

2024 REPORT ON THE STATE OF CYBERSECURITY IN THE UNION PANEL SERIES

FROM ASSESSMENT TO ACTION: COORDINATED RISK STRATEGY - EXPERTS PERSPECTIVES

1. INTRODUCTION

In December 2024, the European Union Agency for Cybersecurity (ENISA) released the [2024 Report on the State of Cybersecurity in the Union](#), adopted in cooperation with the European Commission and the [Network and Information Systems Cooperation Group \(NS CG\)](#), gathering all EU Member States to cooperate on cybersecurity strategic matters.

The report provides an in-depth assessment of the evolving threat landscape and highlights both the challenges and opportunities for strengthening cybersecurity across the EU. Among the key recommendations is the call to **develop a coordinated, EU-wide supply chain security strategy**, integrating risk assessments, certification schemes, and public-private cooperation mechanisms.

As part of its implementation process, ENISA has launched a series of **policy panels** throughout 2025 to translate the report's recommendations into actionable strategies.

One such discussion took place during the [ONE Conference](#) on 30 September 2025. This session brought together senior cybersecurity experts from industry, regulatory authorities, and international enterprises to discuss how ENISA's recommendations can be transformed into **practical, scalable approaches** for strengthening both **IT and OT supply chain resilience**.

This paper summarizes the main discussion points and conclusions from that event.

2. BACKGROUND

In December 2024, ENISA released the [2024 Report on the State of Cybersecurity in the Union](#). The report offers an in-depth analysis of the current challenges and opportunities for enhancing cybersecurity across the European Union.

The 2024 ENISA Report identifies **supply chain security** as one of the most pressing challenges for the EU's cybersecurity ecosystem. It highlights several interrelated issues:

- **Rising sophistication of supply chain attacks:** Threat actors are increasingly targeting both IT and OT environments through suppliers' software and hardware compromises, software update mechanisms, and identity provider abuse. These attacks exploit interdependencies between IT and OT environments and leverage advanced persistent techniques, rendering traditional defences inadequate.
- **Insufficient maturity and resources for supply chain cybersecurity:** Despite regulatory progress, many organizations, especially SMEs, lack dedicated budgets, personnel, and mature policies for third-party and supply chain risk management.
- **Fragmented implementation of cybersecurity standards:** While initiatives like NIS2, DORA, and EU certification schemes are advancing, their adoption across sectors and Member States remains uneven, undermining the consistency of supply chain protection.

In response to the identified challenges, the Report includes the following recommendation:

- Addressing supply chain security in the EU by **stepping up EU wide coordinated risk assessments** and the **development of an EU horizontal policy framework for supply chain security** aimed at addressing the cybersecurity challenges faced both by the public and the private sectors.

3. THE EXPERT PANEL

Panel Title: From Assessment to Action: Coordinated Risk Strategy.

Moderator: [Hans de Vries](#), Chief Cybersecurity and Operations Officer, ENISA

Panellists:

- [Aernout Reijmer](#), former CISO, ASML
- [Ilias Chantzios](#), Global Privacy Officer, Broadcom
- [Milena Rizzi](#), Head of Regulatory Directorate, National Cybersecurity Agency of Italy

The panel explored how ENISA's recommendation on coordinated supply chain security can move from policy formulation to operational implementation, with a specific focus on OT vulnerabilities, third-party risk management, and EU regulatory alignment.

The discussion focused on understanding unique OT vulnerabilities, legacy system challenges, and supplier cybersecurity. It also explored how to turn frameworks and assessments into actionable governance—balancing regulation with innovation and ensuring proportional, SME-friendly support.

4. KEY INSIGHTS

Disclaimer: The views and opinions expressed by the panellists are those of the individual experts and do not necessarily reflect the official position of ENISA.

Understanding OT vulnerabilities

Experts agreed that **OT systems pose security challenges**. Many OT systems were not **originally designed with cybersecurity in mind** and lack proper patching mechanisms or access controls. In such environments, **availability often outweighs security, creating persistent risk exposure**. In OT, uptime is the priority, which underscores the need for proper governance to ensure system security. Safety must coexist with cybersecurity. To maintain operational safety while implementing cybersecurity controls, clear governance structures and well-defined work agreements are essential. Panellists emphasized that **governance structures** are as essential as technical defences to bridge the security gap in legacy systems.

Translating assessments into action

Panellists highlighted that **risk assessments must lead to measurable outcomes**. Panellists invited to consider that risk assessment should be followed by concrete mitigation steps or resources prioritisation.

While sectoral efforts are progressing, **Europe still lacks common framework** to evaluate cross-sector supply chain resilience, particularly between hardware and software ecosystems. Developing shared indicators would support comparability, accountability, and EU-wide benchmarking.

Evaluating suppliers' cybersecurity posture

The importance of a **standardized and transparent supplier evaluation process** to reduce compliance costs and improve comparability has been a recurrent theme. A supplier that is unresponsive is often the one with weak controls. Experts called for unified assessment criteria to reduce compliance costs and improve comparability across sectors.

A proposed solution was the creation of a **shared platform** containing supplier cybersecurity histories, covering data flows, commitments, and performance. Such system would enhance operational picture and facilitate joint visibility across the EU, allowing both regulators and companies to respond faster to emerging supply chain threats.

Converting frameworks and standards into practice

The experts referenced multiple frameworks and standards, such as ENISA's ICT Supply Chain Toolbox, IEC 62443 (for OT), and TIA SCS 9001 (for ICT), applicable to supply chain security. While the ENISA Toolbox was praised for its flexibility, experts cautioned against overreliance on a single model. **"No single framework solves everything"**, one expert observed, advocating for flexible integration of multiple solutions.

The panel agreed that **framework interoperability and mapping** are key. Aligning existing standards with EU legislation would save organizations time and reduce duplication. Mapping what's already out there and showing an overlap, which ENISA could prepare, would be a game changer.

Regulation and innovation balance

Europe's strong regulatory environment fosters trust but can sometimes slow innovation. Experts emphasized the need for **a sustainable regulation** that evolves with technological advances. It was noted that maintaining **open dialogue between regulators and private actors** is vital for balancing security, practicality, and competitiveness. However, to build and maintain active relationships with authorities, an organization requires enough resources within its security structures.

Coordinated risk assessment and governance

Drawing from **Italy's experience with sectoral public-private partnerships (PPPs)**, the panel noted that structured collaboration enhances risk assessment consistency and information exchange. Experts emphasized that **collaboration between public and private sectors is essential as it provides valuable input for formal risk methodologies**.

On governance, experts discussed whether public institutions are sufficiently listening to private sector feedback and cautioned against introducing divergent national requirements that undermine EU alignment. It was also noted that **information sharing and reporting mechanisms are gradually improving under the NIS2 directive framework**, helping to close this coordination gap.

Supporting SMEs and Proportionality

The panel stressed that **proportionality** must underpin all cybersecurity policies. Experts noted that **regulators must engage with all stakeholders** to ensure balanced and informed policymaking. They also cautioned that if requirements are set too high, SMEs risk being excluded from supply chains, stressing the need to secure the supply chain as a system rather than penalize its smallest participants.

ENISA's and the NIS Cooperation Group ongoing work on **EU procurement guidelines** was cited as a positive step toward ensuring smaller vendors can meet cybersecurity requirements **in a scalable and cost-effective manner**.

5. CONCLUSIONS

The panel agreed that a key next step for the EU would be to advance from fragmented risk assessment efforts toward a more integrated and coordinated approach to supply chain security, encompassing both IT and OT systems.

Key takeaways include:

- **Governance and collaboration** are as important as technical solutions in supply chain security.
- **Flexible integration of existing frameworks** is preferred over creating new, isolated standards.
- **Transparency, simplification and proportionality** must guide policy design.
- **Public-private partnerships** and **EU-wide mapping of standards** can accelerate adoption and reduce duplication.
- **SME inclusion and resource allocation** are critical for systemic resilience.

In conclusion, the notion of "from assessment to action" represents a substantive principle, not merely a phrase. It encapsulates a collective commitment to **operationalizing cybersecurity across the EU supply chain**, balancing security, innovation, and competitiveness through coordinated governance, shared accountability, and a unified risk management culture.