McCann FitzGerald

Briefing
DORA - Digital Operational Resilience Act

This briefing was produced by the Institute of Directors in association with McCann FitzGerald LLP for use in Ireland. McCann FitzGerald LLP is one of Ireland's premier law firms, providing a full range of legal services to many of Ireland's leading businesses. Clients include international organisations, major domestic concerns, emerging Irish companies and clients in the State and semi-State sectors.

Europe's Digital Operational Resilience Act will introduce detailed and comprehensive rules on digital operational resilience at EU level for EU financial entities. This briefing highlights the key elements of this new framework which firms should be aware of.

What is DORA?

The Digital Operational Resilience Act ("**DORA**") aims to consolidate and upgrade information and communications technology ("**ICT**") risk requirements in the financial sector in a single European legal act. DORA will introduce targeted rules in respect of ICT risk-management capabilities, incident reporting, operational resilience testing and ICT third-party risk monitoring.

For the purposes of DORA, '*digital operational resilience*' is defined as the '*ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third–party service providers, the full range of ICT–related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions*'.

When will DORA take effect

DORA will take effect on 17 January 2025.

Who will DORA apply to?

DORA will apply to a wide range of financial entities, including:

- credit institutions;
- payment institutions and electronic money institutions;
- investment firms;
- AIFMs and UCITS management companies; and
- (re)insurance undertakings, (re)insurance intermediaries and ancillary insurance intermediaries.

It should be noted that DORA will apply in a proportionate manner taking into account a financial entity's size and overall risk profile, and the nature, scale and complexity of its services, activities and operations.

What does DORA do?

DORA introduces uniform requirements concerning:

- ICT risk management;
- reporting of major ICT–related incidents and notifying, on a voluntary basis, significant cyber threats to the competent authorities;
- digital operational resilience testing;
- information and intelligence sharing in relation to cyber threats and vulnerabilities;
- measures for the sound management of ICT third–party risk;
- requirements in relation to the contractual arrangements concluded between ICT third–party service providers and financial entities; and
- rules for the establishment and conduct of the oversight framework for critical ICT third–party service providers.

What are the key aspects of DORA to be aware of?

Role of the management body

DORA will require the management body of a financial entity to hold ultimate responsibility for managing ICT risk. Members of the management body will need to actively keep up to date with knowledge and skills to understand and assess ICT risk and its impact on the operations of a financial entity, including by following specific training on a regular basis, commensurate to the ICT risk being managed.

Risk management framework

Financial entities will be required to put in place a sound, comprehensive and well–documented ICT risk management framework. The ICT risk management framework must be documented and reviewed at least once a year, or periodically in the case of microenterprises, as well as upon the occurrence of major ICT–related incidents, and following supervisory instructions or conclusions obtained from digital operational resilience testing or audit processes.

Protection and prevention

Financial entities will be required to continuously monitor and control the security and functioning of ICT systems and tools and minimise the impact of ICT risk on ICT systems through the application of appropriate security tools, policies and procedures. Financial entities will also be required to have in place mechanisms to promptly detect anomalous activities and to identify potential material single points of failure.

Response and recovery

Financial entities will be required to put in place a comprehensive ICT business continuity policy. Financial entities will also need to regularly review this policy and ICT response and recovery plans.

Learning and evolving

DORA will require financial entities to put in place capabilities and staff to gather information on vulnerabilities and cyber threats, ICT–related incidents and analyse the impact they are likely to have on an entity's digital operational resilience. Financial entities will be required to put in place post ICT–related incident reviews after a major ICT–related incident disrupts their core activities.

Communication

Financial entities will be required to have crisis communication plans in place which will enable a responsible disclosure of, at least, major ICT–related incidents or vulnerabilities to clients and counterparts as well as to the public, as appropriate.

Simplified ICT risk management framework

Certain smaller and non-interconnected financial entities will be permitted to employ a simplified ICT risk management framework. The European Supervisory Authorities (the "**ESAs**") have developed draft regulatory technical standards ("**RTS**") in order to specify details of this simplified framework.

ICT–related incident management process and classification

Financial entities will be required to define, establish and implement an ICT–related incident management process to detect, manage and notify ICT–related incidents. Financial entities will also need to classify ICT–related incidents and determine their impact based on specific criteria, including the number and/or relevance of clients or financial counterparts affected, the amount or number of transactions affected by the incident and the criticality of the services affected.

Reporting of major ICT–related incidents and voluntary notification of significant cyber threats

Financial entities will be required to report major ICT–related incidents to the relevant competent authority. Financial entities may, on a voluntary basis, notify significant cyber threats to the relevant competent authority when they deem the threat to be of relevance to the financial system, service users or clients. The ESAs have developed draft RTS in order to establish reporting criteria, including materiality thresholds for reporting.

Digital operational resilience testing

DORA will require financial entities to establish, maintain and review a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk-management framework. Financial entities, other than microenterprises, will need to ensure that appropriate tests are conducted on all ICT systems and applications supporting critical or important functions on at least a yearly basis. Certain financial entities will be required to carry out threat-led penetration testing ("**TLPT**") covering several or all critical or important functions of a financial entity. The ESAs are mandated to develop RTS in respect of TLPT.

Management of ICT third-party risk

DORA also sets out general principles for the management of ICT third-party risk which includes adopting and regularly reviewing an ICT third–party risk strategy, maintaining a register of information in relation to all contractual arrangements with ICT third-party service providers and reporting information on ICT third-party service providers to the competent authority. DORA will require contractual arrangements with ICT third-party service providers to include specific termination provisions and also require financial entities to put in place exit strategies.

Oversight framework of critical ICT third–party service providers

DORA introduces a new oversight framework for critical ICT third–party service providers. The ESAs will designate the ICT third–party service providers that are critical for financial entities and appoint an ESA as 'Lead Overseer' for each critical ICT third–party service provider. An oversight forum will also be established to support the Lead Overseers.

DORA Policy Products

On 19 June 2023, the ESAs launched a public consultation on the first batch of policy products under DORA (here). This consultation includes four draft RTS and one set of draft implementing technical standards ("**ITS**"). The ESAs state that these technical standards aim to ensure a consistent and harmonised legal framework in the areas of ICT risk management, major ICT-related incident reporting and ICT third-party risk management. The consultation runs until 11 September 2023.

What do financial entities need to do now?

While DORA will not apply until 17 January 2025, given the scope of DORA and the likely need to engage with ICT third-party service providers, it would be prudent for financial entities to prepare for compliance as soon as possible.

In scope financial entities should consider:

- establishing a DORA implementation team which benefits from management support and buy-in;
- conducting a gap analysis of existing ICT risk management frameworks against DORA requirements;
- reviewing ICT contractual arrangements, assessing ICT third-party risk;
- commencing engagement with ICT third-party service providers, as required; and
- less mature organisations may need to commence the process of conducting a thorough cyber hygiene review.

Further information is available from

Financial Services Regulation

Josh Hogan
Partner
+353 1 607 1720
josh.hogan@
mccannfitzgerald.com

Darragh Murphy
Partner
+353 1 607 1433
darragh.murphy@
mccannfitzgerald.com

Judith Lawless
Partner
+353 1 607 1256
judith.lawless@
mccannfitzgerald.com

Fergus Gillen
Partner
+353 1 611 9146
fergus.gillen@
mccannfitzgerald.com

Adrian Farrell
Partner
+353 1 607 1312
adrian.farrell@
mccannfitzgerald.com

Asset management and investment funds

Mark White
Partner, Head of Investment Management Group
+353 1 607 1328
mark.white
@mccannfitzgerald.com

Iain Ferguson
Partner
+353 1 607 1414
iain.ferguson
@mccannfitzgerald.com

Hugh Beattie
Partner, Head of London Office
+44 20 7621 1000
hugh.beattie
@mccannfitzgerald.com

Morgan Dunne
Partner
+353 1 607 1250
morgan.dunne
@mccannfitzgerald.com

Anna Moran
Consultant
+353 1 607 1494
anna.moran
@mccannfitzgerald.com

Tony Spratt
Consultant
+353 1 607 1367
tony.spratt
@mccannfitzgerald.com

Technology and innovation

Adam Finlay
Partner
+353 1 607 1795
adam.finlay@
mccannfitzgerald.com

INSTITUTE OF DIRECTORS
IN IRELAND

Institute of Directors in Ireland, Europa House, Harcourt Street, Dublin 2
01 411 0010 | info@iodireland.ie | www.iodireland.ie

1891_06_2023