

ESA updates on DORA

The European Supervisory Authorities (“ESAs”), which include the European Securities and Markets Authority (“ESMA”), the lead European financial services regulator, have recently issued updated documentation in relation to the Digital Operational Resilience Act (“DORA”) including guidelines, Regulatory Technical Specifications (“RTS”) and Implementing Technical Standards (“ITS”). The implementation date of DORA is 17th January 2025 so the added details and insights of regulatory expectations in these documents are highly valuable in preparing for regulatory compliance.

Background

DORA was passed in January 2023 and once effective will essentially require European financial services providers to put in place specific measures to support their digital operations with a view to ensuring that they have the necessary resilience, including to safeguard against cyber-attack etc. The primary legislation is underpinned by more detail through the RTS and ITS, with additional detail on regulatory expectations set out in guidelines.

Latest updates

On 26th July 2024, the ESAs published their joint Final report on the draft RTS on subcontracting under DORA. These specify the applicable conditions for subcontracting information and communication technology (“ICT”) services that support critical or important functions under DORA. They also set out requirements for the implementation and management of such sub-contractual arrangements and the applicable requirements throughout the lifecycle of contractual arrangements between financial entities and ICT third-party service providers, including regarding ongoing risk assessment.

Other Measures

On 17th July 2024, the ESAs published four final draft RTS, one set of ITS and 2 guidelines.

These consisted of:

- RTS and ITS on the content, format, templates and timelines for reporting major ICT-related incidents and significant cyber threats;
- RTS on the harmonisation of conditions enabling the conduct of the oversight activities;
- RTS specifying the criteria for determining the composition of the joint examination team (JET); and
- RTS on threat-led penetration testing (TLPT).

The guidelines published were:

- Guidelines on the estimation of aggregated costs/losses caused by major ICT-related incidents; and
- Guidelines on oversight cooperation.

This was the second batch of policy documents under DORA with three RTS and an ITS from the first phase being adopted earlier this year.

How Clerkin Lynch Can Help

Clerkin Lynch’s financial services team can assist with preparation for compliance with DORA as well as related preparatory work. Reach out to the contact details below for more information.



Mark Browne
Partner
email:
markbrowne@clerkinlynch.com
Phone: 01 611 4400

