POSITION PAPER

#FERMAFOCUS #DIGITALISATION

20 June 2025

Open Consultation on the Revision of the Cybersecurity Act: FERMA's Response

The Federation of European Risk Management Associations (FERMA) brings together 23 risk management associations in 22 European countries, representing over 6000 risk active in a wide range of organisations. Our response to the open consultation on the revision of the Cybersecurity Act reflects the perspective of risk professionals who contribute to the cyber-resilience of the EU economy, as they play a key role in anticipating, mitigating and securing insurance coverage for cyber risks, as well as in the reporting of cyber incidents.

1 On the simplification of cyber reporting obligations

European companies face an increasingly challenging environment, marked by the rising volume, complexity, and sophistication of cyber threats: since 2018, cyberattacks are considered as the most critical risk by Risk Managers worldwide (see: FERMA's *Global Risk Manager survey,* 2024).

However, EU companies are experiencing substantial administrative burdens due to disparate and often duplicated reporting obligations – and particularly for those operating across multiple EU Member States or sectors (see: FERMA's white paper *'Cyber Reporting Stack: Navigating EU Requirements'*, 2024). Compliance with varying notification timelines and procedures across different legislations significantly diverts resources away from actual cybersecurity risk management.

The complexity stems primarily from a multilayered landscape of EU cyber legislation (i.e., GDPR, NIS 2, DORA, Cyber Resilience Act etc.), each requiring businesses to reporting ICT-related incidents to different authorities (Data protection authorities, ENISA, CSIRT etc.) according to different, tight timelines. This is especially problematic, since it can lead to (i) confusion in determining the applicability and interpreting reporting requirements, (ii) resource misallocation when efforts would be best spent responding to the crisis, and (iii) substantial penalties in case of non-compliance.

To address this challenge, FERMA advocates for the establishment of a 'single-point-of-entry system' for cyber incidents reporting, allowing companies to report the incident once on a centralized EU-wide platform, which would then share the information with all relevant authorities. We also call for the harmonisation of timelines and definitions to ensure the consistent interpretation of EU legislation and reporting standards across member states.

2 On the mandate of ENISA

In FERMA's view, ENISA has an important role to play in enhancing the cyber resilience of the EU economy. We support any action by ENISA aiming to (i) build cybersecurity capacity, (ii) raise awareness and educate on cybersecurity, (iii) develop cybersecurity certifications and standards to elevate the cyber risk maturity of the EU market, and (iv) share knowledge and data about the cyber risks landscape. We call for ENISA to support industry stakeholder in the form of best practices and guidance to address both technical and non-technical cyber risks, in line with a multi-risk approach compatible with an Enterprise-wide Risk Management (ERM) methodology.

Moreover, we think that ENISA should contribute to building a shared EU situational awareness of cyber risks. In today's volatile cyber risk landscape, it is critical that all relevant entities share a clear vision of the EU exposure to cyber risks of all kinds. A shared EU situational awareness of cyber risks is therefore essential for an integrated, whole-of-government approach to cyber risk management and cyber incident response, itself the foundation for a cyber resilient EU which benefits citizens and businesses.

3 On the European Cybersecurity Certification Framework

FERMA calls for cyber risk management processes to be the topic of a dedicated European cybersecurity certification. Effective cyber risk management processes are an essential aspect of cybersecurity as they provide a system for an organisation to identify, assess, prevent and mitigate cyber risks, taking into account all the technologies, products and/or services produced, used and/or deployed by said organisation.

A cyber risk management certification would be a clear indicator for relevant stakeholders, such as business partners or insurance providers, that the certified organisation has robust cyber risk management practices in place, which will contribute to fostering trust in the market. Such a measure would also contribute to improving the insurability of cyber risks, risk and insurance managers are increasingly concerned that some of their activities might become uninsurable in the future, with cyber risks being perceived as a likely area where coverage might withdraw (see: FERMA's *Global Risk Manager survey,* 2024).

FERMA

The Federation of European Risk Management Associations brings together 23 risk management associations in 22 European countries, representing over 5600 risk managers active in a wide range of organisations. FERMA provides the means of co-ordinating risk management and optimising the impact of these associations outside their national boundaries on a European level.

www.ferma.eu

Contacts

Adrien Boudet
adrien.boudet@ferma.eu
Axel Grislin
axel.grislin@ferma.eu