5 Key Takeaways from the EU's Digital Operational Resilience Act (DORA)

IThe Digital Operational Resilience Act (DORA) came into effect on January 17, 2025, with extensive guidelines and a detailed regulatory framework for how all financial services entities doing business in the European Union ensure data resilience against unplanned disruptions. It also recognizes a reality broadly accepted by cybersecurity professionals that it is no longer a question of if a cyberattack occurs, but when. This crucial EU legislation brings a new level of rigor and accountability to the financial services industry that will continue to evolve to safeguard the stability of the EU and global financial ecosystem.

Many sectors of the financial services industry beyond traditional banks and credit institutions now fall under DORA regulations, including payment providers, investment firms, trading venues, insurance providers, and third-party information

and communication technology (ICT) service providers. Sectors that are new to this level of regulation may struggle to comply as indicated by European financial regulators' DORA "Dry Run exercise." They will also likely face additional scrutiny by interconnected customers, partners, and other stakeholders as a new operational risk.

Non-compliance no longer means just the potential for a very large fine but also reputational damage and liability for a company, its directors, and its partners.

Five Takeaways for Financial Services Firms from EU's DORA

While it remains to be seen how quickly financial regulators act, DORA represents a shift from guidelines for data readiness and cyber resilience to enforcement of it. Given the expansive nature of DORA, which significantly broadens the EU's financial regulation of information technology, European financial regulators, lacking unlimited expertise and resources, may face challenges enforcing all aspects of DORA immediately. As a result, regulators are likely to adopt a targeted approach, focusing on the most critical and visible areas of noncompliance.

Other things that every firm doing business in financial services needs to know about DORA:

1. **Five pillars:** This may be the most far-reaching regulation ever enacted. DORA's five pillars include:
    - Information and communications technology (ICT) risk management
    - Incident reporting
    - Digital operational resilience testing
    - Third-party risk management
    - Information sharing

2. **Broad impact across the ecosystem:** The breadth and depth of DORA is unprecedented. The act applies to banks, insurance companies, investment firms, and the like, but it also includes critical third parties. The objective is to ensure that risk stemming from increasing dependence on firms providing support and services, such as cloud service providers, ISVs, and payment processors, are addressed directly at the service provider level, rather than on an individual firm basis.
3. **Harmonizing and expanding existing regulations:** The first objective of DORA is to harmonize existing regulations across the EU. But it goes much further and dramatically expands regulatory coverage and requirements. For example, DORA introduces more stringent reporting requirements for cyber incidents and imposes strict timeframes for reporting.
4. **Enterprise-wide impact:** Unlike previous approaches to cybersecurity, compliance with DORA is not solely an IT issue. Firms must adopt an enterprise-wide approach, involving legal, compliance, risk management, as well as IT from the outset.
5. **Preparing for DORA compliance:** DORA is scheduled live as of January 2025, so financial services firms need to be working to ensure a smooth transition. It's crucial for organizations to implement the necessary changes.

Top "To-dos" for UK and EU OR Readiness: What Financial Organizations Are Prioritizing

One of the top priorities for DORA compliance is the submission of accurate and technically compliant registers of information. Submitting an accurate register that details the organization's most significant IT providers may be more beneficial than submitting incomplete information about all of its IT providers.

For data protection leaders and CIOs, DORA is a call to action to examine legacy systems and consider whether they are capable of withstanding today's cyber

threats and can deliver the performance required for efficient, rapid service recovery. Beyond identifying and mapping key systems, applications, and workloads with respective ICT providers, organizations should carefully consider the core capabilities that protect, defend, and recover these systems. Critical capabilities include:

- **Data protection and cyber recovery:** Rapid recovery capabilities are essential under DORA as a way to minimize the operational impact of an attack. For critical systems (e.g., payments), the only way to achieve the most stringent, ultra-short recovery time objectives required by operational resilience regulations is to recover using storage-based immutable snapshots. These snapshots should be securely stored in an isolated (or virtually air-gapped) repository.
- **Early-warning threat detection:** Identifying and remediating potential cyber threats earlier is an important aspect of data protection and readiness. The capability to continuously scan data to detect anomalies and identify threats like ransomware and malware in real time and automate remediation is essential for faster containment of an attack.
- **Isolated recovery environments (IRE) or cleanrooms for resilience testing:** Establishing a completely self-contained, isolated recovery environment where data can be restored for forensic and application analysis and validated as clean before returning to production speeds recovery. IREs also allow organizations to continuously test and improve cyber recovery practices for organizational readiness.
- **Scalability and performance:** Businesses will continue to evolve their services, face new regulatory requirements, and deal with emerging cyber threats. It’s important to consider a solution’s ability to scale as data requirements change across distributed, hybrid environments while maintaining high-performance speeds for data protection and recovery.

A Great Leap Forward for Regulation in the EU and UK

The EU's Digital Operational Resilience Act (DORA) along with resilience regimes from UK regulators (and others) represent a giant leap forward in regulation for the financial services industry. What's more, their implementation dates are drawing near, making preparation and action essential. Strengthening OR within the financial services sector is a necessary and laudable goal, but it will not come without great cost, both in terms of time and resources.

Compliance with Confidence

Organizations that delay establishing robust capabilities to meet DORA and other evolving resilience regulations, such as PSD2, NIS2, APRA CPS 230, and the European Cyber Resilience Act coming into effect in 2026, may find themselves with mounting challenges to overcome. They may also find themselves at a competitive disadvantage to firms that can demonstrate their ability to remain resilient in the face of disruptions in the global financial ecosystem. Working with partners who understand the regulation's resilience requirements and deploying robust solutions can help organizations ensure they are compliant and better prepared to meet new regulatory challenges and defend their data environment against emerging threats.

Pure Storage and Commvault have come together to build a joint solution, modular in design, that helps financial institutions enhance their cyber resilience practices and address key pillars of DORA for incident response and resilience testing. The solution is built by integrating the leading cyber resilience capabilities of Commvault® Cloud with the highly secure, high-performance Pure Storage platform. Learn more about the solution and our commitment to cyber resilience in this solution brief.

Are You Cyber Ready?

Readiness reflects mature cyber resilience, where technology, people, and

processes work seamlessly to enable business continuity in the face of any cyber challenge. Evaluate your organization's cyber resilience with Commvault's Cyber Maturity Assessment.

To learn more, download our white paper, "Strengthening Operational Resilience in Financial Services," or contact us for a free expert consultation.