A&L Goodbody

A CLOSER LOOK AT THE EU'S DORA

ISSUES FOR FINANCIAL INSTITUTIONS TO CONSIDER

INTRODUCTION

The regulation of risk arising from the use of digital technology has been an area of increasing focus for the EU. In this briefing, we take a closer look at the latest regulatory developments in the area of digital resilience in the regulated financial sector.

Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (**DORA**), together with Directive (EU) 2022/2556 as regards digital operational resilience for the financial sector (**DORA Directive**), entered into force on 16 January 2023. DORA will directly apply in EU Member States from 17 January 2025 and Member States are required to implement the DORA Directive by that date.

In this document we provide an overview of key DORA requirements, together with an analysis of how the requirements in respect of ICT risk management and ICT third-party risk management align with existing Central Bank of Ireland (**CBI**) cross industry guidelines.

OVERVIEW

DORA is a cross-sectoral EU Regulation, applying to a wide range of regulated financial entities. It aims to mitigate ICT risk by enhancing financial entities' technology and cyber risk management and resilience. DORA creates a regulatory framework under which all in-scope firms need to ensure they can withstand, respond to, and recover from, ICT-related disruptions and threats, including cyber-attacks. DORA aims to achieve a high common level of digital operational resilience across the EU financial sector by consolidating and upgrading financial entities' ICT risk requirements as part of the operational risk requirements that have, up to this point, been addressed separately in various EU legal acts.

SCOPE

DORA applies to most 'financial entities' regulated under EU law, including credit institutions, payment institutions, investment firms, crypto-asset service providers, trading venues, and insurance and reinsurance undertakings.

DORA also applies to '*ICT third-party service providers*', i.e. undertakings providing digital and data services through ICT systems to one or more internal or external users on an ongoing basis (**ICT Services**). This would include undertakings providing services such as cloud platforms, data analytics and data audit services to in-scope financial entities.

KEY AREAS

DORA expressly addresses ICT risk by setting down targeted rules for the following five key areas

01 ICT RISK MANAGEMENT

02 ICT THIRD-PARTY RISK MANAGEMENT

03 INCIDENT REPORTING

04 DIGITAL OPERATIONAL RESILIENCE TESTING

05 INFORMATION AND INTELLIGENCE SHARING

KEY AREAS

01 / ICT RISK MANAGEMENT

DORA OBLIGATIONS

Financial entities subject to DORA must have an internal governance and control framework in place that ensures an effective and prudent management of ICT risks. This is in order to achieve a high level of digital operational resilience. The entity's management body bears the ultimate responsibility for managing its ICT risk. In particular, the management body must define, approve, oversee and be responsible for the implementation of all arrangements related to the entity's ICT risk management framework.

The ICT risk management framework must include strategies (including a digital operational resilience strategy), policies, procedures, ICT systems protocols and tools that are necessary to adequately protect all ICT assets and address:

- identification of all ICT supported business functions, roles and responsibilities and all sources of ICT risk cyber threats and ICT vulnerabilities
- protection and prevention by continuously monitoring and controlling the security and functioning of ICT systems and tools and minimising the impact of ICT risk through the deployment of appropriate ICT security tools, policies, and procedures
- detection of anomalous activities, including ICT network performance issues and ICT-related incidents, and to identify potential material single points of failure
- response and recovery by putting in place a comprehensive ICT business continuity policy
- backup policies and procedures and restoration and recovery methods and procedures
- learning and evolving by gathering information on vulnerabilities and cyber threats, ICT-related incidents, and analysing the impact they are likely to have on digital operational resilience
- having in place crisis communication plans for the responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts, as well as to the public, as appropriate

ALIGNMENT WITH EXISTING CBI GUIDELINES

The ICT risk management obligations under DORA broadly align with those in the CBI Cybersecurity Guidelines. In particular, the management body bears ultimate responsibility for managing the financial entity's ICT Risk, and firms must put in place, and maintain, a comprehensive ICT risk management framework.

Whilst there is broad alignment, the prescriptive obligations under both DORA and the CBI Cybersecurity Guidelines are not identical. For example, DORA requires a 'digital operational resilience strategy' as part of the ICT risk management framework, which is not expressly required under the CBI Guidelines (although they do provide for a cyber risk strategy). Firms should therefore review their existing governance framework in respect of ICT risk management, along with their ICT risk management frameworks, to ensure DORA compliance.

KEY AREAS

02 / ICT THIRD-PARTY RISK MANAGEMENT

DORA OBLIGATIONS

DORA sets out prescriptive obligations on financial entities and ICT third-party service providers in respect of ICT third-party services, and enhanced obligations in respect of ICT third-party services supporting critical or important functions of financial entities.

Financial entities are obliged to manage ICT third-party risk as an integral component of their ICT risk management framework. DORA sets out prescriptive obligations regarding the adoption of a strategy on ICT third-party risk, maintenance of a register of information in respect of all ICT third-party contract service providers, annual reporting requirements, audit requirements and ensuring ICT third-party service providers comply with appropriate information security standards. DORA also specifies mandatory terms for inclusion in contractual arrangements on the use of third-party ICT services, from pre-contractual assessment to termination.

DORA specifies additional terms for inclusion in contractual arrangements on the use of ICT third-party services supporting critical or important functions. These are inclusive of full service-level descriptions, requirements for the ICT third-party service provider to implement and test business contingency plans, the right for the financial entity as customer to monitor, on an ongoing basis, the ICT third-party service provider's performance, and exit strategies.

ALIGNMENT WITH EXISTING CBI GUIDELINES

The requirement for financial entities to distinguish between ICT third-party services generally and those supporting critical or important functions aligns with the existing European Banking Authority (**EBA**) and CBI guidance on outsourcing. In particular, the definitions of 'critical or important function' are broadly aligned. The CBI's Cross-Industry Guidance on Outsourcing (the **CBI Outsourcing Guidance**) currently provides a more prescriptive methodology for the assessment of criticality or importance of activities or functions; however, the regulatory technical standards (**RTS**) to be drafted by the European Supervisory Authorities (**ESAs**) in this regard will be of considerable benefit to financial entities conducting this integral assessment under DORA.

We see significant alignment between the DORA requirements in respect of ICT third-party services and the existing EBA, EIOPA and CBI guidance on outsourcing, in particular in respect of the following:

- the proposed proportionate approach to the management of ICT third-party risk
- the financial entity's retention of responsibility for compliance with, and the discharge of, all obligations under DORA and applicable financial services law
- the requirement to maintain and update a register of information in relation to all contractual arrangements with ICT third-party service providers
- the addressing of key risks such as sub-outsourcing risk, concentration risk, offshoring risk, and data security (although 'sensitive data risk' is not directly addressed in DORA)
- the prescriptive approach to mandatory provisions in contractual arrangements on the use of ICT third-party services supporting critical or important functions
- it is of note, however, that DORA is more prescriptive than current CBI expectations in respect of required provisions of other contractual arrangements for ICT third-party services.

This means that a greater focus may now be placed on such contracts in order to address the specific requirements of DORA, which are aimed at all ICT agreements (not only applicable to critical/important ones).

Whilst there is this alignment, DORA and the existing regulatory guidance are not identical and financial entities therefore need to carefully consider the impact of any differences between the two. Firms will need to review their classification of ICT third-party services relating to 'critical or important' functions, as well as their current ICT third-party contracts, risk management frameworks, policies and strategies. Firms should also review and update, as necessary, their existing contractual arrangements on the use of ICT third-party services to ensure compliance. The forthcoming ESA RTSs should assist with this review. The extent of this review and updating exercise may vary from one institution to the next, but firms should ideally start planning now for the application of DORA in January 2025 to allow time for any necessary remediation exercise to take place.

KEY AREAS

03 / INCIDENT REPORTING

Financial entities are subject to the following four key obligations in respect of DORA incident reporting:

- ICT-related incident management process: financial entities must define, establish, and implement ICT-related incident management process to detect, manage and notify ICT-related incidents
- classification of ICT-related incidents and cyber threats: financial entities must classify ICT-related incidents and determine their impact based on specific criteria such as the number and/or relevance of clients or financial counterparts affected, and its duration and economic impact
- reporting of major ICT-related incidents: RTS will specify materiality thresholds and the content of reports, and ITS will establish standard forms, templates, and procedures for reporting
- voluntary notification of significant cyber-threats to the relevant competent authority: where financial entities deem the threat to be of relevance to the financial system, service users, or clients

04 / DIGITAL OPERATIONAL RESILIENCE TESTING

Financial entities must establish, maintain, and review a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk management framework. DORA sets out prescriptive requirements in respect of:

- testing of ICT tools and systems
- advanced testing of ICT tools, systems and processes based on threat-led penetration testing (**TLPT**)
- testers for the carrying out of TLPT

KEY AREAS

05 / INFORMATION AND INTELLIGENCE SHARING

Financial entities may exchange cyber thread information and intelligence amongst themselves, including indicators of compromise, tactics, techniques, procedures, cyber security alerts and configuration tools. This is provided that such information and intelligence sharing:

- aims to enhance the digital operational resilience of financial entities
- takes place within trusted communities of financial entities
- protects the potentially sensitive nature of the information shared and complies with GDPR obligations

ENFORCEMENT OF DORA

Compliance with DORA will be supervised by the competent authority responsible for overseeing the in-scope firm. DORA grants these competent authorities all supervisory, investigatory, and sanctioning powers necessary to fulfil their supervisory duties, including the following broad enforcement powers:

- to access, receive or take copy of any document or data in any form
- to carry out on-site inspections and investigations, including summoning individuals for explanations or interviews
- requiring corrective and remedial measures for breaches of DORA.

Member States must also establish appropriate administrative penalties and remedial measures for breaches of DORA, to include at least the following;

- orders requiring the firm/individual to cease any conduct which contravenes DORA and to prevent any repetition of that conduct
- requiring a temporary or permanent cessation of any practice or conduct contrary to DORA and to prevent any repetition of that practice or conduct
- adopting any measures, including pecuniary, to ensure that firms comply with DORA
- requiring, insofar as national law allows, data traffic records held by a telecommunications operator where there is a reasonable suspicion of a breach of DORA
- issuing public notice, including public statements indicating the identity of the firm/individual and the nature of the breach
- these enforcement and administrative powers may be imposed on members of the management body or any other individual who is responsible for the breach of DORA by a firm. These enforcement powers are in addition to any action the CBI may take against senior members of a firm under the Individual Accountability Framework.

A&L Goodbody has a host of resources on our dedicated Individual Accountability Framework hub.

NEXT STEPS

DORA will apply from 17 January 2025 and the ESAs are tasked with publishing the technical standards in advance of that date. These will be delivered in two tranches and are due to be finalised by 17 January 2024 and 17 July 2024 respectively.

On 19 June 2023, the ESAs published drafts of the first of the two tranches of technical standards for public consultation, which closed on 11 September 2023. The consultation on the second tranche is expected to launch in November or December of this year. The technical standards will assist with the implementation of DORA's regulatory obligations, but firms should keep in mind that these standards will not be finalised until much closer to the DORA implementation deadline.

Whilst there is clear alignment between DORA obligations and existing regulatory requirements, firms will need to assess the impact of any differences and take account of DORA's wider scope and more prescriptive approach. It is important that financial entities review their existing operational resilience, outsourcing and ICT risk management frameworks, as well as existing relevant ICT contracts and templates, and plan how they will make the changes needed to comply ahead of the January 2025 implementation date.

KEY CONTACTS

For further information in relation to this topic, please contact your usual ALG contact or any of the practitioners set out below.

FINANCIAL REGULATION ADVISORY


Patrick Brandt
Partner


Kevin Allen
Partner


Christopher Martin
Of Counsel


Louise Hogan
Associate

COMMERCIAL & TECHNOLOGY


Mark Ellis
Partner


Andrew Sheridan
Partner


Chris Bollard
Partner

INSURANCE


Laura Mulleady
Partner


James Grennan
Partner


Sinéad Lynch
Partner

DISPUTES


Chloe Culleton
Partner


Dario Dagostino
Partner


Mark Devane
Partner


Laura Corrigan
Senior Associate

A&L Goodbody

DUBLIN

A&L Goodbody LLP
International Financial Services Centre
3 Dublin Landings
North Wall Quay
Dublin 1
Ireland

BELFAST

A&L Goodbody Northern Ireland LLP
42 - 46 Fountain Street
Belfast BT1 5EF
Northern Ireland

LONDON

A&L Goodbody
Augustine House
Austin Friars
London EC2N 2HA
United Kingdom

NEW YORK

A&L Goodbody LLP
The Chrysler Building
405 Lexington Avenue
New York, NY 10174
USA

SAN FRANCISCO

A&L Goodbody LLP
580 California Street
Suite 1200
PMB #86803
San Francisco, CA 94104
USA

PALO ALTO

A&L Goodbody LLP
228 Hamilton Avenue
Palo Alto, CA 94301
USA

© A&L Goodbody LLP 2023. The contents of this document are limited to general information and not detailed analysis of law or legal advice and are not intended to address specific legal queries arising in any particular set of circumstances.