Preparing your organisation for the Digital Operational Resilience Act (DORA) deadline

Insights - 25/03/2024

The Digital Operational Resilience Act ("**DORA**") is a European Union ("**EU**") Regulation which entered into force on 16 January 2023 and is aimed at strengthening the operational resilience of the EU's financial services sector against information and communication technology ("**ICT**") cyber-attacks.

Organisations to which the provisions of DORA will be applicable have until 17 January 2025 – approximately 10 months from now - to implement measures to comply with the Regulation.

The purpose of DORA practically, is to ensure business continuity in circumstance of an unexpected disruption by, for example, system downtime as a result of malicious activities by unauthorised threat actors. The EU's objective in implementing DORA is to require in-scope firms to put in place measures to withstand, react to, and mitigate against cyber-related disruptions and risk.

What organisations will DORA apply to?

DORA will apply to an extensive range of financial entities based in EU member states, some examples of which are as follows:

- insurance and reinsurance undertakings
- insurance intermediaries
- crypto-asset service providers
- credit institutions
- banks
- payment institutions and electronic money institutions
- investment firms

- AIFMs and UCITS management companies and
- cloud computing platforms

It is estimated that approximately 22,000 financial entities or more [1] across the EU will fall within the scope of DORA.

Focus of DORA

The areas which DORA will focus on can be broadly summarised as follows:

- Reporting – reporting of significant ICT related incidents to competent authorities
- Oversight of critical third-party providers – the implementation of oversight framework for critical ICT third-party providers. The European Supervisory Authorities, will designate certain ICT service providers as "critical"
- Information Sharing – covering the sharing of information and intelligence in relation to cyber threats and vulnerabilities
- Resilience Testing – the implementation of basic and advanced ICT testing
- ICT risk management – the introduction of principles and requirements on ICT risk management; and
- ICT third-party risk management – the monitoring and management of ICT third-party risk.

Actions to be taken before January 2025

The specific regulatory technical standards and implementing technical standards of DORA will be finalised and published over the coming months. In-scope firms will need to immediately commence taking preparatory steps including the implementation of incident reporting; operational resilience testing, and intelligence gathering and sharing. Some of the steps in-scope organisations should consider taking are as follows:

- Initial Gap Assessment – review and identify gaps in ICT risk management frameworks, relevant existing ICT contracts, assessing potential gaps and planning the implementation of any changes required in advance of January 2025
- ICT risk management - conduct an asset review of critical business services, where they are hosted, what they host and what processes they support
- Testing – Article 26 of DORA provides for the implementation of advanced testing of ICT tools based on Threat-Led Penetration Testing ("TLPT"), a controlled attempt to compromise the cyber resilience of an entity. It is recommended that organisations take steps to understand

the skills required to run testing and conduct appropriate training

- Third Party Provider ("TPP") Management – map out current TPP contracts and review vulnerabilities to inform and improve risk containment strategy. The practical application of this will comprise of asking questions such as whether there are plans in place for mitigating the loss of critical vendors
- Monitoring National Competent Authorities ("NCA") Guidance – the Central Bank of Ireland is one of the many NCAs across Europe and will begin to undertake its oversight role under DORA in the coming months. Organisations should monitor the Central Bank's updates for guidance on conformity with DORA over the coming months.

Sanctions / Penalties

The penalties and remedial measures of DORA are contained in Article 50, which permits "competent authorities" within EU Member States to supervise, investigate and sanction to fulfil their duties. Competent authorities will have the power to access and take documentation, carry out on-site inspections, summon representatives of financial entities, interview persons and order corrective and remedial measure for breaches of DORA.

The potential penalties and measures available to be imposed by competent authorities on in-scope firms pursuant to DORA can be summarised as follows:

- an order requiring the cessation of conduct in breach of DORA and to desist from repetition of that conduct
- the temporary or permanent cessation of any practice or conduct contrary to the provisions of DORA
- the adoption of any type of measure, including pecuniary, to ensure continued compliance with legal requirements
- to access existing data traffic records held by telecommunication operators related to the investigation of breaches
- to issue public notices, including public statements, indicating the identity of the natural or legal person and the nature of the breach.

Conclusion

The potential penalties and concomitant reputational damage to organisations for failure to comply with DORA mean that in-scope organisations need to take immediate steps to prepare for the implementation of DORA prior to January 2025. Insurers, in particular, should consider the implications of DORA on coverage and policy wording, if they have not done so already.

For more information please feel free to contact a member of our Dispute Resolution team in Ireland via their contact details below.

[1] DORA and its impact on UK financial entities and ICT service providers - PwC UK

About Ogier

Ogier is a professional services firm with the knowledge and expertise to handle the most demanding and complex transactions and provide expert, efficient and cost-effective services to all our clients. We regularly win awards for the quality of our client service, our work and our people.

Disclaimer

This client briefing has been prepared for clients and professional associates of Ogier. The information and expressions of opinion which it contains are not intended to be a comprehensive study or to provide legal advice and should not be treated as a substitute for specific advice concerning individual situations.

Regulatory information can be found under Legal Notice

Meet the Author

Cian O'Gorman

Associate

Ireland

E: cian.o'gorman@ogier.com

T: +353 1 584 6766

Key Contacts

Stephen O'Connor

Partner

Ireland

E: stephen.oconnor@ogier.com

T: +353 1 232 1074

Related Services

Dispute Resolution

Crypto Disputes