MAPLES GROUP

UPDATE

Four Months to Go: Key Steps to Implement DORA

What You Need to Know

- The Digital Operational Resilience Act ("DORA")[1] imposes new requirements on certain financial entities relating to information and communication technology ("ICT") management.
- Impacted firms should take certain action prior to the implementation deadline of 17 January 2025.

Background

DORA creates a European regulatory framework to strengthen the financial sector's resilience to ICT disruptions and threats[2]. The implementation deadline is 17 January 2025.

DORA will apply to a wide range of financial entities and covers most regulated firms ("Firms"), including investment firms, fund managers, payment institutions, credit institutions, trading venues, insurance undertakings and re-insurance undertakings. It will impose new requirements on Firms relating to the management of ICT risk; ICT incidents; digital operational resilience testing; and the management of third-party ICT risk.

This update outlines the key action points Firms should address to prepare for its implementation.

Conduct a Gap Analysis

Many Firms have already taken steps to improve their digital operational resilience to comply with applicable requirements under national law, for example, the Central Bank of Ireland's ("Central Bank"') Cross Industry Guidance on Operational Resilience (CP140). Similarly in Luxembourg many regulated entities are subject to rules governing ICT incident reporting, such as under the circular 24/847 of the Commission de Surveillance du Secteur Financier ("CSSF"). DORA, however, is more prescriptive and contains more detailed requirements on digital operational resilience which may require Firms to update their existing systems, policies and practices.

To determine potential compliance gaps, Firms should undertake a gap analysis on their current ICT frameworks, including their existing ICT systems, policies and procedures, to determine what elements need to be updated to comply with DORA.

Develop an ICT Risk Management Framework

DORA requires Firms to update their governance policies to ensure effective and prudent management of ICT risk and to develop and implement a sound, comprehensive and well-documented ICT risk management framework as part of their broader risk management system. Therefore, Firms will need to assess their ICT supported business functions, roles and responsibilities; the information assets and ICT assets supporting those functions; their roles and dependencies in relation to ICT risk; and, on an ongoing basis, identify all sources of ICT risk.

[1] Regulation (EU) 2022/2554

[2] For an overview of the DORA framework, see our previous legal update: https://maples.com/knowledge/dora-new-eu-operational-resilience-regime-for-the-financial-sector

Appropriate policies and processes will also need to be developed on monitoring and controlling the security and functioning of ICT systems, the detection of anomalous activities and ICT business continuity. Firms should also ensure that they have capability to gather information on vulnerabilities, cyber threats and ICT-related incidents, and analyse the impact that they are likely to have on their digital operational resilience.

Scope of ICT Third-Party Service Providers

Entities providing digital, information or communication technology services, i.e. ICT services, to Firms will be considered ICT third-party service providers within the scope of DORA.

This will include cloud service providers, data analytics firms and a range of other technology vendors. It may also include other regulated financial services firms as an entity cannot be automatically deemed out of scope on the basis that it is primarily a provider of regulated financial services (rather than a dedicated provider of technology services). It must therefore be determined, in each case, whether a service provider is providing ICT services.

Third-Party ICT Services

DORA expects Firms to manage third-party ICT risk as a key principle within their ICT risk management frameworks. This includes adopting and regularly reviewing a strategy on ICT third-party risk, and a policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers. Firms will also need to maintain registers of information on all contractual arrangements on the use of ICT services provided by ICT third-party service providers.

Firms will also need to assess and, if necessary, update their existing contractual arrangements with third-party ICT service providers to ensure that they include specific elements required by DORA.

Firms should also assess the adequacy of their due diligence procedures with third-party ICT service providers.

Proportionality

DORA allows Firms to apply proportionality when implementing the new rules by considering their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations. Firms should undertake a proportionality assessment identifying any aspects of DORA it is disapplying and the rationale for this.

Manage ICT Risk Incidents

To meet their DORA ICT risk management obligations, Firms will need to implement ICT-related incident management processes to detect, manage and notify ICT-related incidents. Firms will also be expected to record all ICT incidents and significant cyber threats.

'Major' ICT-related incidents must be reported to their relevant national competent authority within prescribed timeframes.

To ensure that notifications are made within the prescribed timeframes, Firms should put in place policies and procedures addressing the detection, management, recording and assessment of ICT-related incidents and the Firm's processes for reporting major incidents.

Implement ICT Testing Programmes

Firms should implement or assess the adequacy of their existing digital operational resilience testing programmes for ICT tools and systems and make any necessary DORA compliance updates. Firms should also ensure that testing on all ICT systems and applications which support critical or important functions is carried out at least annually.

Firms should also determine whether they are subject to the obligation to carry out Threat-Led Penetration Testing ("TLPT") every three years. The requirement to conduct TLPT is based on various impact-related and systemic character-related factors as well as a Firm's ICT risk profile.

Regulatory Engagement

EU regulators have commented on DORA readiness and engaged with industry across the EU. For example, in Luxembourg, on 19 August 2024, the CSSF launched a DORA Readiness Survey to gain a better view of the readiness of Firms it supervises for the introduction of DORA.

On the Irish side, given the late timing of finalising some technical standards, the Central Bank has called for a more measured regulatory approach during DORA's initial implementation phase. This call for a "Day 1/Day 2" perspective should be welcomed by Firms facing challenges in fully implementing DORA obligations on time.

How we can Help

We are supporting clients across different industry sectors implementing DORA, including providing perimeter advice on the scope of DORA and the interpretation of core concepts within the new regime, delivering training to boards and staff, updating contracts with ICT providers (including intra-group and sub-contracting arrangements) and amending policies and procedures to bring firms' compliance and risk management frameworks in line with DORA.

Further Information

For further information, please liaise with your usual Maples Group contact or any of the persons listed below.

Dublin

Stephen Carty
+353 1 619 2023
stephen.carty@maples.com

Lorna Smith
+353 1 619 2125
lorna.smith@maples.com

Philip Keegan
+353 1 619 2122
philip.keegan@maples.com

Alison Gibney
+353 1 619 2158
alison.gibney@maples.com

Luxembourg

Johan Terblanche
+352 2855 1244
johan.terblanche@maples.com

Donnchadh McCarthy
+352 2855 1222
donnchadh.mccarthy@maples.com

September 2024