The new EU Digital Operational Resilience Act (DORA)

17 April 2024

The question

What can financial services entities and ICT providers expect from DORA and what do they need to do prepare for it?

The key takeaway

The EU's Digital Operational Resilience Act (**DORA**) will require financial services entities and third party information, communication and technology (**ICT**) providers operating in the EU to comply with new technical requirements and standards to protect against digital threats by 16 January 2025.

The background

DORA came into force on 16 January 2023 and its provisions will be fully implemented by 17 January 2025.

DORA consolidates and improves existing legislation focused on ensuring that ICT security for financial services across the EU are resilient, particularly in response to cyber attacks. DORA will apply to 21 different types of entities including credit institutions, investment firms, insurance undertakings, crypto asset service providers, and critical ICT third party providers.

DORA identifies six areas for new uniform standards for regulating financial services' digital security. These include:

- principles and requirements for ICT risk management;
- digital operational resilience testing;
- reporting requirements for major operational and security related ICT incidents;
- voluntary notification of significant cyber threats to DORA's supervisory authorities;
- risk management requirements for third party ICT suppliers; and
- an oversight framework for critical third party ICT suppliers.

The above framework will be supervised by three European Supervisory Authorities (ESAs), namely the European Banking Authority, the European Insurance and Occupational Pensions Authority, and the European Securities and Markets Authority. The ESAs are also granted power to work with non-EU regulatory and supervisory authorities to manage international risks from third-party ICT providers.

The development

On 17 January 2024, the first batch of standards to implement DORA were delivered. These included: (i) Regulatory Technical Standards (**RTS**) on an ICT risk management framework; (ii) RTS on criteria for the classification of ICT-related incidents; (iii) RTS to specify the policy on ICT services supporting critical or

important functions provided by ICT third-party service providers; and (iv) Implementing Technical Standards to establish templates for a register of information.

This is the first of two batches of draft technical standards, with the second set due to arrive in June of this year. The second batch is expected to include proposed timelines and templates for technical incident reporting, guidelines on aggregating costs and losses caused by cyber attacks, and technical standards for threat-led penetration testing.

These technical standards (which still need approval from the European Commission) specify the detailed requirements that must be met by the financial services entities to which DORA applies, and are to be read in tandem with DORA itself (which imposes other requirements). The standards will then be implemented throughout 2024 and oversight will begin after 16 January 2025.

Why is this important?

DORA is expected to provide clarity on the ICT risk management framework across the EU financial services sector. Financial services entities and third party ICT providers in scope will need to ensure they are prepared and able to comply with DORA's comprehensive and technical requirements. In addition to technical updates, businesses will need to ensure their internal governance frameworks and policies (including training programmes) meet requirements under DORA. Non-compliant businesses may be fined 1% of their average daily worldwide turnover for each day of non-compliance.

The new standards and requirements also mark some divergence from those applicable to UK financial services entities. Businesses that operate in both the UK and EU must therefore assess compliance with each regime.

Any practical tips?

It has been more than a year since DORA came into force, so most businesses in scope will have already begun their compliance exercise. Many will already have in place systems and processes that meet the requirements under DORA, as they would have had to comply with the previous ICT regulatory framework. However, the new standards that have been published (and more that will come) will be helpful to provide clear guidance on regulators' expectations. Businesses should therefore ensure that their systems and processes clearly meet these standards.

Spring 2024