SPOTLIGHT

Sponsored by: Hitachi Vantara

Achieving operational resilience in a digitally transformed financial industry landscape in compliance with EU DORA requirements.

DORA Requirements: The Imperative to Act Upon a New Paradigm of Resiliency and Risk Management

December 2024

Written by: Maria Adele Di Comite, Research Director, IDC Financial Insights Corporate and Retail Banking, and George Briford, Research Director, IDC Financial Insights

Introduction

General Introduction to DORA — The Objectives of the Regulation

The European Union (EU) Digital Operational Resilience Act (DORA) entered into force in January 2023 and mandates compliance by January 17, 2025. This regulation aims to bolster IT security and resilience in financial entities transacting in the EU by minimizing systemic risk from interconnected systems.

As customers — both individuals and corporations — demand real-time services anytime and everywhere, banks must process transactions and provide visibility to them in real time through processing acceleration, automation, and improved data management. To provide customer-centric value propositions, financial entities leverage the ecosystem collaboration and embed third-party services. Their challenges are twofold: they must meet customer expectations by providing ubiquitous real-time services to remain competitive while managing an augmented cyberattack surface where not all elements are under their direct control.

AT A GLANCE

KEY STATS

According to IDC's 2024 *Financial Insight Survey* and IDC's 2024 *EMEA Security Technologies and Strategies Survey*:

- 46% of financial entities consider compliance, regulatory requirements, and risk management as their top business priority.
- 47% of financial entities will have a clear map of critical functions and related ICT providers by January 17, 2025.
- 49% of financial entities state they are aware of DORA but have not yet undertaken exploratory work.

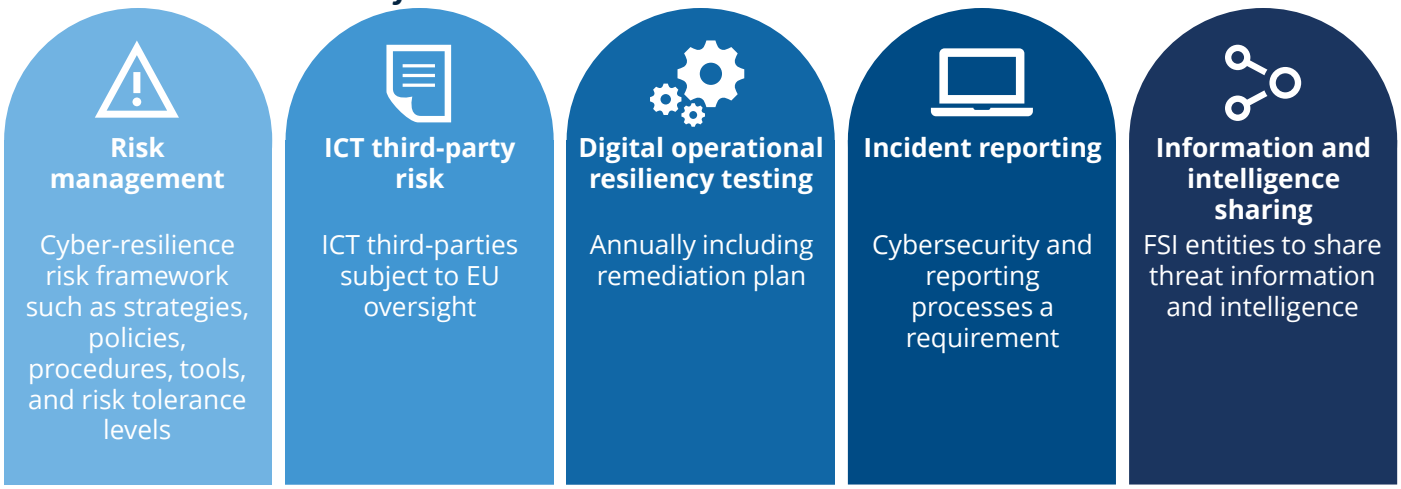
Digital transformation creates an interconnected and interdependent ecosystem, leading to significant systemic risk. Under DORA, financial entities must address risks from operating in a digitally augmented space by enhancing their information and communication technology (ICT) capabilities to mitigate systemic risk and strengthening governance and control measures. Notably, digital operational resilience is not solely an IT issue; board commitment is essential, along with the involvement of various stakeholders across the organization, including operations, procurement, and legal, as well as education, training, and testing that involve the entire workforce.

A Short Recap on DORA and Its Key Requirements

With DORA, the European regulator aims to strengthen the financial sector's resilience to ICT-related incidents. Three major innovations come with this regulation in relation to other risk management legislation. First, it aims to harmonize rules across all financial entities, establishing consistent requirements for banking, insurance, capital markets, and ancillary service providers such as credit bureaus (collectively FSIs). The second innovation represents a paradigm shift, recognizing that financial entities often rely on third-party services, thereby bringing ICT partners within the scope of regulation and under the scrutiny of European Supervisory Authorities (ESAs) (i.e., EBA, ESMA, and EIOPA). This approach means that critical ICT third parties providing services to financial institutions, such as cloud platforms, data analytics, and audit services, are also subject to this new regulation. A third innovation is the shifting from a traditional business continuity planning and disaster recovery approach to include cyber-resilience as the ability to identify, respond, and recover swiftly from an IT security incident. This shift represents a set of processes and technologies that mitigate the impact of cyberincidents.

DORA consists of five core pillars that address various aspects of ICT security to provide a comprehensive digital resilience framework for the relevant entities (see Figure 1).

FIGURE 1: ***The Five Pillars of DORA***



Source: IDC, 2024

Financial entities must withstand, respond to, and recover from ICT incidents, ensuring the continued delivery of critical functions while minimizing disruption for customers and the financial system. Achieving ICT resilience requires implementing, continuously maintaining, and upgrading proper measures and controls for ICT systems and related third parties. A specific focus on cyber-resilience should be applied across all the pillars. A key component of this effort is constantly testing the effectiveness of business and ICT continuity plans. Requirements can be grouped in the five pillars:

- **Risk management:** ICT risk management frameworks and tool requirements build on the well-known traditional disaster recovery and business continuity strategies that significant banks within the single supervisory mechanism already implemented. In addition, DORA broadens the range of entities included in the regulation to encompass all financial entities and ancillary service providers. The scope of the risk management framework is very broad as the

objective is to support and manage activities with the task of identifying and assessing ICT risk by providing tools to map the financial entity's digital landscape, including assets and processes. This enables financial entities to pinpoint vulnerabilities and assess their potential impact. Integral to the framework is also the capability to facilitate the development and implementation of risk mitigation plans. A proper risk management framework must cover the full value chain including identification, protection, detection, response, and recovery. All entities must reconsider risk management, acknowledging that malicious actors continuously evolve their techniques, that AI plays a significant role on both sides, and that the shift toward real-time processing and 24 x 7 availability introduces additional challenges.

- **ICT third-party risk management:** This is the most wide-reaching regulatory innovation introduced by DORA. Financial entities must clearly map their critical functions, underlying assets, and related ICT third-party service providers. Given the importance of critical ICT third-party service providers, substantial benefits arise from cooperation between IT, business operations, risk management, compliance, legal, and procurement.
- **Digital operational resilience testing:** Financial entities, regardless of proportionality criteria, must implement a comprehensive testing plan that includes regular tests such as vulnerability assessment, scenario-based testing, end-to-end testing, and penetration testing to identify gaps and potential failures. Critical ICT systems and applications must undergo annual testing with qualified, independent testers following risk-based plans, maintaining records to support continuous improvement, internal audits, and ESA investigations. In addition, non-microenterprise financial institutions are required to conduct advanced Threat-led Penetration Testing (TLPT) every three years, with the last deadline set for January 17, 2028. Financial entities may also require third-party critical service providers to participate in these tests, and contracts reflect enhanced testing obligations.
- **Mandatory incident reporting:** DORA aims to simplify mandatory incident reporting, requiring financial entities to provide initial, intermediate, and final reports for major incidents, in line with ESAs' final Regulatory Technical Standards (RTS) of July 17, 2024. Financial entities must promptly address the incident itself while managing the mandatory reporting. Ensuring that personnel can track, retrieve, and audit the provided information is also paramount.
- **Voluntary information and intelligence sharing:** DORA has introduced a statement that allows financial entities to participate in trusted, ecosystem-driven collaborative information-sharing arrangements to enhance overall financial system resilience. To ensure the organization can properly exploit the data from these arrangements, financial entities must also review workflows and notifications to ensure that they promptly involve all internal stakeholders as appropriate.

To comply with the previous five pillars, financial entities must collaborate with their ICT partners. Implementing DORA will significantly impact organizational processes, so it is important to consider all involved stakeholders within the financial organization. Members of the C-suite, including the CIO, CISO, chief compliance officer, and chief risk officer, play crucial roles in this effort, alongside ICT governance. In addition, procurement and legal teams have relevant roles in reviewing contractual agreements and managing the onboarding and continuous monitoring of critical ICT third-party providers. The CHRO is equally important, as this role involves tackling educational activities, staff reskilling, and testing to ensure employees gain the necessary skills for new compliance requirements.

Financial entities must also define clear exit strategies to mitigate systemic risk if operational issues arise with an existing ICT partner. Each entity must identify and select alternative solutions and service providers to ensure a smooth transfer

of critical services if necessary. For ICT vendors, DORA's impact is twofold: It opens new opportunities and makes the market more fluid while imposing additional compliance obligations with which ICT vendors must comply.

Finally, noncompliance with DORA is not an option, as it imposes direct penalties on critical ICT third-party providers and mandates EU member states to establish significant penalties for violations. For financial institutions, these penalties must be proportionate to the severity of noncompliance and can include monetary fines and public disclosure of the breach, harming institutional reputation, eroding customer trust, and reducing stakeholder value. For critical third-party ICT providers, fines can reach up to 1% of their average total annual worldwide turnover.

Financial Entities Are Implementing Resiliency Measures But Not at the Needed Scale and Pace

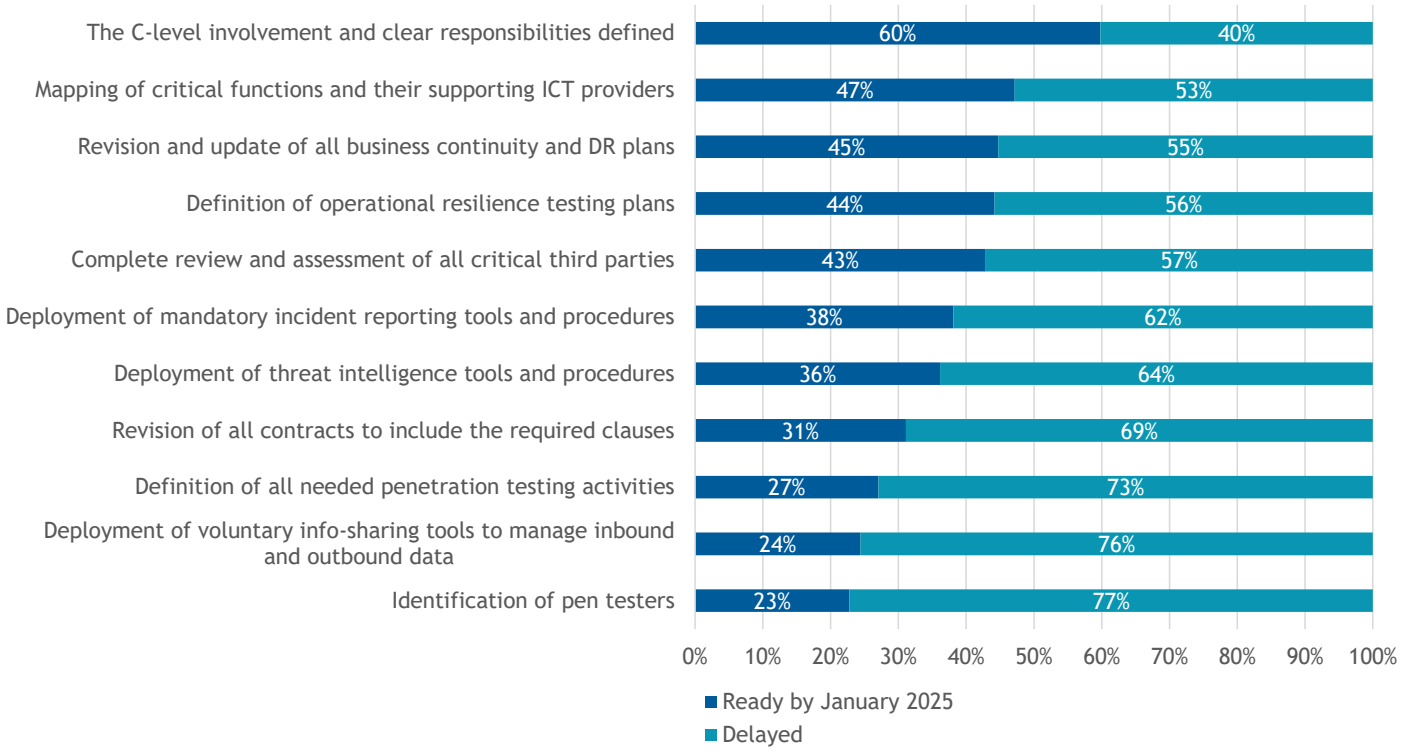
Financial entities are prioritizing a number of key initiatives in the area of compliance, regulatory requirements, and risk management to achieve harmonization with the ever-growing rule books related to resiliency. Cybersecurity is high on the list to conform with various standards around the world in addition to DORA, such as the NIST Cybersecurity Framework 2.0, New York Department of Financial Services part 500, and Japanese Economic Security Promotion Act.

Taking care of operational resilience by complying with rules applied worldwide is another category of initiatives. Financial entities understand that data security underpins everything they do and is one of the major threats to their business models.

All of the five DORA pillars represent hurdles for the majority of financial entities that will not be compliant in time to meet the January 2025 deadline. According to IDC's October 2024 *Financial Insights Survey* covering worldwide financial organizations, senior management is involved with pushing toward compliance in terms of their own involvement and responsibilities, but financial organizations subject to the act are lagging when it comes to actually carrying out the initiatives and work needed to meet the stipulated requirements for DORA (see Figure 2).

FIGURE 2: ***Organizations Are Slow to Achieve DORA Readiness***

Q *What is your progress on each of the below requirements for DORA compliance by the January 2025 deadline?*



Note: Respondents were financial organizations.

Source: IDC's Financial Insights Survey, October 2024

Challenges to Tackle to Become Compliant With DORA

There are a number of practical steps financial entities can take to improve their DORA readiness and avoid the risks of being penalized by the regulatory bodies as well as by various stakeholders. Centralizing cybersecurity and IT security organizations, improving regular security controls, and implementing a zero trust architecture should all rank high on the list of actions financial entities need to take.

Shifting from Disaster Response and Recovery to Full Cyber-Resilience

ICT risk management requires much more attention from the C-suite than it has previously received. Corporate leaders are responsible for developing a clear digital operational resilience strategy and ensuring appropriate budget and skills allocation. This focus on enhancing ICT risk management is essential. DORA compliance sets a clear requirement for the boardroom to take responsibility for managing ICT risk at their organization. Digital operational resilience is a moving target and one that entails modern tools for monitoring and tracking activities that achieve continuous improvements. To

support this requirement, financial entities must establish internal reporting channels, and the risk management framework must shift from reactive disaster and business continuity measures to a defense-in-depth cyber-resiliency strategy.

A proper cyber-resiliency solution must ensure a financial entities' data is accessible, secure, and compliant through proactive threat identification and detection in addition to reactive response and recovery measures:

- **Identification:** The solution must map and pinpoint risk across an institutions' attack surface from ICT supply chain to cyber and SDLC. Regular vulnerability and testing leveraging advanced threat intelligence to simulate real-world attack scenarios is required to mitigate continuously evolving threats.
- **Protection:** It must ensure comprehensive data protection by prioritizing integrity, privacy, and restricted access. This involves content validation and protection against unauthorized changes, identifying any modifications as data is accessed and transmitted. Strong identity and access management policies and tools are critical, along with privacy-enhancing technologies to safeguard data confidentiality and integrity during use.
- **Detection:** It must rapidly detect threats, particularly cyberattacks, by leveraging solutions that match the speed and scale of threat actors. These solutions should include AI-driven ransomware, threat, and anomaly detection, supported by always-on monitoring teams or automated processes with failover, to swiftly initiate incident response plans and mitigate impact.
- **Response and recovery:** The solution must rethink disaster recovery and business continuity to meet real-time banking demands and counter evolving cyberthreats. Timely replication and backup across geographies are essential to safeguard critical services during cyberattacks and ensure data accessibility. Traditional synchronous replication, which risks propagating attacks to recovery sites, must be replaced with more resilient data storage approaches including asynchronous or hybrid approaches.

Achieving DORA Compliance Through a Holistic Approach to Cyber-Resilience — the Benefits of End-to-End Solutions

To fully comply with DORA, financial entities must adopt a holistic approach to cyber-resilience. Such an approach ensures that solutions address the entire cycle from threat detection to business recovery and rebirth. It is essential to review team resources, tools, and procedures to reduce complexity; cut costs through economies of scale; increase responsiveness; and accelerate time to compliance. Future proofing is also necessary to ensure that financial entities can comply with evolving regulatory requirements and address emerging DORA-like regulations in the United States, the United Kingdom, Japan, Canada, and Australia.

Financial entities need solutions that address the following components, which align with the DORA pillars:

- **ICT risk management and governance:** This involves the management of requirements and stakeholders, education and simulation, evaluation of the CISO role, and reassessment of all stakeholder contributions to enhance cyber-resilience. ICT risk management must ensure that all phases are properly addressed and receive adequate attention, addressing identification, protection, detection, response, and recovery. In addition, financial entities should challenge and reevaluate existing disaster recovery and business continuity management practices to prevent cyberincidents from propagating through the disaster recovery site.

- **Incident management and reporting:** Timely detection and proper workflow management are prerequisites for preventing and managing incidents. Incident reporting must evolve from static, standalone tools to more dynamic and auditable ones. AI can also improve incident analysis and monitor system performance.
- **Testing:** Financial entities must plan multiple testing activities. A significant change relates to penetration testing, where they should organize joint penetration testing activities with ICT partners to ensure appropriate commitment regarding skills, resource allocation, and communication. They should also implement tools to run and track all testing activities.
- **Third-party risk management:** This represents the main paradigm shift that DORA brings. As financial entities' IT infrastructures rely on cloud service providers and other third parties, each entity must develop a risk-based plan for due diligence, contractual reviews, and coordinated activities with ICT partners.
- **Information sharing:** This includes voluntary ecosystem-driven collaborative initiatives and mandatory incident reporting to the requisite authorities. Financial entities must provide initial, intermediate, and final reports for major incidents. It is also crucial to track all communications and ensure the process is auditable.

Considering Hitachi Vantara

For over 15 years, Hitachi Vantara has helped leading banks and financial firms manage emerging threats, complex regulations, and ediscovery challenges to reduce operational and compliance risk. With its defense-in-depth solution, Hitachi accelerates financial entities' DORA compliance journey with compliance gap assessment, remediation, solution implementation, and management across required hardware, software, and services. The company supports financial entities in addressing key requirements, including governance and AI-driven cyberthreat and anomaly detection through mitigation, vulnerability assessments, and comprehensive testing, such as TLPT. It ensures business continuity through ransomware and disaster recovery at scale, offering guaranteed cyber-resilient and always available high-end to midrange performance storage offerings. Further, Hitachi is a trusted DORA-compliant third party to FSI customers that supports governance, operational resilience evidence, and testing, reducing client compliance burden.

The concept of cybersecurity and resiliency in general requires a partner able to create a holistic overview and reduce the complexities involved. Although DORA regulations clearly state that the financial entity cannot outsource its responsibilities, by bringing in an experienced partner it can gain confidence and reduce the risk gap.

Challenges

There are several challenges facing financial entities:

- Many have not completed all preliminary requirements on time and may still struggle to identify their assets and the underlying critical third-party ICT service providers. Furthermore, the boardroom's attention and involvement still need to be reinforced with appropriate awareness programs to get the full picture of the changes to risk frameworks, and in turn risks to their business, arising from DORA.
- Financial entities do not take a consolidated approach to tackle many of their vulnerabilities. They lack a central center of excellence where talent, tools, and domain knowledge are developed and deployed in a synergistic manner. Instead of sourcing point solutions, financial entities should look to compensate for gaps in their

capabilities by working with a "one-stop-shop" type of partner to fully benefit from a faster deployment in a coordinated manner through a well-proven governance.

- The attack surface is augmented far beyond the direct control of internal infrastructures. Even with the help of solution partners such as Hitachi Vantara and others, keeping the augmented attack surface under control is a paramount effort and ensuring end-to-end resilience and data protection requires a continuous effort to fight against malicious actors who are also exploiting technological innovation.
- Governance can become complicated due to the extensive interactions necessary with the numerous third-party ICT providers that each financial entity has.
- Current IT and procurement resources may not be suitable for the continuous monitoring and evaluation of third parties and associated risks.

Conclusion

Digital transformation is a double-edged sword. Financial entities face multiple challenges in an interconnected digital landscape:

- **IT and infrastructure upgrades:** To meet evolving customer expectations, banks must pursue digital transformation. Access is omni-channel, employees are distributed, infrastructure is mostly hybrid, and value creation often relies on ecosystem collaboration.
- **Cyberthreats and risks**: Achieving cyber-resiliency requires a shared responsibility model that focuses on comprehensive security and resiliency strategies, given the strong dependencies on integration with critical third-party providers, which increases the attack surface and systemic risks.
- **Regulatory requirements:** Compliance is continuously evolving to protect customers and their data while minimizing systemic risk. DORA and similar regulatory requirements across several jurisdictions force financial entities to rethink their strategic approach to resilience and adopt a more holistic view.
- **Risk of penalties:** Many financial entities are far from reaching DORA compliance in January 2025, and thus expose themselves to administrative penalties and remedial measures besides risking the trust of various stakeholders, such as investors and clients.
- **Lack of urgency:** Many financial institutions have not started the laborious work of exploring and filling the gaps in their journey to achieve DORA compliance.
- **Assurance through a third party:** Financial entities can benefit from bringing onboard an external party that can provide the necessary capabilities ranging from talent and skills to proven tools and robust governance.

DORA regulation does not inhibit the financial industry's digital transformation but addresses the interdependence of an ecosystem-driven economy and mitigates systemic risk across the financial services industry augmented space.

IDC believes that this regulation will play a crucial role in shaping a financial entity's data resiliency and compliance approach. The deadline for DORA compliance is January 2025, but improvements can and will occur beyond this milestone as research shows many financial entities will still struggle to be fully compliant in January 2025.

About the Analysts

Maria Adele Di Comite, *Research Director, IDC Financial Insights Corporate and Retail Banking*

Maria Adele is research director for IDC Financial Insights European research team and is responsible for the IDC Financial Insights Corporate Banking Digital Transformation Strategies program. She has strong competencies in financial services strategy, cybersecurity, and regulatory evolution. She has been living and working in three different countries (Germany, Belgium, and Italy) and she speaks five languages. She is an expert in B2B business strategy, with significant experience in financial services, system integration, and consulting.

George Briford, *Research Director, IDC Financial Insights*

George Briford is research director for IDC Financial Insights. His major experience spans over designing pragmatic operating models and leading transformation and change management initiatives as project and program manager for universal banks in Europe, Eurasia, and East Asia. Briford has experience in working for major management consulting firms as well as various roles in banks. His main domain is retail and small business banking with a focus on strategy development, sales and distribution operating models, customer relationship management strategy, and business architecture including digital enablement of its key components.

MESSAGE FROM THE SPONSOR

Hitachi Vantara helps banks and financial institutions achieve operational resilience with a defense-in-depth approach, offering tailored assessments, remediation, and comprehensive solutions, both managed and unmanaged, that meet evolving regulatory demands — delivered from one partner. Hitachi is trusted to provide unbreakable cyber resilience, data protection, and compliance solutions by 9 of the top 10 global banks and all top 10 insurers. As a DORA-compliant third-party, it simplifies compliance with governance support, operational resilience evidence, and testing. Learn more about Hitachi's DORA compliance solutions backed by a Cyber Resiliency Guarantee at www.hitachivantara.com.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
blogs.idc.com
www.idc.com