ManageEngine

Double trouble or double defense: What NIS2 and DORA mean for finance

Resilience is the new compliance standard

In finance, risk is a language you speak fluently. But nowadays, risk isn't just market volatility—it's cyberattacks, cloud outages, and supply chain failures that hit faster than a flash crash. To rein in this digital fragility, the European Union (EU) has introduced two heavyweight compliance mandates:

Network and Information Systems Directive (NIS2): Focused on boosting cybersecurity across key sectors, including finance.

Digital Operational Resilience Act (DORA): Aimed at making financial institutions more resilient to IT disruptions.

These aren't duplicate rules—they're two sides of the same shield. And as a financial organization, you're expected to meet both. So the real question isn't why you need to comply—but how fast can you align?

The smart breakdown: NIS2 vs. DORA for financial entities

Category	NIS2 Directive	DORA Act
Nature	Directive—requires national transposition	Act—directly applicable across the EU
Applies to	All essential sectors (energy, health, finance, etc.)	Only financial entities and their ICT providers
Primary goal	Raise baseline cybersecurity standards across sectors	Ensure financial organizations can survive and bounce back from ICT disruptions
Risk focus	Cyber protection, incident handling, and supply chain security	ICT resilience, continuity, recovery testing, and vendor oversight
Board accountability	Mandated governance and accountability at the leadership level	Same as NIS2—explicit board oversight for resilience and incident preparedness
Third-party scrutiny	Expected oversight of service providers	Deep oversight—crucial scrutiny of ICT vendors and contractual resilience obligations
Reporting deadlines	Notify about incidents within 24 hours	Structured ICT incident and recovery reporting within strict timelines
Penalties	Up to €10 million or 2% of global turnover	Doesn't set fixed fines, but ICT providers can face daily penalties of 1% of their average global turnover for up to six months until they comply

Common myths about NIS2 and DORA

Myth 1:

If both NIS2 and DORA apply to you, complying with DORA alone is sufficient

While DORA takes precedence as a sector-specific regulation, it does not replace NIS2. Financial institutions must still comply with NIS2's general requirements, such as cross-sector cooperation and information sharing—where DORA does not provide full coverage. Full compliance means aligning with both frameworks, not just one.

For example, say a bank suffers a cyberattack that disrupts its internal communication systems. It follows DORA's incident reporting process and submits a report to the financial regulator. However, NIS2 requires reporting to national cybersecurity authorities and may also mandate coordination with computer security incident response teams and sectoral authorities, depending on the nature of the disruption. If the bank only reports the incident under DORA and does not engage with NIS2 mechanisms, it risks partial compliance.

Myth 2:

If I'm ISO 27001 certified, I'm automatically compliant with both NIS2 and DORA

While ISO 27001 can provide a strong foundation, it is not a substitute for NIS2 or DORA compliance. Both frameworks have specific legal requirements, such as reporting obligations, supervisory cooperation, and risk classification that ISO standards do not cover.

For instance, an organization may have well-documented controls and policies aligned with ISO 27001 but still lack a mechanism to classify ICT-related incidents according to DORA's severity levels or fail to meet the 24-hour initial reporting window mandated by NIS2. Similarly, ISO 27001 doesn't require engagement with national or EU-level supervisory bodies or sector-specific threat exercises. Regulators can view this as a gap—highlighting that ISO helps, but it doesn't tick all the boxes.

Myth 3:

Outsourcing IT or cybersecurity shifts the responsibility for NIS2 and DORA compliance to the service provider

Even if you outsource IT services, cloud infrastructure, or cybersecurity operations, your organization remains fully accountable for compliance with both NIS2 and DORA. These regulations make it clear that the obligated entity retains legal and operational responsibility for risk management, incident reporting, governance, and third-party oversight.

For example, under DORA, you must assess and monitor your ICT third-party providers, ensure contractual compliance, and report on their resilience posture. Similarly, NIS2 expects you to understand and control risks across your entire supply chain. Delegation is not exemption. Regulators will come to you—not your vendor—if something goes wrong.

Take a unified approach to dual compliance with ManageEngine

ManageEngine helps organizations comply with both NIS2 and DORA regulations by strengthening their overall IT governance, cybersecurity posture, and operational resilience.

How ManageEngine solutions help you comply

For NIS2 compliance	For DORA compliance
Implements strong access controls and network segmentation to secure critical systems.	Enforces privilege-based access and segregation of duties to control internal ICT risks.
Detects threats in real time and manages vulnerabilities across endpoints and infrastructure.	Integrates ICT risk into enterprise risk management and continuously assesses digital risks.
Maintains detailed audit logs and supports incident detection and reporting within deadlines.	Ensures incident impact analysis, reporting timelines, and root cause documentation.
Enables continuous monitoring and centralized visibility across network and information systems.	Enables advanced operational resilience strategies, including stress testing and simulations.
Supports governance policies and accountability across IT and operational technology systems.	Tracks compliance with risk frameworks and supports board-level oversight of digital resilience.
Aids in sector-specific threat response coordination and regulatory reporting.	Ensures monitoring of third-party ICT providers and manages outsourcing risks.

Discover how ManageEngine simplifies both journeys:
mnge.it/nis2 | mnge.it/eudora

In addition, ManageEngine solutions support regular testing of digital infrastructure and provide tools for maintaining compliance documentation and traceability across IT environments. By enabling visibility, control, and automation across diverse IT operations, ManageEngine assists businesses to meet both NIS2's cybersecurity demands and DORA's resilience and risk management requirements—helping them reduce regulatory risk while ensuring uninterrupted digital service delivery.

Disclaimer: The complete implementation of DORA and NIS2 requires a variety of processes, policy, people, and technology controls. Coupled with other appropriate solutions, processes, people controls, and policies, ManageEngine's solutions can help organizations align with DORA and NIS2. Organizations must do an independent assessment of ManageEngine's features and identify to what extent they can help them comply with these directives. This material is provided for informational purposes only and should not be considered as legal advice for DORA and NIS2 compliance. ManageEngine makes no warranties, express, implied, or statutory, as to the information in this material. Please contact your legal advisor to learn how DORA and NIS2 impact your organization and what you need to do to comply with DORA and NIS2.

ManageEngine
a division of Zoho Corp.

For more information:
www.manageengine.com | sales@manageengine.com