INTER
INSTITUTIONAL
CYBERSECURITY
BOARD

**Ref: DECISION n° IICB/25/D007**

# Interinstitutional Cybersecurity Board (IICB)

## Annual Report 2025

The present document responds to the obligation of annual reporting due from the Interinstitutional Cybersecurity Board (IICB) respectively to the European Parliament and Council, and to the European Commission, pursuant to Articles 10(14) and 25(1) of Regulation 2023/2841.

This document was prepared by the IICB Executive Committee and, following a discussion during the IICB Meeting of 21 November 2025, submitted for approval by written procedure on 2 December 2025, and adopted with decision n° IICB/25/D007 on 16 December 2025.

INTER
INSTITUTIONAL
CYBERSECURITY
BOARD

# Contents

INTER
INSTITUTIONAL
CYBERSECURITY
BOARD

## Foreword by the IICB Chair

It is an honour for me, as the Chair of the Interinstitutional Cybersecurity Board, to present you with the Board's second annual report since the entry into force of the Regulation laying down measures for a high common level of cybersecurity at the European Union institutions, bodies, offices and agencies – the now called 'Union entities'.

We live in an increasingly tense geopolitical environment. Union entities are targeted by threat actors exploiting technical or human factors to advance their political or criminal agendas. Cybersecurity of the EU public administration remains a priority. Throughout the past two years, Union entities have been coordinating their efforts for strengthening their preparedness and resilience, adopting a comprehensive approach.

Let's have a brief look at what we already have achieved together.

Looking back, 2025 was a **highly operational and demanding** year. Union entities worked on consolidating and assessing their internal frameworks in line with the Regulation's milestones and deadlines. This included establishing a cybersecurity risk management, governance and control framework. It also encompassed conducting a maturity and risk assessment and taking appropriate risk management measures. The IICB stood by their side, supporting their efforts, providing guidance and facilitating reporting. All the milestones foreseen for 2025 were completed on time.

Focus was also placed on gathering lessons learnt and addressing the challenges Union entities faced while implementing the rules. Cooperation between the IICB and CERT-EU proved instrumental in that regard, opening a path towards continual improvement.

Let's be clear: the implementation of the Regulation is more than a box ticking exercise. It requires strategic cooperation to ensure all Union entities – regardless of their size, mission or existing cybersecurity mechanisms – are ready to face emerging threats.

A key challenge we seek to address is supply chain security and digital sovereignty. The IICB is evaluating the resilience of Union entities' ICT supply chain. As of mid-2025, Union entities can benefit from FREIA, a framework contract that enables them to outsource cybersecurity services and partner with actors in the private sector – mostly, European companies. At the same time, the IICB also seeks to establish a service sourcing mechanism that will allow less mature Union entities to benefit from the expertise and experience available across the block.

I am very proud of the efforts made by the whole community, their readiness to establish mutual trust, and willingness to cooperate and move forward together. Looking to 2026, we will continue to coordinate our approach to cybersecurity and the common threats we face, recognising the diversity among the Union entities, but also taking advantage of the benefits that it brings.

## Executive Summary

In 2025, the Interinstitutional Cybersecurity Board (IICB) continued to operate within an increasingly complex digital landscape, characterised by the emergence of new risks and threats. Union entities were consistently targeted by a growing range of threat actors, reinforcing the strategic importance of cybersecurity for the stability and resilience of the Union's public administration.

During the year, notable progress was achieved in implementing Regulation (EU, Euratom) 2023/2841. Union entities developed and implemented their cybersecurity risk management frameworks, completed maturity and risk assessments and enhanced their overall preparedness. These achievements showcase the growing maturity of Union-wide cybersecurity. At the same time, the experience and feedback shared regarding the implementation of the Regulation has provided the IICB with valuable lessons learnt, helping to refine future cooperation while taking into consideration the diverse operational realities within Union entities.

In parallel, the IICB placed particular emphasis on addressing supply chain security and strengthening Union entities' ICT environment, starting with the assessment of their potential overreliance on non-EU vendors. This strategic focus aims to reinforce the Union's technological sovereignty and ensure greater autonomy in its cybersecurity capabilities.

To maximise efficiency in times of competing budgetary priorities, the IICB also promoted service sourcing mechanisms and the establishment of shared services through CERT-EU's work on combined service offerings. Moreover, the interinstitutional framework contract for the procurement of cybersecurity professional services (FREIA) enabled Union entities to outsource such services from trusted private sector partners – predominantly within the Union. This collaborative approach has strengthened both operational capacity and cost-effectiveness across Union entities.

In parallel, under the steering of the IICB, CERT-EU continued to support Union entities in implementing the Regulation, notably in developing their risk management frameworks and assessing their cybersecurity maturity and risks. At the same time, it has been pursuing its data-centric development to be able to provide more tailored services to Union entities.

Looking ahead, the IICB is committed to supporting Union entities in addressing the complex threat landscape they operate in and achieving a high common level of cybersecurity. Through these efforts, it aims to ensure the long-term resilience, autonomy and credibility of the Union's public administration.

# Introduction

*"The EU must enhance its resilience, utilise current tools effectively, and develop new ways to confront these evolving threats stemming from state and non-state actors, both now and in the future."*[1]

Cybersecurity is fundamental to the European Union's stability, prosperity and the protection of its citizens. In an era marked by increasing geopolitical tensions, hybrid warfare and rapid technological change, safeguarding our digital infrastructure has become a strategic imperative. At the same time, new technologies present both opportunities and vulnerabilities, requiring the Union to strengthen its capacity to anticipate, prevent and respond to emerging risks.

Since our last report, the cybersecurity landscape has witnessed notable contextual developments, leading to the **emergence of new risks**:

- The **rapidly changing geopolitical context** that we must understand, interpret and continually adjust to,
- The sophistication and development of **new techniques and technologies** (notably artificial intelligence) used by threat actors, amplifying their offensive capabilities,
- Our **growing reliance on digital solutions** in communication and cooperation, expanding our attack surface,
- The **increasing complexity of digital solutions**, with the inherent risk of introducing technical or human vulnerabilities that can be exploited by our opponents,
- Shifts in the **global market**, raising concerns about digital sovereignty, supply chain security and stability, as well as overreliance on non-EU suppliers.

These risks translate to increased threats for Union entities, which remain highly attractive targets. According to the 2025 ENISA Threat Landscape,[2] organisations in public administration not only remain the most targeted sector but also the number of incidents affecting them **increased significantly**: **38% of all recorded incidents, compared to 19% in 2024**. At the same time, the CERT-EU Threat Landscape Report 2024[3] confirmed the need for Union entities to be alert to cyberespionage and/or prepositioning, especially in light of the rising interplay between geopolitics and cybersecurity. Supply chain security also demands significant attention.

CERT-EU deals with thousands of malicious cyber activities targeting Union entities or their peers every year. In 2025, CERT-EU analysed more than 800 such activities in depth. In general, CERT-EU issues approximately 180 **Threat Alerts** per year to Union entities on the basis of these analyses, including recommendations and lines of action. In 2025, this number was already exceeded in mid-November. On average, this corresponds to more than a threat alert every other business day. This requires

[1] ProtectEU: a European Internal Security Strategy
[2] ENISA Threat Landscape 2025
[3] CERT-EU - Threat Landscape Report 2024 - A Year In Review

resource-intensive efforts not only from CERT-EU but also from Union entities, as they need to look for signs of malicious activities in their ICT environments and swiftly act in case such signs are identified.

The number of reported **significant incidents** affecting Union entities dropped in 2025 compared to the previous year, with 8 cases confirmed as of early November for 2025. Although the number of such incidents may have decreased, Union entities still face a worrisome threat landscape in 2025. The number of CERT-EU's Threat Alerts reaching a historical high this year illustrates this.

In addition, since the beginning of 2025, CERT-EU has identified more than 30 **threat actors** directly targeting Union entities using over 160 different techniques. When it comes to **state-sponsored actors** targeting Union entities, CERT-EU has noted two concerning trends:

- they originate from diverse countries (at least four), indicating that Union entities are attractive targets in the geopolitical landscape,
- they successfully leverage diverse initial access techniques to breach Union entities (exploitation of vulnerabilities as zero-days, advanced social engineering, supply chain targeting, spear phishing using non-public Union entities information as lure), which makes detection and mitigation particularly challenging.

In conclusion, the threat level for Union entities remains **very high**, and **cybersecurity** continues to be **a priority**. Failing to continuously **address the full spectrum of constantly evolving threats** targeting our IT systems and staff, could lead to significant cybersecurity incidents disrupting business continuity, causing financial losses or leading to political, legal and reputational damages. The risk is further amplified by the unavailability of highly specialised human resources.

**Regulation (EU, Euratom) 2023/2841 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union** (hereafter 'the Regulation') is critical in that regard. 2025 marked the second year of its implementation; a highly operational year during which Union entities were called to enhance their cybersecurity posture by implementing the Regulation's requirements and achieving the first **tangible milestones**.

The IICB is called to showcase the progress made in the implementation of Regulation through annual reporting. Specifically:

1. Article 10(14) states that "*the IICB shall submit a report to the European Parliament and to the Council detailing progress made with the implementation of this Regulation and specifying in particular the extent of cooperation of CERT-EU with Member State counterparts in each of the Member States".*
2. Article 25(1) states that "*the IICB, with the assistance of CERT-EU, shall report to the Commission on the implementation of this Regulation. The IICB may make recommendations to the Commission to review this Regulation.*"

In accordance with paragraph 14 of Article 10 of the Regulation, the annual report shall *"constitute an input to the biennial report on the state of cybersecurity in the Union adopted pursuant to Article 18 of Directive (EU) 2022/2555".*

Considering the above, and with a view to simplification and reduction of the administrative burden, this annual report covers the topics pursuant to both Articles 10 and 25 of the Regulation.

## Methodology for the drafting of the report

The report draws from the lessons learnt and reflections resulting from the activities of the IICB during its second year, in particular the experience with the implementation of the Regulation and related guidelines by the Union entities and CERT-EU. It refers to the documents prepared with the assistance of the IICB Secretariat, such as Decisions and summary reports, and by the Executive Committee, such as the Multiannual Strategy of the IICB for 2024 - 2029.

# Progress, challenges and achievements in 2025

The sections below provide a thematic overview of the achievements and challenges of the IICB during its second year of operations. Further information is available in the Annex.

## 1. Following the letter and spirit of the Regulation – *implementation*

For the IICB and all Union entities, **2025 was an intense year** for the implementation of the Regulation with several milestones due.

Union entities relied for this exercise on the set of guidelines adopted by the IICB at the end of 2024[4], but also on the unfailing support of CERT-EU.

The first milestone regarded the establishment by each Union entity, by 8 April 2025 – and based on an initial cybersecurity review – of a **cybersecurity risk management, governance and control framework ('the Framework')**.

- ⇨ The results from the initial cybersecurity review provided a snapshot of the cybersecurity posture of Union entities and an initial overview of the principles, rules and roles in place in Union entities to ensure their cybersecurity. On this basis, Union entities prepared their Frameworks, including cybersecurity policies, standards, guidelines, notices, methodologies, process definitions and supporting tooling. The Frameworks also outline the steps foreseen in their evolution.

The second milestone under the Regulation was the completion by 8 July 2025 of a **cybersecurity maturity assessment** incorporating all the elements of each entity's ICT environment, in accordance with Article 7 of the Regulation. The IICB issued an additional guideline asking each Union entity to carry out a **cybersecurity risk assessment**, incorporating all the elements of its non-classified ICT environment by the same date.

- ⇨ This enabled the IICB to have an overview of the maturity level of Union entities against the different domains covered by the adopted maturity assessment guidelines, but also of their risk posture. While this exercise proved useful for Union entities, it also enabled the IICB to identify possible improvements for the assessment and reporting methodology itself[5].

The third milestone required Union entities to take, by 8 September 2025, appropriate and proportionate **technical, operational and organisational measures to manage cybersecurity risks** that were identified in their risk assessment.

- ⇨ While this milestone was not subject to specific reporting to the IICB, all Union entities are expected to address the identified risks in their upcoming cybersecurity plan.

[4] Decision n° IICB/24/D013 of the IICB approving guidelines on the framework, maturity assessment, risk management measures and cybersecurity plan, 6 September 2024
[5] See Section 2 below.

Finally, taking into consideration the outcomes of these milestones, each Union entity **will approve by 8 January 2026 their cybersecurity plan**, in accordance with Article 9 of the Regulation. Formally, these plans aim to increase the overall cybersecurity of each Union entity. In practice, they will also enable the IICB to identify strategic priorities at the interinstitutional level, focus its efforts accordingly, support in a more harmonised and tailored way all Union entities, and thereby contribute to reaching a high common level of cybersecurity within all Union entities.

Overall, Union entities have demonstrated the utmost diligence in implementing the Regulation and reporting to the IICB, but also a genuine desire to improve and to use the new tools it provides to generate synergies where feasible and benefit from existing interinstitutional experience.

## 2. Unity through diversity – *from challenges to opportunities*

The Regulation applies to all Union entities, providing a framework to ensure a **high common level** of cybersecurity across the Union administration. This shared framework is essential to protect the continuity and integrity of operations and ensure the resilience of the Union entities' large digital ecosystem. However, Union entities are highly diverse in terms of size, structure and mission.

This became even clearer in 2025 as implementation efforts intensified and Union entities reported on the results and processes they put in place to respond to the milestones. Their heterogenous estates, diverse attack surfaces, organisational approaches, internal governance arrangements, resource availability and technical capacity raised challenges. The IICB was called to strike an appropriate balance between common requirements and tailor-made adjustments.

With the first cycle of implementation close to completion, the IICB has already initiated a review to take into consideration the lessons learnt and to better address the specificities of Union entities. For instance, in the ongoing revision of the guidelines, the IICB deliberately sought to avoid the extremes of a framework that would be either too broad and generic, or too narrow and prescriptive. In 2026, within the Technical Advisory Groups for Tools and Methodologies and CERT-EU guidelines, Union entities will work together to capture their diverse needs, while still promoting convergence towards a high common level of cybersecurity.

This experience proves that Union entities' differences are a source of mutual learning and improvement. Exchanges between entities have been instrumental in identifying shared priorities and designing pragmatic solutions that can be adapted across diverse operational realities. Throughout 2025, they have already come together voluntarily in the IICB's Technical Advisory Groups to promote common approaches, information exchange and best practices:

- On Tools and Methodologies, to help Union entities benchmark their capabilities, anticipate future trends, make the best use of new technologies and stay ahead of the curve.
- On the Human Factor, to feed and stimulate exchanges amongst Union entities regarding expertise and resources for raising the staff cyber awareness and for training newcomers, management, IT staff and end users in cybersecurity.

Furthermore, in June 2025 the IICB initiated exchanges between Union entities on post-quantum cryptography (PQC). Led by the Commission, a working group open to CERT-EU and interested Union

entities was set, allowing for the exploration and enhancement of potential synergies. The ambition of the IICB is for this work to lead to a proposal on standards on cryptography, guidelines for the implementation of the new standards and migration, and communication and awareness raising initiatives.

The IICB is now looking towards the future: **enhancing cooperation between entities is a strategic priority** for 2026. The next step is creating additional opportunities for learning from other entities' experience and sharing best practices.

As such, we see that our differences stimulate exchanges, inspire complementary approaches that enrich our collective expertise and enhance our understanding of the core topics we are addressing all together. They spark the design of new ways to address cybersecurity challenges commonly and, ultimately, to raise the levels of maturity.

## 3. Adapting to the threat landscape – *enhancing resilience and preparedness*

In 2025, the cybersecurity threat landscape evolved significantly, presenting challenges that required enhanced coordination among Union entities. While the IICB's main focus was the implementation of the Regulation, a series of complex developments highlighted the need for strengthened collective resilience. For example, Salt Typhoon and related actors' targeting of telecommunications companies in the United States and the EU, also raised alerts for CERT-EU and Union entities.

The cybersecurity landscape facing Union entities is characterised by increasing sophistication and frequency of attacks. Key observations include identity-based attacks, which underscore the necessity of robust multifactor authentication measures. Moreover, the ongoing exploitation of software vulnerabilities highlights the critical need for proactive and timely patch management. The threat landscape is evolving towards more targeted and tailored attacks, which among others include social engineering tactics that exploit the human factor, highlighting the need for a culture of cybersecurity awareness and vigilance among staff as one aspect of a comprehensive defence strategy.

In addition, the IICB was called to develop a reactive approach to improve the preparedness and increase the resilience of Union entities. Efforts focused on securing internal and inter-entity communications, including recommendations for the systematic adoption of end-to-end encryption (to start with, for IICB and Executive Committee meetings) and the initiation of work on Post-Quantum Cryptography. Looking to 2026, the IICB is expecting CERT-EU to further develop good practices on the use of secure communication channels. Beyond that, the IICB will assess the feasibility of identifying dedicated secure communication channels for clearly identified use cases, based on existing or forthcoming Union initiatives, to be used across all Union entities but also with their counterparts in the Member States. These measures aim to strengthen the overall cyber resilience and autonomy of the Union's institutional ecosystem.

Parallel to these operational challenges, political instability and broader security concerns have refocused attention on the Union's technological dependencies. In alignment with the European Internal Security Strategy's emphasis that "*cybersecurity and technological sovereignty are closely*

*interlinked*"[6], the IICB began considering a forward-looking approach to address this dependency. This included exploring ways to leverage its mandate to support Union entities in assessing and mitigating IT supply chain risks.

CERT-EU in particular issued a request towards Union entities that would allow it to further develop its Full-Spectrum Adversary Approach[7] and analyse threats related to the growing geopolitical tensions and the digital supply chain in all its aspects. This work will remain a key priority for the IICB in 2026.

## 4. Finding synergies – *resources optimisation*

The optimisation and reinforcement of Union entities' resources are at the heart of their efforts for a high common level of cybersecurity. The European Internal Security Strategy[8], adopted earlier this year, points to the scale of the challenges: Europe currently faces a **substantial skills gap**, missing nearly **300,000 cyber experts**. This shortage directly affects Union entities.

In its Special report 05/2022, the European Court of Auditors observed that the overall level of preparedness of Union entities was not commensurate with the scale of existing threats. It was also noted that allocation of resources to cybersecurity varied widely among them with smaller entities operating with no dedicated cybersecurity experts, leaving them particularly exposed. At the time of the mid-term revision of the 2021-2027 Multiannual Financial Framework (MFF), the assessment performed for Union institutions concluded that cybersecurity staff would **need to increase by approximately 75% by 2027** to meet operational and strategic priorities. Yet, this ambition must be viewed in the broader context of the Union's many competing political and budgetary priorities. While the required resource increase may be difficult to achieve in the short term, the need for reinforcement has been reiterated in the proposal of the next MFF.

In parallel, enabled by the Regulation, Union entities, through the IICB, have adopted a pragmatic and collaborative approach to resource management with a focus on optimising, coordinating and service sourcing mechanisms. In 2025, the IICB played a central role in this process by promoting **a common approach and identifying synergies across Union entities**. Notably:

- Its common maturity assessment exercise allowed for the identification of the areas to which the resources should be allocated in the first place and where they can have the greatest impact.
- Its Technical Advisory Groups (TAGs) enabled joint work on competences, capabilities and resource optimisation. These groups promote efficiencies, reduce duplication and facilitate the exchange of expertise across Union entities.
- The progress made in the development – with the help of CERT-EU – of combined service offerings allowed Union entities to become sourcing partners and benefit from each other's well-developed service management practices.

[6] ProtectEU: a European Internal Security Strategy
[7] Further explained in section 5 below.
[8] ProtectEU: a European Internal Security Strategy

- The entry into force of the FREIA framework contract at the end of May 2025 made additional capacity available, enabling the procurement of external cybersecurity services. More than 70 Union entities now benefit from streamlined access to operational, advisory and capability development services and improve efficiency in resource use. FREIA serves as a first step towards coordinated procurement across Union entities.

These activities represent a concrete example of how collaboration and creative resource management can translate into practical gains for cybersecurity implementation. Building on these developments, the IICB will continue to explore joint procurement and shared service models to support Union entities in achieving their strategic priorities within existing constraints.

The resource gap in cybersecurity remains substantial, given the increased number and severity of attacks. Nonetheless, the actions taken by the IICB demonstrate determination and adaptability in the face of competing priorities. Through innovation and collaboration, the IICB and Union entities are constantly working to make the best of existing resources.

Promoting synergies and working together should remain a key objective for the IICB. Nonetheless, it may only partially compensate for the need of structural reinforcement with increased staffing and budget allocation, for which continued political support remains essential. The IICB is confident that upcoming political decisions will recognise cybersecurity as a key component for assuring the long-term resilience of Union public administration, also in light of the 2028-2034 MFF proposal made by the Commission which calls for the allocation of further resources in this critical area.

# 5. A Cybersecurity Service at the core of our action – *CERT-EU activities*

## a. Support for the assessments and risk management measures

In 2025, CERT-EU supported Union entities in achieving all the targets set by the Cybersecurity Regulation. Support was given through consultations, but also in dedicated posture improvement meetings. An even more extensive on-demand service was also performed for a limited number of entities. CERT-EU also released in 2025 a good practice document on risk management measures, serving as a starting point for Union entities to take the necessary steps to comply with Article 8 of the Regulation. Another good practice document was released for an initial Framework checklist. It is a supporting document with the objective to verify that all areas have been examined and covered, allowing entities to ensure that the necessary steps have been taken to establish the initial Framework.

Under the combined service offerings, ENISA joined forces with CERT-EU to embed their risk-assessment experience into a dedicated joint service. The pilot, which was focusing on providing support for using the ENISA methodology, started in December 2024 and was closed in July 2025. Two agencies participated in this exercise.

## b. Cooperation with counterparts in the Member States

CERT-EU is an active member of the CSIRTs Network. In 2025, CERT-EU participated in all official meetings of the Network, providing updates on its work and threat landscape observations. It also participated in CyberSOPex 2025, an exercise for testing the Standard Operating Procedures of the

Network. Moreover, CERT-EU regularly contributed to the deliverables and development of the Network, implementing strategic decisions in collaboration with other members. CERT-EU notified all significant incidents of Union entities to its respective national counterparts, as required by the Regulation. When relevant, CERT-EU engaged in *ad-hoc* collaboration for an exchange of views and best practices.

## c. Full-Spectrum Adversary Approach evolution

In 2025, CERT-EU started the implementation of its full-spectrum adversary approach (FSAA) initiative. The focus was placed on the organisation of knowledge bases and the development of data-centric practices, with the aim to better anticipate and detect how adversaries target Union entities, their supply chain and ecosystem. The first concrete implementation for Union entities was the release of the first FSAA deliverable, named My Threats, in September 2025.

## d. General status of calls for action and inventory information requests

In July 2025, CERT-EU issued an ad hoc request to all Union entities asking them to provide information from their respective ICT system inventories with the aim to support its mission and tasks based on data-driven understanding of Union entities' infrastructures and their risks profiles. CERT-EU leverages these data to enrich its threat intelligence and delivery of services, tailoring them to individual Union entities. CERT-EU is also working with Union entities on replacing a number of cybersecurity products in their environments, as requested in a Call for Action in February 2024.

## e. Enhanced Security Monitoring

CERT-EU has been developing its Security Monitoring service to ensure functioning outside of regular office hours when there is particular demand from Union entities. To establish a solid foundation for this service, CERT-EU conducted a pilot phase of the project in 2025.

## Overall assessment and conclusions

2025 was a highly productive year in the implementation of the Regulation. In a complex and continuously evolving threat landscape, the IICB focused on supporting Union entities in their efforts to reach a high common level of cybersecurity. All the milestones of the Regulation were met on time, which materialised in all Union entities having established their internal cybersecurity frameworks, assessed and reported on their cybersecurity maturity and progressed in the implementation of risk management measures. An enhanced cybersecurity posture for the Union's public administration is a tangible outcome of the Regulation and the IICB's work, and is an important step in Union entities' continuous and collective improvement process.

However, the work does not stop here. A strong cybersecurity posture requires constant effort and adaption to the threat landscape. Looking towards 2026, the IICB has an important mission: taking stock of Union entities' reporting on the progress made to date and evaluating their cybersecurity plans to identify synergies and priorities for common action. In parallel, it will also review and improve its guidelines, ways of working and reporting mechanisms in light of the lessons learnt from this first cycle of implementation. This work has already begun: the feedback received from Union entities points the IICB towards streamlining and ensuring consistency in its guidelines, while taking into consideration the similarities, but also the diversity, among the Union entities. The IICB will also look into the introduction of peer reviews to support this effort, taking inspiration from the methodology adopted under other cybersecurity-related regulations, such as the NIS2 Directive[9].

Emerging risks related to secure communications, supply chain security and sovereignty, already discussed in 2025, will also be at the forefront of the IICB's 2026 agenda. Considering the current threats and geopolitical context, this work will aim at strengthening the security of Union entities' ICT environment and addressing the full spectrum of threats they face through tailored guidance provided by CERT-EU.

We are aware that Union entities remain highly attractive targets for threat actors. Coordinated preparedness, incident response and crisis management are therefore crucial for enhancing Union entities' resilience. The IICB has an important role to play in supporting crisis coordination and preparedness. With this in mind, it will further develop and test its crisis coordination/cooperation mechanisms.

In early January 2026, with the submission of Union entities' cybersecurity plans, the first cycle of milestones foreseen by the Regulation will be completed. With this experience and valuable lessons learnt, 2026 will be a year of execution of Union entities' cybersecurity plans – an effort in which they can count on the facilitation and support from the IICB and CERT-EU.

[9] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) http://data.europa.eu/eli/dir/2022/2555/2022-12-27

# Annex I - Achievements and progress with the implementation of the Regulation in 2025

## 1. Administrative and organisational aspects

### a. IICB Meetings in 2025

In 2025, the IICB held three meetings: on 14 March (IICB5), 27 June (IICB6) and 21 November (IICB7). Notably, on 14 March, it tackled the establishment of the foundations for monitoring, discussing the IICB's monitoring framework, including scope, methodologies, and key metrics. It approved the Work Programme of the Technical Advisory Group on the Human Factor. The monitoring framework and the discussed Work Programme for the Technical Advisory Group on Tools and Methodologies were approved *via* written procedure. The IICB also exchanged on curtailing of Union entities' overreliance on non-European vendors.

On 27 June, the IICB held a discussion on the experience and feedback of Union entities on the implementation of the Regulation as well as a first discussion on the compliance measures related to the Regulation's Article 12, notably the format for communication as well as the timelines and implementation details for the different steps. It also mandated the Commission to lead work on Post Quantum Cryptography and keep the IICB informed.

On 21 November, the IICB tackled the issue of adapting to the evolving threat landscape. It also discussed and approved the statement of work for the TAG on Tools and Methodologies on a revised approach to maturity assessment, as well as the way forward on the review of the Article 5 guidelines. The Executive Committee presented its Strategic Orientations for 2026. The IICB also discussed the content of the present report.

### b. IICB Decisions in 2025

Throughout 2025, the IICB adopted several Decisions to ensure alignment with the **priorities** and the **deadlines** of the Regulation. In particular, in order to ensure a smooth functioning of the Technical Advisory Groups, for which a clear mandate is paramount, the IICB adopted the related work programmes. The IICB also approved its Monitoring Framework, aiming to provide clear guidance on indicators to monitor the implementation of the Regulation by the Union entities. Last but not least, following high level discussions focusing on experience with the implementation of the first iteration of the guidelines which the IICB adopted in 2024, the TAG on Tools and Methodology was tasked with a specific Statement of Work, to provide recommendations for the revision of the guidelines on cybersecurity maturity assessment.

Where necessary, those decisions were formalised as IICB Decisions, on top of the conclusions reflected in the meeting's summary reports.

Notable Decisions can be found below:

- Decision n° IICB25D005 on the approval of the IICB Monitoring Framework,
- Decision n° IICB25D006 on the approval of a new statement of work for the Technical Advisory Group on Tools and Methodologies.

# 2. Implementation of the Multiannual Strategy

## a. Strategic Objective 1 – Fostering cooperation of Union entities on the full cybersecurity spectrum

Towards the accomplishment of this Strategic Objective, the IICB reached the following targets in 2025:

### *i. Reporting on Technical Advisory Groups*

In 2025, the IICB approved the work programmes for the Technical Advisory Groups on Tools and Methodologies (TAM), and on the Human Factor (HF) (IICB5). In line with the work programmes, the Chairs of each TAG reported the progress made in their activities to the IICB (IICB7).

### *ii. Identification of common needs for cybersecurity solutions by Union entities*

In 2025, the IICB continued working to ensure efficient information exchange and discussions on the cybersecurity of Union entities, as well as to identify their main needs for the future. In that regard:

*Essential Eight Mapping*

The IICB endorsed a deliverable prepared by the Technical Advisory Group on Tools and Methodologies, mapping the Essential Eight maturity model to other methodologies for maturity assessment (IICB5). This mapping aimed to help Union entities using different models to better understand their posture under a common methodology and identify areas for improvement.

*Combined Service Offerings*

Combined service offerings enable the development of cybersecurity services (e.g., cloud app hosting, secure code reviews, penetration testing, awareness raising, risks assessments, etc.) which should help address the challenges faced by Union entities and improve their cybersecurity posture, while leveraging capabilities and expertise from more mature organisations. This allows for the enhancement of the collective cyber resilience of Union entities and for less mature Union entities to have turnkey, best-in-class solutions with the right security controls, configurations and tools. It also enables CERT-EU to deliver its services towards achieving a common cybersecurity baseline.

CERT-EU reported to the IICB on the state of play and evolution of combined service offerings, including the launch of pilot projects (IICB5, IICB6, IICB7). In 2025, multiple projects related to Combined Service Offerings (CSO) have progressed:

- Cloud app hosting: throughout the year, research was conducted both on the technical aspects as well as on the possible users.

- Domain Name System Resolver: in 2025, CERT-EU initiated the DNS-resolver project, did market research based on gathered requirements, selected a European based vendor and is currently finalising a proof of concept.
- Digital Workplace (DWP) as a Service: EC DG DIGIT has implemented a comprehensive and state-of-the-art workplace solution, 'DWP as a Service' (DWPaaS). The scope was clarified between CERT-EU and EC DG DIGIT throughout the year. In July 2025, this service was published internally in the EC DG DIGIT Service Catalogue.
- Code reviews: in 2024, CERT-EU launched 'Code Review' as a pilot product. The service is available to Union entities.
- Penetration testing: all operational and administrative processes are currently in place. The service can be used when needed.
- Risk Assessment: the pilot was closed in July 2025. Based on the pilot's feedback, ENISA and CERT-EU have agreed to set-up a follow-up initiative in 2026.

*Outsourcing cybersecurity professional services for Union entities*

The IICB took note of the new set of framework contracts (FREIA) for the procurement of external services for support and consultancy in the field of cybersecurity, capability building and advisory services (IICB6). Signed by the Commission in May 2025, FREIA allows more than 70 Union entities to benefit from partnerships with the private sector in a rational and optimised way.

These framework contracts define key roles and competencies in the cybersecurity field and enhance a common understanding across Union entities. Benefiting from and promoting successful achievements at the European level, these framework contracts were designed based on ENISA's European Cybersecurity Skills Framework (ECSF).

While following strictly the Financial Regulations for their set-up, a vast majority of these contracts were attributed to European suppliers. This showcases the quality and competence of the European industry in the field of cybersecurity but also supports its development.

In practice, this means streamlined access to technical operations services, support for policy implementation and advisory services and capability development services. This is undoubtedly beneficial for the implementation of the Regulation. It opens new avenues for optimising the use of Union entities' resources and enables the first stage of coordinated procurement. The IICB will work on this concept, which could support Union entities in finding the best solutions to meet their strategic priorities.

## b. Strategic Objective 2 – Providing strategic direction to CERT-EU and accompanying its development

Towards the accomplishment of this strategic objective, the IICB reached the following targets in 2025:

*Monitoring framework reporting mechanisms*

The IICB endorsed a monitoring framework, defining the scope, methodologies, and key figures and metrics for monitoring the implementation of the Regulation (IICB5; Decision nº IICB25D005). The framework represents an important step for the IICB, enabling it not only to perform its mission and task of supervising the implementation of the Regulation across Union entities, but also to assist them in enhancing cybersecurity.

In particular, the monitoring framework allows Union entities to compare their cybersecurity level to that of peers and receive guidance on how to prioritise their efforts and cybersecurity investments. It also enables the IICB to identify areas for improvements to the guidelines, as needed. Last but not least, the framework allows CERT-EU to determine which services are needed most for Union entities and adapt its service catalogue accordingly.

*Approval of CERT-EU AAR and WP*

In compliance with Article 11(a) and 11(i) of the Regulation, the IICB approved the Work Programme 2025 and Annual Activity Report 2024 of CERT-EU (IICB5; Decision nº IICB25D002).

## c. Strategic Objective 3 – Elevating cybersecurity posture of Union entities to the level of threat they face

Towards the accomplishment of this strategic objective, the IICB reached the following targets in 2025:

*Implementation of the Regulation*

Throughout 2025, the IICB supported Union entities in establishing their internal frameworks and meeting the main deadlines under the Regulation:

| Deadline | Regulation milestones | Status |
|---|---|---|
| **8 April 2025** | Based on an initial review, establish an **internal cybersecurity risk management, governance and control framework** | √ |
| **8 July 2025** | Carry out a cybersecurity **maturity assessment** | √ |
| **8 September 2025** | Ensure that appropriate cybersecurity **risk-management measures are taken** | √ |

CERT-EU reported on the progress made by Union entities in that regard (IICB6; IICB7).

*Feedback and lessons learnt*

As Union entities worked to meet the milestones of the Regulation within 2025, IICB members shared their experience with the implementation of the Regulation and the guidelines proposed by CERT-EU (IICB6). A dedicated workshop was held in September 2025 where Union entities gave feedback on the guidelines on maturity assessment. It was concluded that while the first maturity assessment exercise, conducted based on the Essential Eight model, was successful, there was room for improvement. The

heterogeneous estates, existing policies, and the very large and diverse scope among Union entities generated difficulties in applying a single model for reporting their maturity, especially given the degree to which other models have already been successfully integrated in the internal maturity management processes operated by some entities. As a result, the IICB assigned a new statement of work to the TAG on Tools and Methodologies, asking for a revised approach to maturity assessment and reporting, while taking into consideration the need for capitalising on the positive outcomes of the work already completed (IICB7).

*Cybersecurity awareness-raising*

The IICB contributed to the continuous development of cybersecurity education, skills, awareness-raising, exercise and training programmes in Union entities via its TAG on the Human Factor. Representing 31 entities, the TAG's 61 members met regularly to share their experiences, best practices and resources on training programmes and opportunities. Among others, they also received presentations on how to organise an awareness raising programme (ENISA AR-in-a-box); on cybersecurity training organised by the European Security and Defence College; on the training available in EU Learn.

In June 2025, the TAG also prepared and ran an interinstitutional phishing exercise among 36 Union entities[10]. On 1 October 2025, TAG members gathered in Brussels to kick off the European Cybersecurity Month by organising an interinstitutional event open to staff of all Union entities and streamed to the general public. On 26 November 2025, they met in person in Zagreb on the sidelines of the second Cybersecurity Awareness-Raising Conference – Empowering the Human Element, organised by ENISA.

*Harmonisation of tools and methodologies*

The IICB supported synergies and collaboration among Union entities through the work of its TAG on Tools and Methodologies – now counting 42 members from 20 Union entities. In line with the TAG's 2025 Work Programme, outputs included the Essential Eight Mapping tool (now available on CERT-EU's Agora platform), as well as work on the AWS and Azure cloud security guides and the Zero Trust Tools checklist. The collection of best practices in Artificial Intelligence (AI) and Post-Quantum Cryptography (PQC) is also ongoing. Members also discussed and received presentations on a variety of topics, including post-quantum computing, the Cloud Security Maturity Model and the DevSecOps pipeline.

*Common approach to post-quantum cryptography*

Looking to explore potential synergies between Union entities, the IICB initiated discussions on post-quantum cryptography (IICB6). The Commission proposed to lead this work, involving all key and interested stakeholders, including CERT-EU and volunteering Union entities. Under this initiative, a survey toward Union entities was launched and a dedicated working group was set-up to share knowledge and experience. It is the aspiration of the IICB that this work should ultimately lead to a

[10] Almost 98 000 emails were sent, inviting colleagues to click on a link and enter their credentials to access a simulated login page.

proposal on standards on cryptography, guidelines for the implementation of the new standards and migration, and communication and awareness raising initiatives.

*Curtailing of Union entities' overreliance on non-European vendors*

Responding to the evolving threat landscape, the IICB – with the support of CERT-EU – began to examine the topic of supply chain security and non-European dependencies of Union entities (IICB5; IICB6). This topic is to be further addressed in 2026.

## 3. Strategic orientations for 2026

Following the highly operational year in 2025, the IICB is set to reflect on its accomplishments and lessons learnt for improvement in 2026. The Executive Committee has provided Strategic Orientations to guide the IICB in prioritising its domains of work and effectively organising its efforts to address the challenges posed by the Regulation and strengthen the monitoring of its implementation. The focus will be on addressing the gaps and challenges identified in 2025, further securing the ICT environment of Union entities and further enhancing crisis coordination and cooperation.

## 4. Overview of upcoming deadlines for the Union entities

The Regulation sets obligations for Union entities as well as for the IICB to fulfil in 2026 and to prepare for 2027. These targets should be duly taken into consideration by the IICB in the conduct of its mission and activities for the upcoming year. In particular, the following milestone is present throughout 2026:

- **8 January 2026:** each Union entity shall approve a cybersecurity plan (Art. 9(1)).

Furthermore, 2026 will require preparatory work towards achieving the following 2027 milestones:

- **8 January 2027:**
  - the IICB shall adopt its annual report detailing progress made with the implementation of this Regulation and specifying in particular the extent of cooperation of CERT-EU with Member State counterparts in each of the Member States (Art. 10(14));
  - the IICB shall adopt its annual report, with the assistance of CERT-EU, on the implementation of this Regulation (Art. 25(1));
  - *(+ every two years thereafter): for the Commission to assess and report on the implementation of this Regulation and on the experience gained at a strategic and operational level to the European Parliament and to the Council (Art. 25(2));*
- **8 July 2027** *(+ at least every two years thereafter):* each Union entity shall carry out a cybersecurity maturity assessment incorporating all the elements of its ICT environment (Art. 7(1)).

# Annex II – Acronyms

| | |
|---|---|
| **AI** | Artificial Intelligence |
| **AAR** | Annual Activity Report |
| **AI** | Artificial Intelligence |
| **CERT-EU** | Cybersecurity Service for the institutions, bodies, offices and agencies of the Union |
| **CSIRT** | Computer Security Incident Response Team |
| **CSO** | Combined Service Offerings |
| **EC DG DIGIT** | European Commission Directorate-General for Digital Services |
| **DNS** | Domain Name System |
| **DWP** | Digital Workplace |
| **DWPaaS** | Digital Workplace as a Service |
| **ECSF** | European Cybersecurity Skills Framework |
| **ECSM** | European Cybersecurity Month |
| **ENISA** | European Union Agency for Cybersecurity |
| **FSAA** | Full-Spectrum Adversary Approach |
| **HF** | Human Factor |
| **ICT** | Information and Communication Technology |
| **IICB** | Interinstitutional Cybersecurity Board |
| **IT** | Information Technology |
| **MFF** | Multiannual Financial Framework |
| **PQC** | Post-Quantum Cryptography |
| **TAG** | Technical Advisory Group |
| **TAM** | Tools and Methodologies |
| **Union entities** | institutions, bodies, offices and agencies of the Union |
| **WP** | Work Programme |