# Why DORA and Operational Resilience is also an Infrastructure Problem

## What DORA Means

Over 22,000 financial entities are subject to the EU's Digital Operational Resilience Act (DORA). Its core message is straightforward: financial institutions must be able to withstand, respond to, and recover from Information and Communication Technology (ICT) disruptions. The regulation is built around five pillars: ICT risk management, incident reporting, resilience testing, third-party risk management, and information sharing. DORA also carries enforcement weight: financial entities can face fines of up to 2% of total annual worldwide turnover, and Member State transposition regimes provide for individual penalties against senior management, with ceilings varying by jurisdiction.

DORA is the most prescriptive expression of a broader global shift. Regulators in the UK, the US, Singapore, Australia, and Hong Kong are converging on similar expectations around third-party oversight, operational continuity, and the ability to demonstrate resilience under real-world conditions. For institutions operating across borders, the challenge is architectural, not jurisdictional.

| | | |
|---|---|---|
| **50%** of institutions expected full compliance by end of 2025* | **46%** cite the Register of Information as their biggest hurdle* | **8%** fully compliant on resilience testing or third-party risk* |

## Where Things Stand

Deloitte's European Survey on DORA, provides granular public data on where the industry stands. The picture it paints is readiness is uneven. ICT risk management and incident reporting are furthest along, with more than half of institutions reporting 75%+ compliance. But resilience testing and third-party risk, the pillars that depend most on infrastructure capabilities, show only 8% full compliance on either. Nearly one in five entities remain at the early stages.

Third-party visibility is particularly weak. Thirty-eight percent of entities are still mapping their direct vendor connections. Only 1% have visibility beyond the second tier. Over half exclude third-party providers from incident response plan validation entirely.

*Data throughout this brief draws from Deloitte Digital Operational Resilience Act European Survey for Financial Services Entities

## The Infrastructure Question

A useful way to think about what makes DORA difficult is that the hardest requirements are not only governance problems. They are architectural problems. Each one resolves to what the underlying platform can observe, enforce, automate, and recover.

- Resilience testing requires environments that can be tested without disrupting production, automated failover, non-disruptive upgrades, and isolated recovery environments on demand.
- Exit strategies are supported by workload portability: the demonstrated ability to move critical applications between providers without refactoring or loss of security posture.
- Network segmentation must follow the application, not the network boundary. Forty-two percent of surveyed institutions identify segregation and segmentation of ICT systems as a significant DORA implementation challenge, second only to completing the Register of Information.
- Only 7% have identified the data sets needed to calculate economic impact per incident.

It is one thing to have resilience plans; it is another to show they have been tested, that dependencies are mapped, and that incident response works under real-world conditions.

## How a Unified Platform Addresses These Gaps

The Nutanix Cloud Platform solution provides a unified operating model designed to support hybrid estates across data centers, edge locations, and public clouds. Rather than layering compliance tooling on top of fragmented infrastructure, this approach facilitates resilience within the architectural framework.

| DORA Requirement | Platform Capability |
|---|---|
| **ICT Risk Management** | Unified control plane for visibility across hybrid estates. Architecture designed to support self-healing data availability and customer compliance programs. |
| **Incident Reporting & Resilience Testing** | Native monitoring and anomaly detection for incident telemetry. Automated remediation workflows. Testing and upgrade workflows designed to minimize production disruption. |
| **Third-Party Risk & Exit Strategies** | Hardware and cloud abstraction that supports workload portability across supported providers. On-demand migration tooling. Consistent Kubernetes® container orchestration software for containerized applications.. |
| **Information Sharing** | API-first architecture integrating with SIEM and SOAR platforms for real-time infrastructure data supporting threat intelligence sharing. |
| **Security & Encryption** | Software-defined microsegmentation for zero-trust policy enforcement. FIPS 140-2 validated data-at-rest encryption. Ransomware detection and containment capabilities designed to detect and contain ransomware activity. |
| **Disaster Recovery** | Tiered RPOs from synchronous replication to immutable cloud snapshots. Support for automated remediation workflows. Multi-site geographic redundancy.. |

## The Bigger Picture

DORA is a permanent elevation of ICT risk management to the boardroom. The institutions that navigate it most effectively will be those whose infrastructure facilitates the resilience, portability, and observability the regulation demands, rather than layering compliance processes on top of environments that were not designed for them.

There is also a strategic dimension worth noting. Resilience by design is a strategic approach that can enable companies to adapt and thrive in the face of adversity. Resilience does not have to slow innovation. Done well, it can help enable it.

For a detailed look at how the Nutanix Cloud Platform aligns to the architectural questions DORA raises, download our whitepaper: Building a Resilient Financial Services Infrastructure: DORA and Beyond.

Sources:

Deloitte European Survey on DORA, Q1 2025

Deloitte Operational Resilience Report, LSEG Financial Services Cloud Research

NUTANIX

info@nutanix.com | www.nutanix.com | @nutanix



WhyDORAAndOperationalResilienceIsAlsoAnInfrastructureProblem-FinserExecutiveBrief-FY26Q4-FY26Q4 07162026