European Union Agency
for Cybersecurity

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

MANAGEMENT BOARD DECISION

DECISION No MB/2024/14

OF THE ENISA MANAGEMENT BOARD

of 14 November 2024,

on the general direction of the operation of ENISA (ENISA Strategy)

THE MANAGEMENT BOARD OF THE EUROPEAN UNION AGENCY FOR CYBERSECURITY

Having regard to

- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), in particular Article 15.1 (a);
- Decision No MB/2020/8 of the Management Board of the European Union Agency for Cybersecurity on the general direction of the operation of ENISA (ENISA Strategy);

Whereas

(1) The Management Board launched a review procedure of the ENISA Strategy (adopted by Decision No MB/2020/8) as foreseen in MB Decision No MB/2020/8, Art. 2.2;
(2) ENISA Financial Regulation provides for a two-year cycle of ex-ante and ex-post evaluations in relation to programmes and activities that entail significant spending. Ex-ante evaluations supporting the preparation of programmes and activities shall be based on evidence, if available, on the performance of related programmes or activities and shall identify and analyse the issues to be addressed, the added value of Union involvement, objectives, expected effects of different options and monitoring and evaluation arrangements.
(3) ENISA strategy, adopted in 2020 should be reviewed after 4 years
(4) The revised strategy is a result of close cooperation between the ENISA Executive Director, the Management Board and the ENISA Task Force on supporting the review of ENISA strategy and mandate after seeking input from the ENISA Advisory Group, the National Liaison Officers Network, ENISA staff and the ENISA Task Force on supporting the review of ENISA strategy and mandate;
(5) The Executive Board endorsed this Decision at its meeting held on 17-18 October 2024.

HAS DECIDED TO ADOPT THE FOLLOWING DECISION:

Article 1

The ENISA Strategy is adopted as annexed to this Decision.

Article 2

1) This Decision shall enter into force on the day of its adoption.
2) The Management Board shall launch a review procedure, if relevant, as from 2028 or earlier subject to revised Cybersecurity Act entry into force.

Done in Athens, 14 November 2024

On behalf of the Management Board,

[signed]

Ms Fabienne Tegeler
Chair of the Management Board of ENISA

A TRUSTED AND CYBER SECURE EUROPE

VISION

A trusted and cyber secure Europe

MISSION

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union. We aim to be a centre of expertise on cybersecurity, collecting and providing independent, high quality technical advice and assistance to Member States and EU bodies on cybersecurity.

We support the development and implementation of the Union's cybersecurity policies. We aim to strengthen trust in the digital market, boost the resilience of the Union's critical sectors, and keep our economy, our society and our citizens digitally secure. We aspire to be an agile, environmentally and socially responsible organisation focused on people.

VALUES

Community Mind-Set. ENISA builds and works with communities, respecting their competencies and expertise, and fosters synergies, principles for working in cybersecurity and trust to best achieve its mission.

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

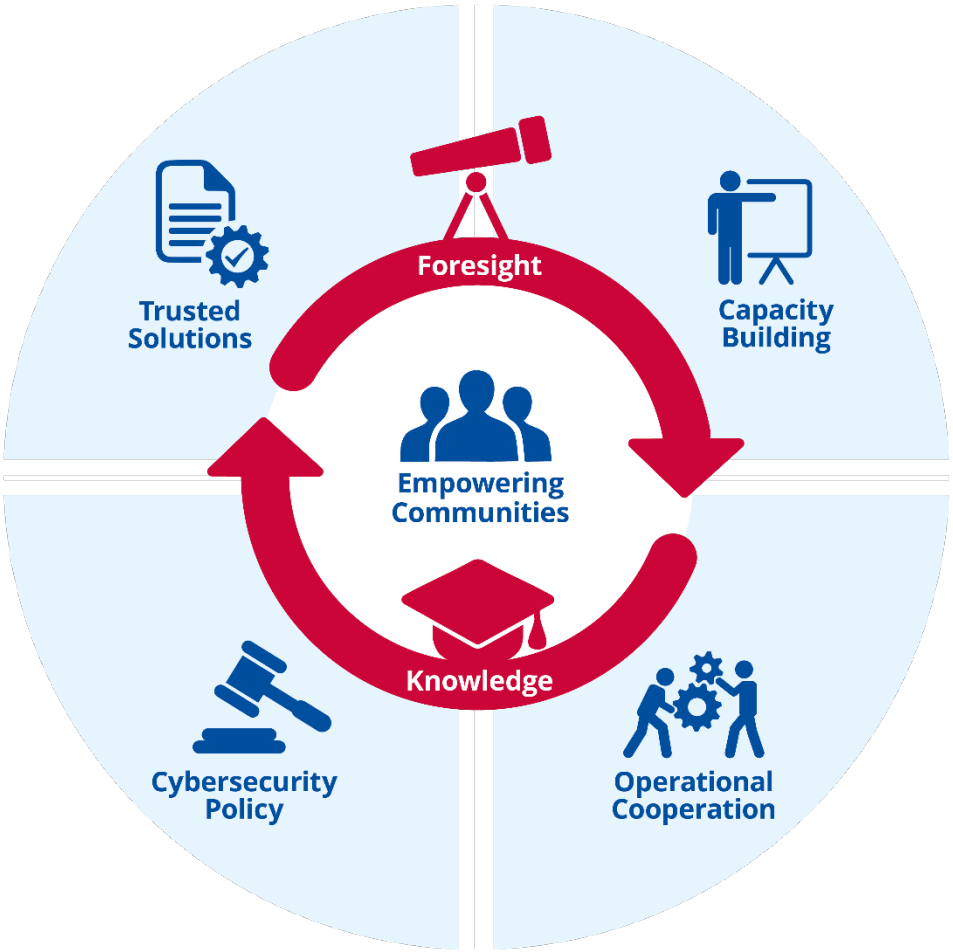
Integrity or ethics. ENISA upholds ethical principles and applies the relevant EU rules and obligations in its services and working environment, ensuring fairness and inclusiveness.

Respect. ENISA respects fundamental European rights and values in offering its services and in its working environment and respects the expectations of its stakeholders.

Responsibility. ENISA assumes its social responsibilities, integrating social and environmental dimensions into its work practices and internal procedures.

Transparency. ENISA adopts procedures, structures and processes that are open, factual and independent in order to limit bias, ambiguity, fraud and obscurity.

OBJECTIVES



Horizontal objectives

Strategic objective. 'Empowered communities in an involved and engaged cyber ecosystem'.

Context. Cybersecurity is a shared responsibility. Europe strives for a cross sectoral, all-inclusive framework for cooperation. ENISA plays a vital role in fostering cooperation among cybersecurity stakeholders (Member States, Union entities and other communities). In these efforts, ENISA emphasises complementarity, engages stakeholders based on their expertise and role in the ecosystem and creates new synergies. The goal is to empower communities to enhance cybersecurity efforts exponentially through strong multipliers across the EU and globally.

What we want to achieve

- A comprehensive EU-wide knowledge base, fostering collaboration, sharing lessons learned and promoting EU expertise in complementarity with Member States and EU entities.
- An empowered cyber ecosystem serving communities in order to understand their role, enhance it, and actively share expertise and best practices.

- Equip communities with knowledge and tools to effectively enhance cybersecurity efforts globally.

Strategic objective. 'Foresight on emerging and future cybersecurity opportunities and challenges'

Context. New technologies, whether still in their infancy or close to mainstream adoption, create novel cybersecurity opportunities and challenges that would benefit from the use of foresight methods. Strategic foresight is not only about technologies but should include additional dimensions, such as political, economic, societal, legal and environmental aspects to name a few. Through a structured process enabling dialogue among stakeholders and in coordination with other EU initiatives on research and innovation, foresight would be able to identify the opportunities and support early strategies to mitigate the challenges in improving EU resilience to cybersecurity threats. To fully reach its goal, foresight should be addressed as a transversal principle across all ENISA's strategic objectives.

What we want to achieve

- Understanding emerging cybersecurity trends and patterns on strategic sectors in the EU using foresight and future scenarios in coordination with relevant activities of the EU in research and innovation.
- Fostering a participatory dialogue while collaborating with diverse stakeholder communities to envisage possible future scenarios.
- Early, timely and continuous assessment of opportunities, challenges and risks to identify targeted measures for various stakeholder communities.

Strategic objective. 'Consolidated and shared cybersecurity information and knowledge support for Europe'

Context. Efficient and effective but also consolidated information and knowledge is the foundation of informed decision-making, as well as proactive and reactive protection and resilience through better understanding of the threat landscape. The much-needed common understanding and assessment of EU's cybersecurity maturity relies on information and knowledge. Consolidating and sharing cybersecurity information and knowledge strengthens the culture of cooperation and collaboration between communities and strengthens networks and partnerships.

What we want to achieve

- Consolidated information and knowledge to better assess the level of cybersecurity across the EU and across important and critical sectors and products to evaluate maturity and proposed targeted recommendations.
- The sharing of information and knowledge for public and private cybersecurity communities in the EU in an accessible, customised, timely and applicable form, with appropriate methodology, infrastructures, resources and tools based on a variety of data sources.
- The promotion of continuous quality assurance and validation methods to achieve longstanding delivery and the improvement of services.

Vertical objectives

Strategic Objective. 'Support for effective and consistent implementation of EU cybersecurity policies'

Context. Cybersecurity is a cornerstone of digital transformation and is a requirement in the most critical sectors of the EU's economy and society. It is also considered across a broad range of policy initiatives. To avoid fragmentation and inefficiencies, it is necessary to develop a coherent approach, while taking into account the specificities of the various sectors and policy domains. ENISA's advice, opinions and analyses aim at ensuring consistent, evidence-based and future-proof implementation, focussed on building up cyber resilience in critical sectors and supporting EU Member States in tackling new risks to the Union.

What we want to achieve

- Support the review of existing policies and to support the Commission and Member States in the development of new policies, by collecting evidence and data, with a view to addressing shortcomings and increasing the level of cybersecurity across the Union;
- Support a consistent technical cybersecurity approach to implement EU policies on risk management, security measures and incident reporting, in line with industry good practices and international standards, by developing a single cybersecurity framework.
- The continuing enhancement of cyber resilience across critical sectors in the EU, addressing gaps, new risks for the Union and emerging threats, by supporting coordinated risk evaluations and resilience stress tests.

Strategic objective. 'Effective Union preparedness and response to cyber incidents, threats and cyber crises'

Context. The benefits of the European digital economy and society can only be fully attained under the premise of cybersecurity. Cyberattacks know no borders. All layers of society can be impacted and the Union needs to be ready to respond to cyber threats incidents and potential cyber crises. Cross-border interdependencies have highlighted the need for effective cooperation between Member States and Union entities for faster response and proper coordination of efforts at the strategic, operational and technical levels. Understanding the ongoing situation is key to being effectively prepared and to be able to respond to cyber incidents, threats and crises.

What we want to achieve

- Technical and operational communities of the EU Member States are supported to cooperate in a secure environment in order to prepare for and respond to cyber incidents, threats, and cyber crises.
- Relevant stakeholders are informed, aware and understand current cyber threats, incidents, vulnerabilities and crises to effectively prepare and respond to them.
- Ability to scale up their capacity to support EU Member States and Union entities to respond to large-scale incidents, threats and crises in a rapid and agile fashion.

Strategic objective. 'Strong cyber security capacity within the EU'

Context. The frequency and sophistication of cyberattacks is rising steadily, while at the same time the use of digital infrastructures and technologies is increasing rapidly. The need for cybersecurity skills, knowledge and competences exceeds the supply. The EU is investing in building competences and talents in cybersecurity at all levels, from the non-expert to the highly skilled professional and across all sectors and age groups. ENISA addresses capacity building across the spectrum. It starts by investing in youth through competence building and training, whilst providing continuous upskilling and reskilling opportunities to professionals, to keep up with the fast-changing nature of cybersecurity. The focus is not only on increasing cybersecurity skill sets in Member States and contributing to the objectives of the Cybersecurity Skills Academy, but also on making sure that the various operational communities always possess the appropriate capacity to deal with the cyber threat landscape. Engaging closely with key players and multipliers in the EU is crucial to ensuring adequate preparedness across sectors and borders, effectively using the lessons learned from well-planned exercises.

What we want to achieve

- An elevated base-level of cybersecurity awareness and hygiene across the EU.
- An integrated approach to acquiring cybersecurity skills through relevant professional experience and educational structures to meet the demand for a workforce skilled in cybersecurity, contributing to the Cybersecurity Skills Academy.
- Well prepared and tested capabilities with the capacity to deal appropriately with the evolving threat environment across the EU.

Strategic objective. 'Building trust in secure digital solutions'

Context. Digital products and services bring benefits as well as risks, and these risks must be identified and mitigated. In the process of assessing the security of Information and Communication Technologies (ICT) products, services and processes and ensuring their trustworthiness, a common European approach covering societal, market, research and foresight, economic and cybersecurity needs is required, along with the possibility of influencing the international community by introducing a competitive edge. Using means such as cybersecurity-by-design, market surveillance and certification will allow us to both enforce and promote trust in digital solutions.

What we want to achieve.

- Provide citizens and companies with the assessment of assurance levels on digital solutions and enable trusted supply chains through means such as certification in the context of the European cybersecurity certification framework.
- Provide technical support for the implementation of a cyber secure digital environment across the EU, where European and national public authorities along with sensitive and critical businesses can meet regulatory obligations through the use of certified solutions.
- Help to boost the cyber resilience of digital solutions and of the single market by supporting the implementation and enforcement of the Cyber Resilience Act, as well as through an effective implementation of the European Cybersecurity Certification Framework, including the maintenance of existing European cybersecurity certification schemes.