SKILLFINDER INTERNATIONAL

DORA

The Digital Operational Resilience Act

STUART EGERTON

Associate Director

PAUL HEYWOOD

DORA Programme Director

17TH JANUARY 2025

ARE YOU READY?

EXECUTIVE SUMMARY

The rapid digitization of the European financial sector in recent decades has made technology integral to financial operations, ushering in new risks. Financial institutions have attempted to address these risks through controls and contingency plans, but many struggle to establish robust defences against ICT-related risks. Operational resilience efforts have often been disorganized, resulting in weak controls and inadequate backup plans. Additionally, insufficient information for management leaves board members and senior managers unaware of elevated ICT risks. Recent high-profile disruptions at European banks have underscored the industry's vulnerability.

To address this, the European Council aims to enhance operational resilience while harmonizing national regulations. The Digital Operational Resilience Act (DORA) provides a comprehensive framework for managing ICT risks in European financial institutions. DORA consists of five pillars covering ICT risk management, incident reporting, resilience testing, third-party risk, and information sharing. Compliance with DORA is challenging and necessitates a purposeful, business-led technology strategy and integrated risk management aligned with critical services.

The potential benefits of improved operational resilience are significant, including reduced financial losses, smoother system implementation, maintained customer service levels, enhanced brand value, lower risk management costs, and reduced regulatory risk. Building digital operational resilience is no longer optional and requires engagement from all levels of the organization, including business lines, senior management, and boards.

DORA is currently coming into effect from 17th January 2025

WHAT IS DORA

DORA, as a component of the EU's Digital Finance Package (DFP), strives to standardize regulations pertaining to operational resilience and cybersecurity across EU member states. This legislation sets forth consistent security requirements for network and information systems employed by financial sector entities and critical third-party service providers engaged in information communication technologies (ICT), such as cloud platforms and data analytics services.

DORA establishes a regulatory framework aimed at ensuring digital operational resilience for all relevant firms, obliging them to demonstrate their capability to withstand, respond to, and recover from various ICT-related disruptions and threats.

The definition of ICT encompasses a wide range of digital and data services delivered via ICT systems to both internal and external users on an ongoing basis.

In the broader context of the DFP, DORA contributes to the EU's efforts to create a harmonized European approach to digital finance. This approach not only promotes technological advancement but also safeguards financial stability and consumer interests. The DFP encompasses additional legislative proposals, including ones addressing crypto assets markets (MiCA), distributed ledger technology, and an overarching digital finance strategy.

Who needs to comply with DORA

DORA's scope encompasses various financial entities, such as credit institutions, payment institutions, investment firms, crypto asset service providers (authorized under MiCA), and more (referred to as "Financial Entities"). Additionally, DORA extends its coverage to ICT third-party service providers that the European Supervisory Authorities (ESAs) classify as "critical" for Financial Entities, using criteria like systemic impact, importance to Financial Entities, reliance on services for critical functions, and substitutability.

ICT third-party providers not designated as critical can choose to voluntarily opt into this oversight framework. Certain categories of ICT third-party service providers are excluded from ESAs' designations, including those providing ICT services within their own financial group or solely within one EU Member State to financial entities that operate there.

Some key obligations:

DORA introduces specific regulations regarding the capacity to manage ICT-related risks, reporting procedures, and testing protocols, all geared toward enhancing the ability of Financial Entities to endure, respond to, and recover from ICT-related incidents. Notably, some of these requirements outlined in DORA, like those pertaining to ICT risk management, partially align with existing EU guidance, such as the EBA Guidelines on ICT.

The proposals encompass stipulations concerning:

Management of IT Risks

DORA establishes fundamental principles concerning internal controls and governance arrangements. The management body of a Financial Entity is tasked with defining, authorizing, supervising, and maintaining continuous accountability for the firm's ICT risk management framework within its broader risk management framework. This framework necessitates the maintenance of robust ICT systems, focusing on distinct functions within ICT risk management, including risk identification, safeguarding and prevention, detection, response, recovery, and communication with stakeholders.

Reporting ICT-Related Incidents

DORA seeks to establish a uniform incident reporting system, encompassing a management procedure for identifying, addressing, and notifying ICT-related incidents.
Incidents classified as "major" must be promptly reported to competent authorities, adhering to stringent timelines that include initial notifications on the same day or the following day, employing mandatory reporting templates. In certain situations, communication with service users or customers may also be necessary.

Testing

DORA mandates Financial Entities to implement a robust digital operational resilience testing program encompassing ICT tools, systems, and processes. Some Financial Entities are required to conduct advanced testing of these elements at least once every three years using threat-based penetration tests.

Information Sharing

DORA includes provisions to facilitate the sharing of cyber threat information and intelligence among Financial Entities. This sharing encompasses indicators of compromise, tactics, techniques, procedures, cybersecurity alerts, and configuration tools, all aimed at enhancing digital operational resilience.

Localisation

Financial Entities may only engage the services of a third-country Critical ICT Third-Party Provider if that provider establishes an EU subsidiary within 12 months of being designated as such.

What's the impact on administration:

DORA introduces requirements for contracts between Financial Entities and ICT third-party service providers concerning ICT services, affecting both existing and new contracts. These requirements encompass all contractual arrangements for ICT service usage, with more extensive criteria applied to contracts supporting critical or vital functions. All relevant contracts must be written, clearly delineating the rights and responsibilities of both the Financial Entity and the ICT third-party service provider.

DORA, unlike existing EBA guidelines on outsourcing, is less prescriptive regarding subcontracting requirements. Financial Entities must conduct a comprehensive analysis of subcontracting arrangements, particularly when dealing with third-country ICT third-party service providers, before entering into contracts. For critical or vital functions, Financial Entities must assess the potential impact of lengthy or complex subcontracting chains on their ability to fully monitor contracted functions and on the competent authority's ability to effectively supervise the entity.

The only contractual requirements related to subcontracting in DORA involve specifying whether subcontracting is permitted, the conditions of subcontracting, and the locations of subcontracted functions, ICT services, and data processing activities.

Management Responsibilities:

To ensure alignment between a Financial Entity's business strategy and its management of relevant ICT risks, the entity's management body must play an active central role in steering and adapting the ICT risk framework and digital resilience strategy. These requirements broadly resemble those found in existing EU guidelines, including the EBA Guidelines on ICT and security risk management and Guidelines on outsourcing arrangements.

The management body bears ultimate responsibility for managing ICT risks within the Financial Entity. It must define clear roles and responsibilities for all ICT-related functions and establish appropriate governance arrangements to facilitate effective and timely communication, cooperation, and coordination among these functions. Except for microenterprises, Financial Entities must appoint a dedicated role to monitor ICT third-party provider arrangements or designate a senior management member responsible for overseeing related risk exposure and documentation.

To fulfil their roles effectively, members of the management body must possess and maintain sufficient knowledge and skills to understand and assess ICT risks' impact on the Financial Entity's operations. This necessitates implementing a regular training program, not only for staff directly involved in managing ICT risks and overseeing ICT third-party provider arrangements but also for management board members.

What should firms be doing now to prepare?

While DORA aims to streamline existing frameworks and standards, its ambitious implementation timeline necessitates immediate organizational preparation. Here are five proactive steps organizations can take to meet these requirements:

1. Conduct a Comprehensive Risk Assessment:

Initiate a risk assessment, including a gap analysis, to ensure compliance with the new regulations by the early 2025 deadline. Identify potential challenges and requirements that may pose significant hurdles, enabling you to proactively address them.

2. Collaborate with Compliance and Training Teams:

Partner with corporate compliance or learning and development teams to fulfil the legislation's organization-wide operational resilience training mandates. Ensuring staff is well-prepared and educated is crucial for compliance.

3. Revise Incident Classification Methods:

Begin adapting your organization's incident classification methodology to align with DORA requirements. This adjustment should include mapping out business processes and workflows to facilitate proper notification to regulators in the event of a major incident.

4. Plan for Large-Scale Penetration Testing:

Start developing a scenario for the forthcoming large-scale penetration test, with the goal of obtaining regulator validation before the 2025 deadline. Engage closely with critical technology and data service providers during this process to ensure seamless cooperation.

5. Leverage Technology for Resilience:

Utilize technology to expedite the establishment of an operational resilience program. Leveraging tools and solutions can help streamline compliance efforts and enhance the efficiency of your resilience program's development.

Taking these proactive measures will not only position your organization to meet DORA's requirements but also help ensure a smoother transition to the new regulatory landscape.

Contacts:

STUART EGERTON

Associate Director

E: segerton@skillfindergroup.com

T: +44 (0) 7494 919 347

SKILLFINDER
INTERNATIONAL