MAPLES GROUP

UPDATE

DORA: Six Key Action Points for Firms

What you Need to Know

- The Digital Operational Resilience Act ("DORA")[1] will apply from 17 January 2025.
- There are several measures regulated firms should action in 2024 prior to its introduction.

Background

DORA entered into force on 16 January 2023, creating a European regulatory framework to strengthen the financial sector's resilience to information and communication technology ("ICT") disruptions and threats[2].
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.

1. Conduct a Gap Analysis

Many Firms have already taken steps to improve their digital operational resilience in order to comply with CP140 (the Central Bank of Ireland's ("Central Bank") Cross Industry Guidance on Operational Resilience). DORA, however, is more prescriptive than CP140 and contains more detailed requirements on digital operational resilience which may require Firms to update their existing systems, policies and practices.

To determine where potential compliance gaps may lie, 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.

2. Develop an ICT Risk Management Framework

DORA will require 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. As part of this process, Firms will need to carry out assessments of 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.

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 and cyber threats, ICT-related incidents and analyse the impact they are likely to have on their digital operational resilience.

[1] Regulation (EU) 2022/2554
[2] For an overview of the DORA framework, see our previous Client Update: https://maples.com/en/knowledge-centre/2023/1/dora-new-eu-operational-resilience-regime-for-the-financial-sector

3. Manage ICT Risk Incidents

To meet their ICT risk management obligations under DORA, Firms will need to establish and 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 the Central Bank within prescribed timeframes. The initial report must be made within four hours from the moment of classification of the incident as major, but no later than 24 hours from the time of detection of the incident. A subsequent intermediate report must be made within 72 hours from the classification of the incident as major, or when regular activities have been recovered and business is back to normal. The final report must be submitted no later than one month from the classification of the incident as major.

In order to ensure that notifications can be made within the prescribed timeframes, we recommend Firms put in place policies and procedures specifically addressing the detection, management, recording and assessment of ICT-related incidents and the Firm's processes for reporting major incidents.

4. 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 updates to comply with DORA. 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 ICT risk related factors regarding the Firm.

If a Firm is required to carry out TLPT, it should put in place the necessary arrangements to carry out such testing. Firms may use either internal or external testers for carrying out TLPT, however if a firm uses internal testers, it must contract external testers to conduct TLPT every three tests.

5. 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, at entity level and at sub-consolidated and consolidated levels, a register of information on all contractual arrangements on the use of ICT services provided by ICT third-party service providers. The required form of this register will be set out in level 2 regulations due to be published in July 2024. However, given the volume of information required to be inputted to the register we recommend Firms begin collating this information well in advance of DORA's application.

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 the specific elements required by DORA, such as:

(a) complete descriptions of all functions and ICT services to be provided, including details of any subcontracting;
(b) details of the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed;
(c) provisions on the availability, authenticity, integrity, confidentiality, access, recovery and return of data;
(d) service level descriptions; and
(e) various assistance obligations.

Firms should also assess the adequacy of their due diligence procedures with third-party ICT service providers and, if applicable, subcontractors.

6. Information Sharing

Under DORA, Firms may exchange among themselves cyber threat information and intelligence to enhance their digital operational resilience. If Firms intend to participate in these arrangements, they should put in place appropriate agreements which respect business confidentiality and ensure they comply with competition law as well as the General Data Protection Regulation.

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

April 2024