MAPLES GROUP

UPDATE

DORA: New EU Operational Resilience Regime for the Financial Sector

On 28 November 2022, the Council of the EU adopted the Digital Operational Resilience Act ("DORA") legislative package which creates a European regulatory framework to strengthen the financial sector's resilience to information and communication technology ("ICT") disruptions and threats.

Overview

DORA consists of both a regulation and a directive which, once implemented, will form a targeted set of quantitative rules for the protection, detection, recovery and repair capabilities against ICT-related incidents by financial sector firms.

Notably, certain unregulated technology providers, such as ICT third-party service providers, are now within the direct scope of financial regulatory requirements for the first time.

The key measures introduced by DORA can be categorised as follows:

- ***ICT Risk Management***
  Under DORA, financial entities are required to have sound, comprehensive and well-documented ICT risk management frameworks as part of their overall risk management system. This framework should include strategies, policies, procedures and protocols that can protect all information and ICT assets to allow firms to quickly and efficiently address risks, maintaining high levels of operational resilience.

- ***ICT-Related Incident Management***
  Financial entities in scope are required to define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents. This includes recording all incidents and significant cyber-threats, putting in place early warning indicators and establishing processes to manage incidents according to their priority and severity.

- ***Digital Operational Resilience Testing***
  The level of testing required will depend on the nature, scale and complexity of the entity in scope, though in all cases independent testing is necessary to assess preparedness for handling ICT-related incidents, and identifying weaknesses, deficiencies and gaps in digital operational resilience. As well as annual testing, certain financial entities will be required to undertake additional advanced testing at least every three years.

- ***Managing of Third-Party Risk***
  Financial entities are required to regularly monitor the ability of a third-party service provider to securely provide services without impacting the firm's overall operational resilience. The key to managing third-party risk will be harmonising contracts between the firm and each third-party service provider, ensuring that, at a minimum, the firm can monitor risks that could emerge given dependence on the stability, functionality, availability and security of the services received.

Many of the above measures – particularly on third-party risk and operational resilience – should

already be familiar to Irish-regulated financial services firms such as: pre-outsourcing due diligence, assessments of ICT third-party concentration risk, requirements applicable to contractual arrangements with ICT third-party service providers, disaster recovery, governance requirements and reporting of major ICT-related incidents.

DORA also introduces new powers for financial supervisors to oversee risks flowing from financial entities' dependency on ICT third-party service providers.

Scope

DORA is far-reaching and will apply to a wide range of financial entities and covers most regulated firms including: investment firms, payment institutions, credit institutions, trading venues, insurance undertakings and re-insurance undertakings.

As mentioned above, previously unregulated entities, such as ICT third-party service providers, will also be in scope.

Timeframe

The DORA regulation and directive were published in the Official Journal of the EU on 27 December 2022 and came into force on 17 January 2023. The DORA regulation comes into effect directly on 17 January 2025 and the DORA directive must be transposed into national law by EU member states by the same date.

Proportionate Application

Financial entities must adopt the rules in a proportionate manner, taking into account the firm's size and overall exposure to digital risk, and the nature, scale and complexity of their services, activities and operations.

A more proportional, simpler set of rules will apply to "small and non-interconnected firms" which meet the conditions in Article 12(1) of the Investment Firm Regulations ("IFR")[1].

"Microenterprises" also benefit from a more flexible regime and are exempt from the application of certain requirements.

DORA and the Central Bank's Guidance on Operational Resilience

We previously discussed the Central Bank's Cross Industry Guidance on Operational Resilience ("Guidance") in our December 2021 client update[2].

The Guidance applies only to regulated financial service providers ("RFSPs"), as defined in Section 2 of the Central Bank Act 1942. Such RFSPs are expected to adhere to the Guidance by 1 December 2023. These firms may therefore already be in the process of enhancing their operational resilience frameworks.

The Guidance is broader in scope than DORA as it relates to operational resilience for all types of disruptions – not just ICT-related disruptions. However, DORA is generally more prescriptive and exceeds the Guidance requirements.

The Central Bank provided firms with reassurance at the consultation stage that there were no contradictions between the Guidance and the (then-forthcoming) DORA legislation. It also committed to update the Guidance to align with relevant international operational resilience policy developments.

Therefore any action by firms to comply with the Guidance should be compatible with the measures introduced by DORA.

Next Steps

The European Supervisory Authorities are to develop supporting regulatory technical standards ("RTS"). The RTS on ICT risk management (Article 15) will establish thorough rules on security policies,

[1] Regulation (EU) 2019/2033
[2] https://maples.com/en/knowledge-centre/2021/12/central-bank-of-ireland-publishes-operational-resilience-guidance

firm governance and event detection procedures, while also specifying the required content of business continuity plans. Further RTS on classifying ICT-related incidents and cyber threats (Article 18), ICT incident reporting (Article 20), advanced digital operational resilience testing (Article 26) and third-party risk management (Article 30) will also be drafted.

The various draft RTS are to be delivered to the European Commission 12-18 months after DORA comes into force. Should that timeframe be followed, firms will only have full clarity regarding their requirements under DORA six months before they are expected to be in full compliance.

With this in mind, firms should prepare for the introduction of the new regime in advance of the publication of the RTS. This may involve conducting a gap analysis of the requirements against their current processes and procedures to identify the extent of the work required to ensure compliance with DORA. This can be further assessed once the RTS are available.

How We Can Help

We are currently working with clients to design and implement robust operational resilience and business continuity frameworks to address the Guidance and DORA, including drafting policies and procedures, reviewing third-party arrangements and contracts, assessing oversight, monitoring and testing frameworks, and advising on how to apply proportionality and interpretation of some of the key provisions and how they impact a particular firm's business model.

Further Information

Further information on our Irish Financial Services Regulatory Group, and the services we provide is available on our website[3] and in our brochure[4].

[3] https://maples.com/en/services/specialty-services/irish-financial-services-regulatory

[4] https://maples.com/-/media/files/pdfs/articles-and-chapters/financial-services-regulatory-group---core-services.pdf

If you would like to learn more, please contact 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

January 2023