Lloyd's List Intelligence
Financial Regulation International

www.financialregulationintl.com

Preparing for DORA: Mind the gap

by **Mike Pierides** and **James Mulligan**

From 17 January 2025 financial entities based in the European Union (EU) must have in place processes and policies, and mandatory contract provisions with their third-party technology vendors, that comply with the EU's Digital Operational Resilience Act (DORA). Financial entities are at varying stages of updating their operational risk management frameworks and remediating contracts with technology vendors, and some firms are finding that existing processes and contracts may not be compliant with current regulatory expectations.

McKinsey estimates that EU institutions typically earmarked €5–15 million for DORA program strategy, planning and design, although full implementation costs may be five to ten times that range.[1] Meanwhile, the European Central Bank has signalled that resiliency will be a top priority on its supervisory agenda for the coming year.[2]

This article looks at the mandatory contract provisions under DORA, how they map to existing regulatory regimes in respect of outsourcing arrangements and key considerations for designing a path for contract remediation for DORA compliance.

Scope and objective

DORA applies to financial institutions, investment firms, fund management companies and other regulated financial entities based in the EU. One of DORA's key objectives is to strengthen financial entities' operational resilience by ensuring prudent risk management of a broad array of information communication and technology (ICT) services, including all of an organisation's cloud, software-as-a-service (SaaS), digital data and IT infrastructure arrangements.

A defective software update in July 2024 that globally disrupted several industries, including banks, provided a stark warning of the criticality of operational resilience at the heart of third-party risk management and supply chain design.

Mandatory contract provisions

DORA requires financial entities to ensure that all contracts with third-party ICT service providers, both intra-group and external, include mandatory contract provisions around the following:

- access and audit rights;
- performance standards;
- service locations;
- data and confidentiality;
- business continuity;
- termination rights;
- cooperation with authorities;
- classification, notification and reporting of major ICT-related incidents; and
- compliance with appropriate information security standards and other policies.

For contracts with third-party ICT service providers that support critical or important functions, there are more prescriptive requirements around the following:

- access and audit rights;
- subcontracting;
- reporting obligations;
- business contingency planning and testing;
- participation in threat-led penetration testing; and
- exit planning.

Key gaps between DORA and existing outsourcing regulatory regimes

EU financial institutions and investment firms will be familiar with existing EU regulatory expectations in respect of outsourcing arrangements, such as the European Banking Authority's Guidelines on Outsourcing Arrangements.[3] Those guidelines include many of the same concepts (such as assessing "critical or important functions") and require similar, if not the same, contract terms for outsourcings that support critical or important functions as those listed above.

The key gaps between DORA and those existing regimes are as follows:

1. **The scope of ICT services is broader under DORA**, extending beyond services that the financial entity could otherwise undertake itself to, for example, digital data subscription services, SaaS and certain software licensing.

2. **All contracts for ICT services must contain mandatory contractual provisions under DORA**, not just those supporting critical or important functions. This will require remediating certain contracts which may have fallen outside of outsourcing contract remediation projects, as well as amending contracting procedures for ICT services going forward.
3. **There are additional mandatory contract provisions**, around participation by the ICT provider in the financial entity's digital operational resilience training, providing assistance with ICT incidents, and supporting adherence to the ICT security standards and business continuity requirements under DORA. In respect of ICT services supporting critical or important functions, there are more extensive provisions under DORA in respect of subcontracting such services.
4. **A separate policy must be adopted addressing compliance with the contractual requirements for third-party ICT services supporting critical or important functions**, in addition to maintaining a register of all third-party ICT services arrangements (similarly to the register of material outsourcings).

In certain instances, financial entities may themselves act as an ICT service provider, such as where they provide platform solutions to other financial institutions as their customers. For example, where a bank provides a portfolio management platform to investment firms, it will be a service provider of ICT services (and possibly a critical one). This will impact how regulatory expectations will fall, the contractual positions they take with customers and the policies and procedures they must have in place.

Key considerations for contract remediation

Designing a suitable and efficient path to contract remediation can be a daunting task, especially where financial entities have hundreds of contracts in place with technology vendors. To achieve this, and based on our experience, the contract remediation project should be organised methodically into phases and take account of the following key considerations:

1. Assessment of the contract portfolio should identify ICT service types, criticality or importance of the ICT services, and in-scope EU territories. It may help to segment contracts into those which are brief, standard-form technology contracts and other, more complex outsourcing contracts.
2. Where possible, automating the diligence of individual contracts can create efficiencies, though it is critical that the outputs of automated reviews are validated.
3. Preparing a contract addendum may be the most efficient method of remediation, which is then adapted for individual contracts, and firms can leverage any addenda previously used for compliance with mandatory contract terms for regulated outsourcings. Such an addendum could take a modular form which enables jurisdiction-specific issues to be added or removed, eg to address nuances around incident reporting, and also to adapt remediation for each contract based upon the outcome of diligence.
4. The mandatory contract terms under DORA may be divided into "legal" terms (eg audit provisions, termination rights) and "business" terms (eg service definitions). For the latter, a bespoke remediation process may need to be agreed and documented with applicable business SMEs, to be completed before 17 January 2025 or as soon as possible thereafter.

Now, more than ever, it is extremely valuable to understand how solutions and/or services are integrated into banking operations in order to comply with DORA and, more broadly, to address the evolving challenges to ensuring operational resiliency.

Our experience is that this is currently an area in flux. The vendor community is acknowledging the changes faced by their customers; however, negotiations in respect of remediation can be challenging. One key factor behind these challenges is that vendors and customers are seeking to uniformly apply their own DORA-compliant terms, across their agreements. In summary, the remediation process is still relatively immature, and an industry-wide view of appropriate, compliant contract positions will continue to be developed just as it has been for the implementation of regulatory requirements around outsourcing.

***Mike Pierides**, partner, **Oliver Bell**, Associate, and **James Mulligan**, Associate, all at Morgan Lewis LLP's London office.*

Endnotes

1. McKinsey, *Europe's new resilience regime: The race to get ready for DORA*, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/europes-new-resilience-regime-the-race-to-get-ready-for-dora.
2. European Central Bank, *Outsourcing Register: Annual Horizontal Analysis* (21 February 2024), https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.outsourcing_horizontal_analysis_202402~2b85022be5.en.pdf.
3. *Final Report on EBA Guidelines on Outsourcing Arrangements* (February 2019), https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf.