Converging paths: EU operational resilience and cybersecurity laws

Counsel Camille Saettel, and Partner Sophie Sheldon, explore the overlaps between incoming operational resilience and cybersecurity laws in the EU.

19 August 2024

Information sharing
DORA, NIS2, CER and CRA support information-sharing among in-scope entities. It consolidates knowledge about threats and response strategies for a more secure cyber environment.

New European Union (EU) regulatory frameworks are emerging to tackle escalating digital-risk and cyber-defence challenges. Among them is the Digital Operational Resilience Act (DORA), the Network and Information Security Directive (NIS2), the Critical Entities Resilience Directive (CER) and the Cyber Resilience Act (CRA).

Each is aimed at enhancing the security and resilience of digital infrastructure in the EU. *"Don't be overwhelmed by the regulatory burden,"* says Camille. *"Their focus may be different, but these laws are complementary and interconnected, which means your compliance activity can cover multiple bases."*

DORA: Cybersecurity law focused on operational resilience

DORA is designed to boost operational resilience in the financial, insurance and reinsurance sectors, ensuring that entities can withstand and recover from internal, external and systemic cyber risks. DORA becomes applicable in Member States on 17 January 2025.

Like NIS2 and CER, DORA has extraterritorial reach, applying to entities outside the EU to the extent that they have activities within the EU.

Definition: Critical functions
A function whose disruption is likely to seriously affect the financial performance of a financial entity, the continuity of its activities, or its ability to comply with the conditions of its authorisation.

DORA is *lex specialis*, meaning that it prevails over NIS2. It addresses:

- **ICT risk management**: Entities must document and implement robust business-continuity plans to identify, manage and mitigate ICT-related risks in critical functions.
- **ICT incident reporting**: Entitles must report major ICT-related incidents to relevant competent authorities.

- **Digital operations resilience testing**: Entities must test their digital and operational resilience regularly.
- **Third-party risk management**: DORA is more sector-specific than NIS2, CER and CRA, but brings third-party service providers into scope. It requires them to meet the same standards of resilience. Entities must keep a register of ICT service providers, with full control over the supply chain for important and critical functions. Entities' reliance on outsourcing for ICT services, and interconnections between parties, were exposed, most significantly, by the global CloudStrike software outage on 19 July 2024.

Regulators and entities must adhere to DORA's proportionality principle by considering the size of the entity and the complexity of its services when defining risk exposures and remediation measures.

NIS2: Broad EU cybersecurity measures

NIS2 builds upon the original NIS Directive to strengthen overall levels of cybersecurity across the EU. It enters into force on 18 October 2024.

While DORA focuses on the financial sector, NIS2 is broader. It applies to entities within 11 critical sectors, identified by CER, which include energy, transport, banking, financial markets, health, digital infrastructure and space. Member States must draw up lists of "critical and important entities" within these sectors by 17 April 2025.

NIS2 mandates that critical entities adopt more robust cybersecurity measures and have business continuity, crisis management and supply-chain security policies in place. It holds management, and individuals acting as legal representatives to critical entities, liable.

NIS2 addresses cloud-based software-as-a-service (SaaS) applications, which are not covered by CRA. Like DORA, NIS2 requires entities to report significant incidents to relevant authorities.

CER: Risk management for critical entities

CER is designed to strengthen the resilience of critical entities that provide essential services across the same 11 sectors as NIS2.

Unlike DORA and NIS2, which focus primarily on cybersecurity resilience, CER addresses a broader spectrum of risks, including both man-made and natural hazards. CER goes beyond entity- and sector-specific vulnerabilities to include risks arising from supply-chain dependencies, as well as interdependencies with other Member States and third countries.

Measures apply from 18 October 2024. Member States have until 17 July 2026 to identify critical entities. And, once identified, critical entities have just 10 months to meet resilience requirements. *"Organisations need to think about whether they'll be designated as critical entities and plan ahead,"* says Sophie. *"Because we all know that 10 months isn't very long to turn compliance around."*

CRA: Securing the operational resilience of digital products

While the other regulations are sector-focused, CRA is product-focused. It seeks to establish common cybersecurity standards for hardware and software products with a digital element (PDE). The aim is to

secure PDE throughout its lifecycle.

Approved by the European Parliament on 12 March 2024, CRA enters into force within 20 days of publication. Reporting obligations for manufacturers will apply within 21 months. CRA's extraterritorial reach is yet to be determined.

CRA covers PDE that could be used to transmit data to connected devices or networks. But, unlike NIS2, CRA does not include SaaS. According to Camille: *"If SaaS were covered by CRA, it would ensure an enhanced level of cybersecurity for PDE. This, in turn, would facilitate compliance for entities within the scope of the NIS2 directive and strengthen security of the entire supply chain."*

The onus of compliance is on PDE manufacturers. They are required to implement processes to handle vulnerabilities and provide timely updates and patches. Cybersecurity features and risks must be transparent. Conformity assessments for critical PDE must be carried out by third parties. Meanwhile, importers and distributors must evidence a manufacturer's certificate of conformity before placing PDE on the market.

There are hefty penalties for non-compliance. Fines up to €15 million, or 2 per cent of global annual turnover, apply.

Overlapping EU cybersecurity laws deliver comprehensive response

Together, DORA, NIS 2, CER and CRA provide a comprehensive response to strengthen the EU's resistance against cyber-attacks and to support operational resilience for critical infrastructure and sectors.

Sophie urges companies not to consider the acts and directives in isolation. *"If you set up separate compliances programmes for each, you'll end up in a tangle. The work you do to comply with one regulation will support your compliance with others, provided you see them as something that comes together as a whole. Similarly, think about how the timelines for compliance interact, and make them work for you."*