Blog Post

N° 1/2025

DORA – Status Quo 2025

From the regulatory idea to implementation in practice

Dr. Andreas Windisch

ASQUARED

asquared Blog Post N° 1/2025

September 2025

The Digital Operational Resilience Act (DORA) has been mandatory since January 2025. Banks, insurers, payment service providers, and FinTechs must demonstrate their resilience against IT disruptions and cyberattacks. While major players are making progress, many smaller institutions are still struggling with practical hurdles. Where do we stand? What are the challenges? What are concrete recommendations for action?

DORA in 2025

In September 2020, we reported on the EU Commission's proposed regulation on digital operational resilience in the financial sector – DORA for short. Today, five years later, the regulation is a reality, the transition periods have expired, and companies must deal with the requirements in their daily lives. The following figure shows the key milestones from the publication of the draft to the current and upcoming implementation requirements.

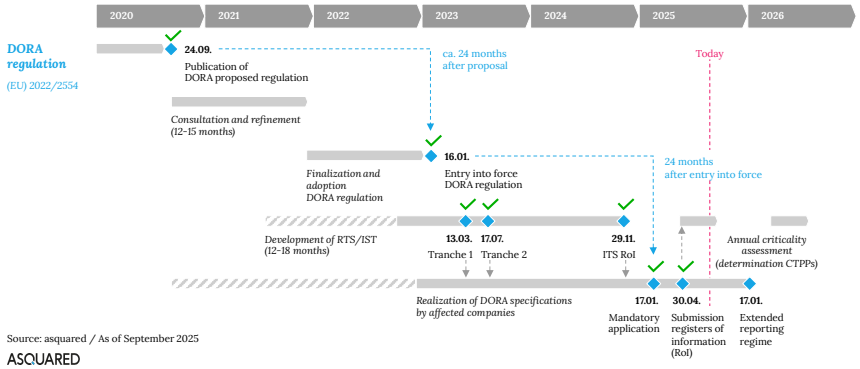

Figure 1: Detailed DORA timeline (as of September 2025)

The implementation obligations have been binding for all affected financial institutions since January 17, 2025. With the expanded incident reporting obligations starting in January 2026, further regulatory requirements are imminent. But where are we today in terms of practical implementation?

Current status of DORA implementation in practice

More than six months after the deadline for mandatory application, a significantly different picture emerges. Large banks and insurance companies have often been able to build on existing regulatory frameworks such as BAIT, VAIT, or EBA guidelines. They

have expanded their governance structures, clearly defined responsibilities at the board level, and formalized processes for incident reporting and IT risk management. For them, DORA is now generally a topic anchored in regular management supervisory meetings.

Medium-sized financial service providers, payment institutions, and investment firms, on the other hand, are in an intensive transformation phase. Although many have established project structures, they are still struggling with the full integration of monitoring tools, the implementation of automated incident reporting, and the adaptation of their outsourcing contracts. Transitional solutions are often still in place, where incidents are detected but not reported with the speed and quality required by DORA.

Smaller institutions and FinTechs face the challenge that DORA compliance is disproportionate to their existing resources. Specialist staff for cyber and resilience issues is scarce, and internal expertise is often lacking. As a result, many smaller market participants work with external consultants or service providers to cover at least basic requirements such as risk inventory and documentation.

Across all industries, only a fraction (approximately 4%) of institutions report having fully integrated DORA as business as usual. For most companies, DORA remains an ongoing implementation program that must be continued alongside their operational business.

Practical Challenges in Implementation

The requirements of DORA are far-reaching and affect all areas of the financial industry. In practice, five typical problem areas emerge:

1 **Banks – Real-time Incident Reporting**
Banks must report serious ICT incidents to the supervisory authority within tight deadlines. The reality: Many international institutions still operate heterogeneous IT landscapes with different logging and reporting systems. In spring 2025, a cyberattack on a large European bank revealed that internal escalation paths were not synchronized, resulting in a delay in the initial notification to the supervisory authority. According to an analysis by CeFPro (May 2025), 43% of institutions struggle with the timely implementation of incident reporting, particularly in connection with the harmonization of internal processes.

2 **Insurance – Resilience Tests Under Real-World Conditions**
Insurance companies are required to regularly conduct comprehensive resilience tests, including threat-led penetration tests (TLPT). In practice, these tests often fail due to complexity: A test at one reinsurer revealed that backup systems were in place but not sufficiently separated from each other. The simulated attack

could therefore also compromise the redundancy systems – a scenario that would have crippled business operations in an emergency. A report by Insurance Europe (January 2025) provides an overview of the challenges of implementing DORA: Full compliance remained a major challenge despite existing practices.

3 **Payment Service Providers – Third-Party Dependence**
Payment providers are heavily dependent on cloud services. A medium-sized institution discovered in spring 2025 that contracts with a US cloud provider did not provide for audit rights or exit strategies in accordance with DORA. This led to costly renegotiations that tied up significant resources in parallel with operations. According to Pillsbury (July 2025), many financial institutions were unable to complete their registers of information and contract amendments until after DORA came into effect—particularly for third-party contracts.

4 **Asset Manager – Data Classification and Protection**
DORA requires precise inventory and protection of critical data. Many asset managers struggle with consolidating historically grown data sets. One case showed that customer data had been stored for years in various legacy systems without emergency plans. The lack of transparency over data flows posed a significant compliance risk. Numerix (February 2025) describes how organizations often struggle to consolidate data and implement due diligence requirements for DORA-compliant third-party providers.

5 **FinTechs – Resources and Expertise**
Startups and young FinTechs often operate agilely but lack established governance structures. A Berlin FinTech with 120 employees discovered that there were no formal processes for incident response. It took external consultants to create basic documentation and organize training. This demonstrates that DORA is a cultural and organizational challenge for small, dynamic players. SANS (May 2025) warn: “If you haven’t started implementing measures yet, you're already late” – many smaller providers lack internal structures and know-how for DORA implementation.

Concrete Recommendations for Action

To overcome the challenges described, companies must become (more) active. Several areas for action emerge, in particular:

1 **Strengthen Governance and Accountability**
Supervisory authorities expect top management to assume responsibility for digital resilience. Companies should therefore firmly integrate DORA topics into their board agenda, strengthen a Chief Resilience Officer or CISO mandate, and conduct regular training for executives.

- Introduce board training on cyber and resilience topics: Regular awareness sessions for board members, e.g., structured according to the NIST Cybersecurity Framework.
- Introduce a Chief Resilience Officer (CRO) or strengthen the CISO: Mandate with a clear reporting line to the board; establishes accountability within the meaning of Article 5 DORA.
- Maturity analyses using COBIT or ISO 27001: Benchmarking against international standards to identify governance gaps.

2 **Implement automated incident response systems**

Manual processes are no longer sufficient. The use of Security Information and Event Management (SIEM) systems, SOAR platforms, and automated reporting tools is crucial to detecting, classifying, and reporting incidents at the speed required by DORA.

- Implement a SIEM system (e.g., Splunk, IBM QRadar, Azure Sentinel) to centrally collect log data and establish real-time correlations.
- Use a SOAR platform (e.g., Palo Alto Cortex XSOAR) to create playbooks for automated responses—e.g., automatically blocking compromised accounts.
- Conduct regular red team/blue team exercises using the MITRE ATT&CK methodology to realistically test incident response plans.

3 **Professionalize contract management**

Outsourcing and cloud contracts should be systematically reviewed and adapted to DORA-compliant standard clauses. These include audit rights, sub-outsourcing regulations, and clear exit strategies. Many companies establish central contract management units that incorporate regulatory requirements into contract design.

- Establish a central outsourcing register in accordance with DORA specifications; tools such as ServiceNow Vendor Risk Management or Archer support oversight.
- Standard contractual clauses in accordance with the EBA Outsourcing Guidelines: Clearly regulate audit rights, sub-outsourcing approval, and exit strategies.
- Conduct supplier audits in accordance with ISO 27036 (IT Supplier Management) to regularly review the security of service providers.

4 **Intensify resilience tests and emergency drills**

DORA requires not only tests but also a clear derivation of lessons learned. Companies should conduct regular crisis simulations – including the

participation of the board and operational teams. This is the only way to realistically identify vulnerabilities.

- Conduct threat-led penetration tests (TLPT) according to the TIBER-EU framework to simulate attacks under real-life conditions.
- Business Continuity Management (BCM) with ISO 22301: Planning and testing of recovery scenarios, including failover to backup data centers.
- Tabletop exercises for board members: Scenario workshops in which management is guided through simulated crises.

5 **Promote cooperation and knowledge sharing**

Cyber threats do not stop at company boundaries. Industry initiatives such as Financial ISACs or national CERTs provide platforms for exchanging threat information. Companies should actively participate to benefit from early warnings and sharpen their own resilience strategies.

- Participation in industry-specific ISACs (Information Sharing and Analysis Centers), e.g., FS-ISAC for financial companies.
- Establish an internal threat intelligence function: Use platforms such as MISP (Malware Information Sharing Platform) or ThreatConnect.
- Regular participation in CERT training (e.g., with national Computer Emergency Response Teams) to integrate early warnings and action recommendations.

Conclusion

Five years after the publication of the draft, DORA is a reality. While major players in the financial sector have adapted their structures, many, especially smaller companies, still face significant challenges. DORA is not a completed project, but an ongoing adaptation process. This means investing now in specific measures: automating incident response processes, revising outsourcing contracts, integrating resilience testing into regular operations, and strengthening governance structures at the board level. Equally important is building a culture of collaboration – for example, through active exchange in cyber threat intelligence networks. Prioritizing these steps not only ensures compliance but also builds sustainable digital resilience.

References

1 TechRadar, „DORA: six months into a resilience revolution“, https://www.techradar.com/pro/dora-six-months-into-a-resilience-revolution

2 TechRadar, „Regulatory compliance: Act now“, https://www.techradar.com/pro/regulatory-compliance-act-now

3 PwC Luxembourg, „DORA: laying the groundwork“, https://www.pwc.lu/en/press/press-releases-2025/dora-laying-the-groundwork.html

4 Help Net Security, „DORA compliance challenges for financial firms“, https://www.helpnetsecurity.com/2025/07/25/dora-compliance-challenges-financial-firms

5 Bird & Bird, „How well is Europe’s financial sector prepared for DORA?“, https://www.twobirds.com/en/insights/2025/global/how-well-is-europes-financial-sector-and-its-it-supply-chains-prepared-for-dora

6 CeFPro, „Most banks still not ready for DORA“, https://connect.cefpro.com/article/view/most-banks-still-not-ready-for-dora

7 Insurance Europe, „Strengthening the industry’s cyber resilience: Insights into the implementation of the Digital Operational Resilience Act“, https://insuranceeurope.eu/news/3275/strengthening-the-industry-s-cyber-resilience-insights-into-the-implementation-of-the-digital-operational-resilience-act

8 Pillsbury, „DORA: EU Financial Entities and Service Providers Face New Operational Resilience Requirements“, https://www.pillsburylaw.com/en/news-and-insights/dora-eu-financial-entities-service-providers.html

9 Numerix, „What the DORA Regulation Means for Financial Institutions in 2025“, https://www.numerix.com/resources/blog/what-dora-regulation-means-financial-institutions-2025

10 SANS Institute, „Navigating DORA & NIS2 Compliance: What EU Financial Sector Organizations Need to Know“, https://www.sans.org/blog/navigating-dora-nis2-compliance-eu-financial-sector-organisations

Authors

Dr. Andreas Windisch is Managing Director at asquared. As a certified computer scientist and with a doctorate in engineering, he acted in leading positions in automotive, technology and consulting firms and disposes of many years of experience in the field of IT transformation management in automotive and financial services sector.

About asquared

Asquared is a Berlin-based consulting firm. Our work focuses on developing practical solutions for the regulatory, technologically and/or socially induced change, associated with direct application and confirmation in an industrial environment.

Our attention is focused on business and technology and their interaction. Reaching from the reorientation of strategies, over the (re)design of products and services to the operationalization - our work focuses on shaping change. On all levels.

We present selected insights of our theoretic and practical research work to a broader audience in the form of publications and lectures.

asquared GmbH
Pappelallee 78/79
10437 Berlin - Deutschland

Phone +49 (0) 30 22 66 79 60
E-Mail contact@asquared.team

asquared.company
asquared.blog
twitter.com/asquaredgmbh
instagram.com/asquaredgmbh
linkedin.com/company/asquared