Beyond Compliance: rethinking Digital Literacy through DORA

White Paper

Ana Luísa Mestre

September, 2025

firmc.nl

DORA's Wake-Up Call: a New Era for Financial and Risk Leaders

The digital landscape is evolving rapidly, and for the financial sector, the stakes have never been higher. Digital Operational Resilience Act (DORA) is not just another regulation; it is a game changer in how financial institutions look at digital risk and security. But why does DORA matter? At a broader level, besides promoting stability and regulatory harmony across the financial system, DORA allows organizations to gain competitive advantage in the market.

Understanding DORA: a Concise Look at its Background and Purpose

It is undeniable: we live in a world where digital transformation is happening faster than ever before. On the one hand, advances in technology and AI are driving the constant creation of new products and services. On the other hand, new technological developments open space for more sophisticated cyberattacks and hackers, threatening cybersecurity and society. When it comes to financial institutions, what they represent, and the personal data they store, it is even more urgent to guarantee their protection. According to the 2024 Global Financial Stability Report, produced by the International Monetary Fund (IMF) (1), over the past two decades, the financial sector has suffered over 20000 cyberattacks (left plot of Figure 1), resulting in a staggering $12 billion loss (right plot of Figure 1).

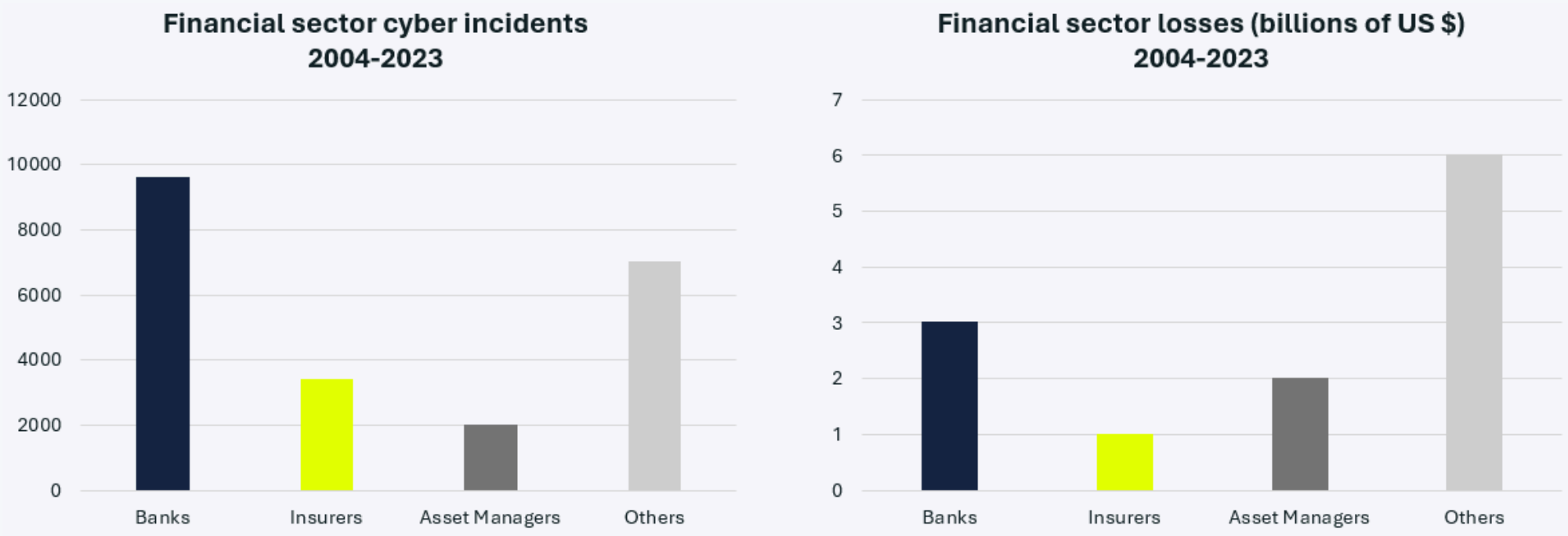


Figure 1. Financial sector losses and cyber incidents. Source: IMF.

The financial sector is very dependent on technology and collaborates a lot with tech partners, which makes it more vulnerable to cyber-attacks. In this landscape, DORA emerges as a strategic response to today's realities (2), calling for a profound shift in how cybersecurity is governed (3).

DORA is a new regulation introduced by the European Union and applicable to nearly all types of firms in the financial sector (e.g.: banks, investment firms, insurance companies) and Information and Communication Technology (ICT) third-party service providers (e.g.: managers of alternative investment funds; crowdfunding, cloud-service, and crypto-asset service providers) (4). Its goal is to ensure that all entities within the EU's financial system resist, respond to, and recover from cyberattacks or critical failures that occurred from ICT incidents. These incidents can target different assets, according to an article published by European Network and Information Security Agency (ENISA) on the digital threats within the financial sector (5), as shown in Figure 2.

Figure 2. Impacted assets from incidents in European financial entities (Jan/2023-Jun/2024). Source: ENISA.

Figure 3 outlines the main milestones regarding DORA implementation. Its first draft was published in 2020, and by early 2025 it had come into full effect, signaling the point at which financial institutions were expected to be fully compliant (6).

Figure 3. DORA Implementation Timeline. Source: European Insurance and Occupational Pensions Authority (EIOPA).

To be compliant with this new regulation, organizations must follow the six fundamental pillars of DORA (7), highlighted on Table 1.

Table 1. Pillars of DORA Compliance.

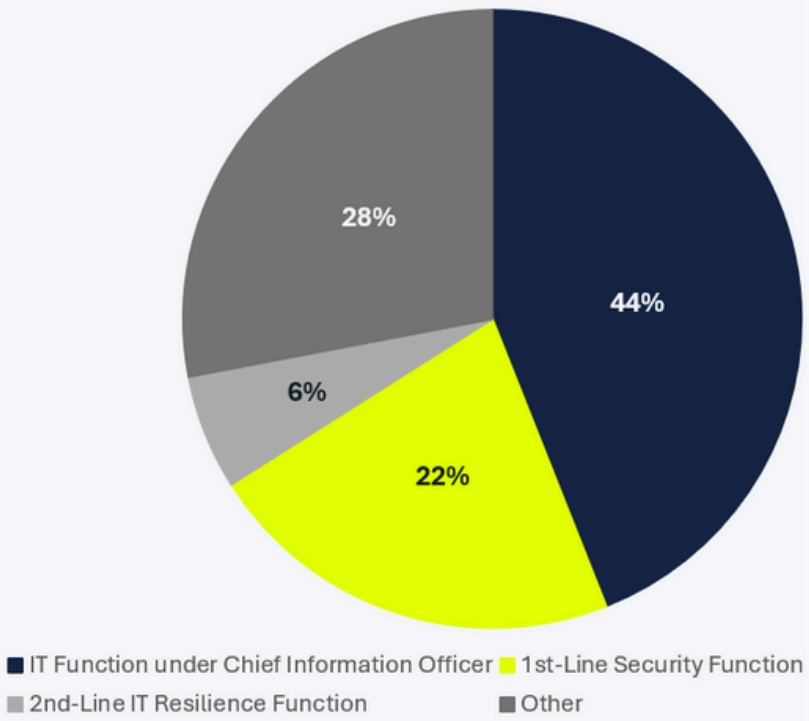
Pillars	Requirements	Practical examples
ICT Risk Management and Governance	• Implement an ICT Risk Management framework (identify, protect, detect, respond, and recover from cyber-attacks). • Regularly assess ICT risks and adapt their defense mechanisms to manage threats effectively.	• Perform regular risk assessments on core banking systems. • Implement layered cybersecurity using appropriate tools (e.g.: Security Information and Event Management (SIEM) tools [a]).
ICT-related Incident Reporting	• Report cyber and ICT-related incidents to competent regulatory bodies, affected clients, and partners.	• For banks, notify the Dutch Central Bank (DNB) within 24 hours after detecting a data breach affecting customer data.
Digital Operational Resilience Testing	• Carry out regular tests on ICT systems to assess their defenses and identify vulnerabilities.	• Simulate Distributed Denial-of-Service (DDoS) attacks [b] and phishing scenarios. • Participate in Threat-Led Penetration Testing (TLPT) [c].
ICT Third-Party Risk Management	• Guarantee that risks associated with ICT providers and subcontractors are thoroughly managed.	• Assess the risk-exposure of using outsourced Know Your Customer (KYC) software. • Ensure cloud vendors like Azure or AWS meet regulatory standards.
Information Sharing	• Foster collaboration through threat intelligence sharing.	• Join and actively contribute to Financial Services Information Sharing and Analysis Center (FS-ISAC) [d] or local threat-sharing initiatives. • Share anonymized threat data with sector peers.
Oversight Framework	• Supervise structure for key external ICT service providers.	• Monitor outsourcing arrangements through detailed SLAs, KPIs, and regular compliance reviews. • Appoint a vendor risk officer to oversee relationships with fintech providers or IT service partners.

Besides following DORA's main pillars, Firm C defends that one size does not fit all, meaning that organizations should scale and adapt these requirements to their business's size, complexity, and risk profile.

In June 2024, McKinsey & Company carried out a series of studies on the implementation of DORA (8) concluding with the following two key findings:

[a] SIEM tools combine security information management (SIM) and security event management (SEM) to enable real-time analysis of security alerts generated by applications and network hardware.
[b] Malicious attempts to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of internet traffic.
[c] Framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat. These enhanced security tests are reserved for financial entities whose failure would have systemic effects, and which are most likely to be targeted by malicious actors.
[d] Non-profit corporation established in 1999 that helps assure the resilience and continuity of the global financial services infrastructure.

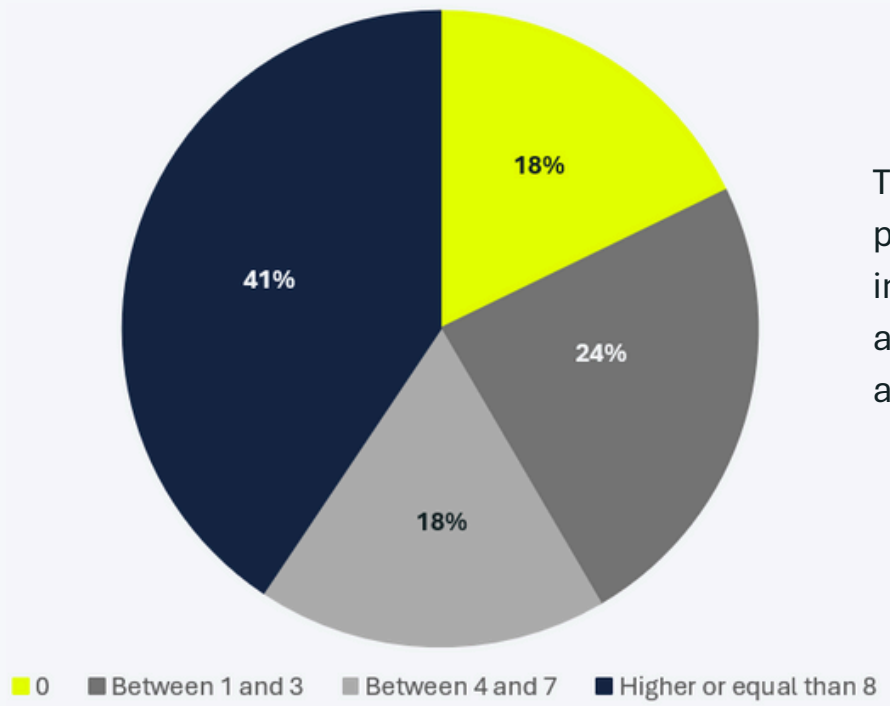
1. Responsibility for ensuring compliance with DORA often falls within the IT department's remit (Figure 4).



Approximately half of organizations still approach DORA as a purely technical or compliance challenge, focusing on cybersecurity, systems, and resilience infrastructure (categories IT Function under Chief Information Officer and 2nd-Line IT Resilience Function). In opposition, others see it more holistically, recognizing that DORA is also a cross-functional transformation that affects strategic governance, risk culture, and operational processes beyond IT alone (categories 1st-Line Security Function and Others). This growing awareness proves that DORA is more than a tech challenge; it is an organization-wide shift that requires alignment across risk, compliance, and operations, touching every layer of an organization.

Figure 4. Organizational function responsible for alignment with DORA, % of respondents (n=18). Source: McKinsey survey on DORA program readiness, 18 executives and DORA program leaders from leading EU financial institutions and ICT providers, Mar 2024.

2. Companies dedicated varying numbers of full-time employees to their DORA-compliance programs (Figure 5).



This insight shows that organizations are divided into how they perceive and prioritize DORA. While some are proactively investing in dedicated teams to embed operational resilience across the business (around 41%), others may risk falling behind as deadlines approach (around 18%).

Figure 5. Number of full-time employees dedicated to DORA program, % of respondents (n=17). Note: Figure do not sum to 100% because of rounding. Source: McKinsey survey on DORA program readiness, 18 executives and DORA program leaders from leading EU financial institutions and ICT providers, Mar 2024.

DORA at Crossroads: Challenge Meets Opportunity

Firm C believes that DORA must be seen simultaneously as a challenge and an opportunity for financial institutions. While there are currently some challenges that need to be addressed and planned for, resolving them will better position organizations to tackle more complex requirements and ultimately gain a competitive edge in the market.

As financial institutions work toward achieving DORA compliance, they are likely to encounter several key challenges. For each of them, Firm C not only identifies opportunities for use cases but also partners with clients to help them navigate this new regulatory landscape with confidence (Table 2).

Table 2. Challenges vs. Opportunities of DORA.

Challenges	Opportunities
Complex and constantly evolving digital ecosystems • Analyze what processes, frameworks and technologies are currently built within companies and the development of cyber threats demands coordination, expertise, adjustments across departments.	**Enhancing collaboration and information sharing** • By sharing insights with industry peers and stakeholders, organizations build a resilient ecosystem and foster a unified European financial landscape.
High costs involved • Investments in cybersecurity, infrastructure, tools and workforce bring security and stability. Failing with compliance may involve fines, operational restrictions, or reputational damage.	**Skill enhancement and other consequent boosts** • By investing in skills development (e.g.: cybersecurity, data protection, incident response), organizations can, in the long-term, use process mining to measure process execution, improve decision-making, and reduce the number of incidents and costs.
Third-party dependencies • Financial institutions have less control over some processes because they are very dependent on third-party providers for critical operations and technological services.	**Strengthening vendor management** • By reporting changes more often, and conducting regular audits, performance assessments, and contingency plans, organizations guarantee a proactive operational resilience risk management strategy from all parties.
Complex legacy systems[a] • Poorly understood patchwork of legacy systems may not be aligned with digital resilience standards of the organization's internal governance and control framework.	**Modernization of legacy systems** • By collaborating with technology partners to upgrade or replace outdated legacy systems, organizations ensure alignment with DORA resilience standards.

In the long term, it is critical that there is monitoring and continuous improvement, preventing future fines associated with new developments in the regulations. DORA compliance is not a one-time effort but an ongoing commitment (9).

[a] Older software, hardware, or technology platforms still in use and often critical to operations but built on outdated architectures or programming languages (e.g.: on-premises ERP systems; fax and paper-based systems; excel-based systems; point-of-sale (POS) systems).

Escrow Software: an invisible and critical piece of the DORA compliance puzzle

Under DORA, financial entities must ensure business continuity and operational resilience, even if a critical ICT supplier fails or goes out of business. Financial institutions must then have strategies for critical third-party providers, including, for example, data/software access in case of emergencies. This is where Software Escrow agreements come in: a continuity safeguard for software dependencies and an exit strategy for financial institutions, in case of emergencies, where a third party securely holds source code and documentation, releasing it to the client if the vendor can no longer provide support (10).

Table 3 illustrates how Escrow supports DORA and why it should be considered in the path for compliance (11).

Table 3. Relating DORA with Escrow Software.

DORA Requirements	Benefits of considering Escrow
Third-party risk mitigation and management	It ensures continuity even if an ICT provider fails.
ICT asset availability	If a vendor disappears, the financial institution can still run, maintain and migrate the system.
Audit and compliance	It can serve as a documented control measure during DORA compliance audits.

Why is Firm C the perfect choice to tackle DORA?

At Firm C, we combine deep regulatory expertise with a pragmatic, data-driven approach to help financial institutions navigate the complex DORA landscape and build resilience where it matters most.

Table 4. Firm C's strengths and actions for DORA Compliance.

Strengths	Actions
Laser-focused on the same domains DORA targets	Bringing a rare combination of domain expertise in Finance, Risk, and Data at the heart of DORA's regulatory framework.
Hands-on, pragmatic approach	Helping organizations implement what DORA requires on the ground, through practical solutions and operational changes.
Independent and agile	Offering agility and independence, tailored solutions, and attention at every step – what our clients need to stay compliant and competitive.
Strategic and long-term vision	Seeing DORA not as a cost, but as a catalyst for building trust, operational strength, and digital literacy, aligning compliance with business goals.
Alignment with Firm C's mission	Navigating this complex regulation with clarity, direction, confidence, and a pragmatic approach.

Conclusion

Firm C believes that DORA compliance should not be seen as an IT Project, but rather as a strategic, enterprise-wide initiative (12).

Before DORA, financial institutions addressed operational risk mainly by setting aside capital to absorb potential losses, a method that did not fully capture the broader dimensions of operational resilience (13). Now, this regulation brings with it the opportunity for organizations to modernize technological infrastructures, increase customer confidence, gain competitive advantage, and incorporate resilience processes in other frameworks like General Data Protection Regulation (GDPR) and Network & Information Security (NIS2) Directive, reducing costs and duplication (14). For these reasons, it is essential that organizations proactively ensure timely readiness for DORA. Early compliance isn't just about avoiding penalties; it streamlines transformation, reduces future costs, and positions firms as leaders in operational resilience.

While this regulation brings much-needed harmonization and clarity, it also introduces complex implementation challenges. For Firm C, however, the financial sector can embrace technological innovation while counting sophisticated cyber threats.

We are committed to helping our clients navigate this new landscape for financial institutions, building resilient, trustworthy financial systems. By connecting regulatory understanding with practical, cross-functional execution, we can help you comply with DORA's stringent requirements regarding risk management, incident reporting, digital resilience testing, and oversight of third-party ICT service providers. This is how we step in to help organizations define a tailored approach for their business, assessing readiness, scale capacity, and build sustainable compliance frameworks.
Need help assessing your DORA compliance readiness? Get in touch with our experts!

References

(1) Fabio Natalucci, M. S. (April de 2024). Rising Cyber Threats Pose Serious Concerns for Financial Stability. Obtido de https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

2) Team, T. (January de 2025). The EU's DORA regulation: definition, timeline and tips for compliance. Obtido de https://tresorit.com/blog/dora-regulation-definition-timeline-and-tips-for-compliance/

(3) Koopman, C. (March de 2024). A digital edge for financial services: Navigating cybersecurity in the era of the Digital Operational Resilience Act (DORA). Obtido de https://www.capgemini.com/insights/expert-perspectives/a-digital-edge-for-financial-services-navigating-cybersecurity-in-the-era-of-the-digital-operational-resilience-act-dora/

(4) Grabski, S. (s.d.). DORA: Why it is relevant to you. Obtido de https://www.pwc.pl/en/articles/dora-why-it-is-relevant-to-you.html

(5) Cybersecurity, E. U. (Jan 2023 to Jun 2024). ENISA Threat Landscape: Financial Sector.

(6) Expert, C. (March de 2024). Digital Operational Resilience Act (DORA). Obtido de https://blog.httpcs.com/en/reglementation-sur-la-resilience-operationnelle-numerique-dora/

(7) Authority, E. I. (s.d.). *Digital Operational Resilience Act (DORA)*. Obtido de https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

(8) Company, M. &. (June de 2024). Europe's new resilience regime: The race to get ready for DORA. Obtido de https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/europes-new-resilience-regime-the-race-to-get-ready-for-dora?utm_source=chatgpt.com

(9) Thompson, A. (February de 2024). Eight challenges organisations face with DORA. Obtido de https://www.northdoor.co.uk/insight/blog/dora-challenges-organisations-face/

(10) Kane, R., & Kaelble, S. (2025, August). Software Escrow, Escode Special Edition. Retrieved from file:///C:/Users/ana_m/OneDrive%20-%20NOVAIMS/Desktop/escrow%20software/Intro_Escode%20Solutions%20.pdf

(11) England, B. o. (2024, November). Outsourcing and third party risk management.

(12) Education, I. (May de 2025). Understanding the Global Impact of the Digital Operational Resilience Act DORA. Obtido de https://www.youtube.com/watch?v=Ymg7sLk_yDQ

(13) DORA | Updates, Compliance. (s.d.). Obtido de https://www.digital-operational-resilience-act.com

(14) Bustos, E. S. (July de 2025). *What is the DORA Regulation and why is it key for financial companies?* Obtido de https://www.apolocybersecurity.com/en/blog-posts/que-es-dora-y-por-que-es-clave-para-las-empresas-financieras