BRJ Logo

Digital Operational Resilience Act: Key considerations ahead of the 17 January 2025 compliance deadline

01 November 2024

This article first appeared in Thomson Reuters Regulatory Intelligence

The Digital Operational Resilience Act (**DORA**) is set to harmonise and strengthen the approach to cybersecurity and digital operational resilience in the EU financial sector. As the deadline for compliance of **17 January 2025** draws near, most in-scope firms will be well underway with their compliance programs. All financial services firms and ICT third-party service providers (**ICT TPPs**), even those based in the United Kingdom, should consider DORA's wide application to their business operations.

What is DORA?

DORA was adopted as a response to the financial industry's growing dependence on information and communications technology (**ICT**) and the associated risks. Recent events, such as the widespread CrowdStrike outage, have underscored the critical importance of robust ICT risk management within the financial ecosystem.

DORA sets out comprehensive requirements on financial entities to manage ICT-related risks and introduces a novel oversight framework for ICT TPPs designated as 'critical' (**CTPPs**) by European Supervisory Authorities (**ESAs**).

Scope of application

DORA's influence extends beyond the European Union, potentially impacting financial services groups and ICT TPPs on a global scale. DORA's application can be categorised in two ways:

1. **Direct**: DORA applies to: (a) a wide range of EU-based financial entities, including banks, insurance firms, payment providers, digital payment providers, and crypto-asset service providers; and (b) CTPPs (under an oversight framework), even those outside the EU.
2. **Indirect**: DORA extends to: (a) multinational or global financial services groups with any EU operations (intra-group arrangements are captured under DORA); and (b) ICT TPPs providing ICT services to EU financial entities (which are not CTPPs).

Key requirements

In respect of the requirements placed on financial entities, DORA is based on five fundamental pillars:

1. **ICT Risk Management:** strategies, policies and procedures to identify, assess, and mitigate ICT-related risks.
2. **Incident Management, Classification, and Reporting:** processes for detecting and managing ICT incidents, including their proper classification and timely reporting to relevant authorities.
3. **Digital Operational Resilience Testing:** testing of systems and applications (incudes testing of CTPPs).
4. **Third-Party Risk Management:** review and amend ICT service contracts to comply with contractual requirements and identify and monitor ICT concentration risks.
5. **Information Sharing:** information and best practice sharing among financial entities to enhance sector-wide resilience.

Financial entities must implement these requirements in a manner proportionate to their size, nature, and risk profile, ensuring a balanced approach to compliance.

As part of the oversight framework, CTPPs are required to establish a subsidiary in the EU within 12 months following its designation by the ESAs (if not already established). EU financial entities are not allowed to make use of a CTPP's services if such subsidiary has not been established.

Focus on ICT contracts

A key aspect of DORA is the requirement for financial entities to include specific provisions in contracts with ICT TPPs. Contractual requirements apply to all ICT service contracts, with more extensive provisions required for contracts supporting a financial entity's critical or important functions.

While some of these requirements align with existing regulations, such as the EBA guidelines on outsourcing and the ESMA guidelines on outsourcing to cloud service providers, DORA introduces new elements and significantly broadens the scope of in-scope contracts. For example, DORA extends beyond a strict focus on third party 'outsourcing" arrangements and also includes intra-group arrangements between EU financial entities and non-EU group service companies.

Financial entities that have already undertaken contract remediation efforts to comply with existing regulations will still need to reassess their contractual arrangements in light of DORA.

Financial entities should also take account of the level 2 legislative measures published by the EU regulators (i.e., regulatory and implementing technical standards) and, particularly from a contractual perspective, the regulatory technical standard related to subcontracting.

Compliance benefits and risks

By enhancing ICT resilience, financial entities and ICT TPPs can improve their ability to manage and mitigate ICT-related disruptions effectively. This will result in a reduction in operational and reputational risks in an increasingly digitised financial landscape.

In respect of non-compliance, EU regulators and relevant competent authorities have been granted broad enforcement powers, including the ability to impose hefty administrative fines and implement remedial measures on both financial entities and CTPPs.

The absence of a formal grace period for compliance beyond January 2025 means that EU regulators and relevant competent authorities could potentially take enforcement action for non-compliance as early as this date, highlighting the urgency for entities to act swiftly in their compliance efforts.

Next steps

With the compliance deadline rapidly approaching, in-scope financial entities should take immediate action to ensure readiness. The first step involves a thorough assessment of DORA's applicability to their operations, followed by a comprehensive gap analysis to identify areas requiring attention across the five pillars.

For the important task of contract remediation, financial entities should undertake a systematic process which includes the following steps:

1. Mapping and categorising all ICT contracts, with particular attention given to those contracts supporting critical or important functions of the financial entity.
2. Collecting and carrying out a gap analysis for existing ICT contracts against DORA's contractual requirements.
3. Engaging with ICT TPPs and amending ICT contracts in accordance with DORA.

Approach to compliance

Financial entities

In order to meet the 17 January 2025 deadline, financial entities should consider taking a pragmatic and proportionate approach to their compliance efforts. This includes:

1. Engaging with ICT TPPs as soon as possible. This is vital to avoid bottlenecks as the January deadline approaches. By initiating discussions in advance, financial entities are likely to have more cooperative and productive negotiations with ICT TPPs who will likely face similar requests from multiple clients.
2. Considering taking a "deemed acceptance" approach with certain ICT TPPs (i.e., on a non-negotiable basis). This approach may, in

some cases, avoid entering lengthy negotiations with some ICT TPPs; however, in turn, financial entities should ensure that the terms proposed are reasonable.

3. Financial entities should focus initially on critical/material contracts (and those supporting critical or important functions). This ensures that the most crucial aspects of the ICT infrastructure are addressed as a priority.

ICT third-party service providers

ICT TPPs, on the other hand, should prepare for an influx of amendment requests from their EU financial sector clients. To streamline this process and potentially secure more favourable terms, ICT TPPs might consider taking a proactive stance by developing standardised DORA-compliant contract addendums and proposing these to their EU financial sector clients.

Key contact

Rowan Armstrong

Partner

rowan.armstrong@brownejacobson.com

+44 (0)330 045 2737

Related expertise

Criminal compliance and regulatory

Data protection and privacy

Financial services and insurance advisory

Financial services regulation