DORA – One Month to Go

Authors:
Darina Colhoun, Director EY & member of Compliance Institute's Payments & Fintech Working Group.

David Spollen, Director EY.

Susana Rosa,
Senior Manager EY.

"Digital operational resilience is a fundamental underpinning of a resilient and well-functioning financial system supporting the economy and serving the needs of citizens. Financial services are fundamentally about information and data. So, the threat surface is large, the risks are significant and increasing, and the potential impact is great."

- Gerry Cross, Central Bank of Ireland Director of Financial Regulation, Policy and Risk ("6-Months to DORA" event, 28 June 2024)

Enter the EU's Digital Operational Resilience Act (DORA); DORA will provide the legislative bedrock for digitally resilient pan-European financial systems. DORA brings together existing provisions addressing digital operational risk in one single legislative act covering:

- Information and Communication Technology (ICT) risk management
- ICT-related incident management, classification and reporting
- Digital operational resilience testing
- Management of ICT third-party risk (including the introduction of an oversight framework for critical ICT third-party service providers)
- Information sharing arrangements.

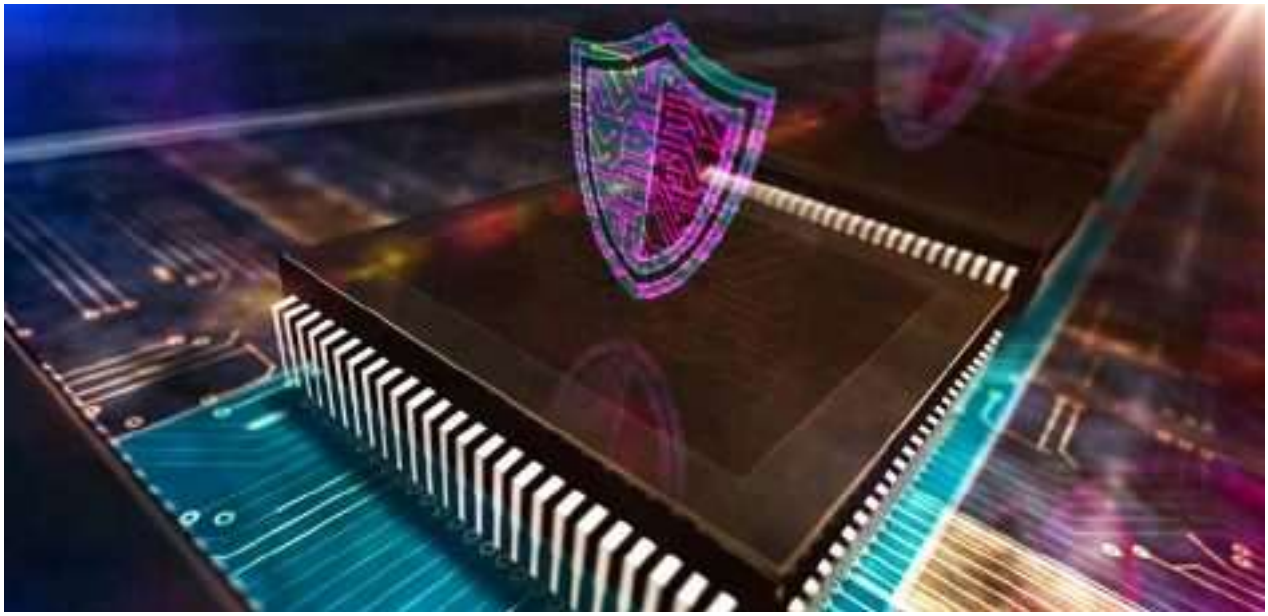
Who is in scope?

The following financial entity types authorised by the Central Bank of Ireland (CBI) are in scope of DORA:

- Crypto Asset Service Providers
- Electronic Money Institutions
- Crowdfunding Service Providers
- Account Information Service Providers;
- Payment Institutions;
- Credit Institutions;
- Insurance, Reinsurance, Ancillary Intermediaries;
- Trading Venues;
- Investment Firms;
- Insurance and Reinsurance Undertakings;
- Manager of Alternative Investment Finds; and
- Management Companies.

CBI Expectations

On 6 November 2024, the CBI held a DORA industry briefing event. The CBI shared its expectations regarding DORA implementation, points of emphasis included:



- That DORA will be legally binding from 17 January 2025 for all financial entities in scope.
- An acknowledgement that some elements of DORA guidance are still in progress and that specific requirements from the Technical Standards are only becoming clearer now.
- The CBI expects financial entities to have completed a comprehensive gap analysis, and to have remediation plans.
- The quality of the approach to DORA and the financial entity's approach to gap analysis, along with the timely closure of gaps will be the initial focus for the CBI.
- In relation to "Day 1 priorities" for financial entities, the CBI will expect that key elements of DORA, such as ICT-related incident identification and reporting are implemented ahead of 17 January 2025.

Ground-breaking Oversight Regime

An interesting aspect of DORA is the introduction of an oversight regime for critical ICT third-party service providers (CTPPs) including cloud service providers. Financial entities, receiving services from CTPPs, remain responsibility for the ICT outsourcing activities and ICT services received. While CTPPs firms are not regulated or supervised by the CBI, DORA provides regulators with a legislative mechanism to ensure oversight including the right of inspection. This is a new era for both regulators and third-party service providers.

Fintechs & Compliance

DORA catches a wide range of authorised firms within its net, however the required lift to achieve compliance is an uneven load across entity types. Larger, more complex regulated financial entities, such as banks, will recognise similarities between DORA requirements and existing Central Bank guidance in relation to outsourcing, operational resilience and IT & cybersecurity risks. For such entities, much of the DORA requirements have already been implemented over the past 5 years. For entities such as payment firms, electronic money institutions, and crypto asset service providers which may not have been subject to this guidance previously, the gaps to compliance are significant and daunting. For firms with smaller Compliance functions, the task of simply reading and assimilating the hundreds of pages of guidance published in 2024 alone is a heavy lift and that's before the challenge of educating stakeholders on DORA and driving compliance gap analyses and remediation plans.

Fintechs' infrastructure relies primarily on critical third-party vendors and technology service providers. A key component of DORA requires firms to build a sound framework to identify and assess their dependency on critical third-party vendors and service providers making DORA a substantial regulatory effort for Fintechs.

Focus Areas

With one month to go until DORA is legally binding, financial entities are busy implementing their DORA plans. With time running out, firms are focusing on:

- Ensuring that documentation such as the ICT Risk Management Framework, Digital Operational Resilience Strategy and the relevant policies are in place and approved by the Board ahead of January 2025.
- Ensuring that they have implemented and sufficiently populated the Register of Information and are in a position to share the register with the CBI by early April 2025.
- Implementing requirements in relation to ICT Incident Management and Reporting of major ICT-related incidents ahead of the deadline.