Similarities and Differences Between NIS2 and DORA

Over recent years, the European Union has significantly strengthened its cyber-resilience framework through two major regulations: the NIS2 Directive and the Digital Operational Resilience Act (DORA). While both aim to limit the damage caused by cyberattacks and IT disruptions, they address different objectives and apply to distinct sectors.

For security and risk decision-makers, it is crucial to understand both the similarities and the differences between these regulations. This clarity enables smarter investment decisions, the design of robust governance models, and the prevention of compliance gaps that could lead to regulatory exposure.

Who is in scope for DORA and NIS2 compliance?

The Digital Operational Resilience Act (**DORA**) primarily targets the financial sector. Its rules apply to banks, insurance companies, payment service providers, investment firms, and other financial institutions governed by EU financial regulations. DORA also extends to critical third-party service providers that support these institutions, such as risk management software vendors and penetration testing firms.

In contrast, **NIS2** has a much broader scope, covering multiple sectors. It applies to essential entities like energy, transport, healthcare, and water supply providers, as well as important entities including manufacturers, digital infrastructure providers, and cybersecurity companies.

Unlike DORA, NIS2 is not limited to a single sector but instead focuses on industries crucial for the functioning of society.

What NIS2 and DORA Mean for Your Business?

With NIS2 and DORA, risk management becomes central to every organization's operations, as both regulations demand proactive identification and mitigation of cyber and operational risks. They also introduce greater responsibility, making leadership directly accountable for ensuring compliance and resilience. Organizations must implement the required measures or risk significant fines and sanctions, highlighting that mandatory compliance is both a legal and strategic necessity.

www.patecco.com | Lothringer Straße 36 | 44805 Bochum |+49 (0) 23 23 - 9 87 97 96 | info@patecco.com

NIS2 and DORA Similarities

Shared Focus Area	NIS2	DORA
Cybersecurity Standards	Requires strong technical and organizational measures to protect networks and information systems	Mandates robust security controls to safeguard financial systems
Risk Management & Governance	Establishes risk-based security management and executive accountability	Requires formal risk management frameworks and board-level oversight
Incident Reporting	Defines strict timelines for reporting significant cyber incidents to authorities	Imposes detailed and time-bound ICT incident reporting obligations
Operational Resilience	Focuses on ensuring service continuity for essential and important entities	Emphasizes digital operational resilience and system recoverability
Regulatory Oversight	Enforced by national supervisory authorities with sanctioning powers	Supervised by EU and national financial regulators with penalty mechanisms

NIS2 and DORA Differences

Aspect	NIS2	DORA
Type of Legislation	EU Directive that sets a minimum standard and must be implemented into national laws before it applies to companies	EU Regulation that directly defines mandatory requirements and applies immediately to organizations
Scope	Applies to essential and important entities across multiple critical sectors	Applies primarily to financial institutions and their critical ICT third-party providers
Focus and purpose	Strengthens overall cybersecurity and resilience of critical services across the EU	Ensures digital operational resilience specifically within the financial sector
Key Components	Cyber risk management, incident reporting, governance obligations, and supervision	ICT risk management, resilience testing, incident reporting, and third-party risk oversight
Compliance Approach	Risk-based and outcome-oriented, enforced by national authorities	Prescriptive and harmonized, with direct supervisory oversight

www.patecco.com | Lothringer Straße 36 | 44805 Bochum |+49 (0) 23 23 - 9 87 97 96 | info@patecco.com