under short- and long-range time-frames. This will enable ENISA to enhance its capabilities in future-readiness and continue its path towards an agile, knowledge-based and matrix way of working. The Agency will continue to look into flexible (50/50) working arrangements to better balance work requirements in a pragmatic manner.

In parallel, ENISA will continue to enhance its secure operational environment to the highest level, and strive for excellence in its infrastructure services based on best practices and frameworks. It will also explore cloud-enabled services that are fit for purpose and provide services in accordance with recognised standards. Besides that, ENISA will strive to promote and foster eco-system solutions, explore opportunities for shared services with other EU agencies, leverage standard technologies where possible and support flexible ways of working. As ENISA aspires to become a trusted partner it will continue to provide customer-focused multi-disciplinary teams that demonstrate a customer centric, can-do and agile attitude.

Objectives

- Engaged staff, committed and motivated to deliver, and empowered to fully use their talent, skills and competences
- Consistent and regular reviews of the Agency's resources to seek an appropriate match with the needs of the organisation, along with obtaining internal and external gains in efficiency across the organisation
- Digitally enabled work-place environment (including home work-space) which promotes performance and balances social and environmental responsibility
- Enable operations at the highest level of security
- Build a culture of continuous improvement, agility, customer centred and can-do attitude

Results

- ENISA as an employer of choice, enabling growth and excellence in a secure environment

Link to strategic objective (ENISA strategy)

- Build an agile organisation focused on people

Outputs

12.1 Manage and provide recurring quality support services in the area of resources, security[34] and infrastructure for ENISA staff, employees, corporate partners and visitors

12.2 Develop and implement the Agency's corporate strategy (including HR strategy) with an emphasis on talent development and growth, innovation and inclusiveness;

12.3 Enhance operational excellence and digitalisation through modern, secure and streamlined ways of working and self-service functionalities

12.4 Provide a secure, safe, modern and welcoming place to work (and telework) including staff welfare

12.5 Establish standards for the provision of services and processes for optimising services

Validation

- Management Board (Output 12.2)
- Management Team
- IT Management Committee
- Budget Management Committee
- Staff Committee

Stakeholders and levels of engagement

Partners

ENISA staff members and EU institutions, bodies and agencies

Involve / Engage

Private sector and international organisations

34 Including full accreditation of the Agency to handle and manage EUCI by end of 2023 confirmed by DG Human Resources and Security.

Key performance indicators

Staff commitment, motivation and satisfaction	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
12.1 . 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)	%	Annual	Staff satisfaction survey	72%	75%
12.2-. Quality of ENISA training and career development activities organised for staff	%	Annual	Staff satisfaction survey	49%	55%
12.3. Reasons for staff departure (exit interviews)[35]	Scale 1–10	As required	HR files	7.1	7.5
12.4 Turnover rates	%	Annual	HR files	3%	3%
12.5 Establishment plan posts filled	%	Annual	HR files	91%	95%
12. 6. Resilience and quality of ENISA IT systems and services	%	Annual	IT reports and staff satisfaction survey	78%	80%
12.7 Percentage of procurement procedures launched via e-tool (PPMT)	%	Annual	Procurement files		> 80 %
12.8 Percentage of payments made within 30 days	%	Annual	Finance files		> 90%
12.9 Late Payments	%	Annual	Finance files		<10%

35 Standardised set of ten questions with a scale of 1 to 10 that provide an opportunity for ENISA to seek feedback about a staff member's experience. The higher the number the better the experience.

Resource forecast

Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)	
		FTE	EUR	FTE	EUR	FTE	EUR
12.1				9	2,138,000		
12.2				3	383,000		
12.3				1.5	964,000		
12.4				1.5	832,000		
12.5				2	100,000		
Activity total		**FTEs:**		**17**	**Budget:**		**4,417,000**[36]

36 Indicated budget excludes staff (TA, CA, SNE) salaries and allowances.

TP-AH-23-002-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
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 978-92-9204-630-9