Browne Jacobson

EU Digital Operational Resilience Act: Countdown to comply with the January 2025 deadline

02 July 2024

DORA explained: The new EU standard for financial services' digital resilience

The financial sector has, in recent years, become increasingly reliant on information and communications technology ('ICT') systems and on information in digital form to deliver financial services, such that it is now of critical importance to the operation of daily functions. The digitisation and reliance on ICT by financial entities will only continue to accelerate as they seek to harness data and capitalise on the benefits that new technologies, such as generative AI, offer.

As the sector's dependency on ICT has increased, so too has its vulnerability to cyber risk – which can not only impact the financial entity in question but also, due to the interconnectedness of the industry, impact other financial entities, sectors and even the wider economy.

In response, after a long period of consultation, on 16 January 2023 the European Union's Digital Operational Resilience Act ('DORA') entered into force. DORA applies across the EU on a uniform basis and has the primary objective of providing a comprehensive and unified framework to enhance the digital operational resilience of the EU financial sector and to minimise disruption to financial entities in the EU.

Scope

The scope of financial entities captured by DORA extends well beyond EU banks, insurers and payment and electronic money institutions to capture many other types of financial entities operating in the EU, including crypto- asset service providers and crowdfunding service providers (together 'financial entities').

Whilst DORA will not apply directly to financial services firms in the UK, multi-national/UK financial services groups with EU operations will need to ensure that those financial entities are DORA compliant.

DORA also directly applies to certain ICT third party service providers which are designated as "critical" by European Supervisory Authorities ('ESAs'), including those that are based outside of the EU providing services to financial entities.

January 2025 deadline

Financial entities operating in the EU are required to fully comply with the extensive conditions required of them under DORA by 17 January 2025. Despite the significant challenge financial entities, as well as ICT third party service providers to those financial entities ('ICT TPPs'), are facing to achieve compliance by this date, the ESAs have confirmed that this deadline will not move and that no additional "transitional period" will apply beyond this date.

On this basis, financial entities will need to expediate efforts this year to fully understand and implement DORA's requirements, some of which – secondary legislation in the form of certain 'Regulatory Technical Standards' which set out the technical detail and methodology to meet the level 1 DORA general principles and requirements – will only be finalised in mid July 2024.

In this article, we summarise what DORA means for financial entities and ICT TPPs and what they should do now to meet the looming deadline.

Financial entities: Key requirements

Financial entities are required to comply with prescriptive DORA requirements in relation to ICT risk and resilience albeit, for some of those requirements, on a proportionate basis considering the size, nature and risk profile of the financial entity and its activities.

DORA's requirements are comprehensive and fall into five key pillars:

- ICT risk management.
- Incident management, classification and reporting.
- Digital operational resilience testing.
- Third-party risk management.
- Information sharing.

Each pillar has extensive requirements to be implemented by 17 January 2025.

We have focused below on one requirement – directly relevant to the legal function – the ICT contract requirements, which fall in the third-party risk management pillar.

ICT contract remediation

A key aspect of the third-party risk management pillar is the requirement for financial entities to address the risks arising from contractual arrangements on the use of "ICT services" concluded with ICT TPPs. This requirement, in particular, will be time consuming for financial entities due to the dependency on ICT TPPs to agree terms, who themselves are likely to be inundated with requests from financial services clients to amend existing contracts.

DORA prescribes "two tiers" of contractual provisions to be included in a financial entity's contracts with ICT TPPs for the provision of "ICT services" – with more extensive contractual provisions for contracts supporting a financial entity's critical or important functions (or 'CIFs').

Although many of DORA's contractual requirements should already be contained in a comprehensive ICT contract and are broadly in line with existing financial services regulations – such as the EBA guidelines on outsourcing and the ESMA guidelines on outsourcing to cloud service providers – DORA does contain "new" requirements to be included in ICT contracts. For example, an ICT TPP is required to provide assistance at no additional cost or at a cost determined ex-ante where an ICT incident related to the ICT service occurs. The scope of contracts captured by DORA to be remediated by 17 January 2025 is also far broader (e.g., by not being limited to "outsourcing" arrangements).

On this basis, financial entities which have already remediated contracts to comply with other regulations will still need to reassess their contractual arrangements in accordance with DORA.

DORA is also clear that intra-group arrangements (e.g., between a financial entity in the EU and a group services company in the UK) are to be treated the same for the purpose of contractual remediation as a contract a financial entity may have directly with an ICT TPP outside of the financial entity's group.

Critical ICT TPPs: Key requirements

DORA applies to an ICT TPP directly where an ICT TPP is designated by the ESAs as critical to financial entities in the EU ('CTPP').

The basis upon which ESAs will designate an ICT TPP as a CTPP has been finalised (in a delegated regulation dated 22 February 2024) but as yet, no CTPPs have been designated.

Under the oversight framework appliable to CTPPs, CTPPs will have requirements directly placed on them as well as being required to pay oversight fees (also prescribed in a delegated regulation dated 22 February 2024).

One such requirement on CTPPs, is to establish a subsidiary in the EU within 12 months following its designation (if this is not currently the case), otherwise financial entities will not be able to continue to make use of that CTPP's ICT services.

CTPPs may be subject to investigations and inspections by ESAs, with non- compliance with DORA exposing CTPPs to substantial financial penalties (up to 1% of the average daily worldwide turnover in the preceding business year until compliance is achieved within certain limits) as well as public notices.

What should financial entities and ICT TPPs be doing now?

Financial entities:

- Understand the extent to which the financial entity falls within scope of DORA and ensure DORA's requirements, as set out in the level 1 text and delegated legislation, are understood.
- Establish and/or amend all policies, processes, procedures and frameworks to meet DORA's requirements by 17 January 2025.
- From a contractual remediation perspective: identify and map ICT TPPs and contractual arrangements (including intra-group) to each financial entity (categorising those which support CIFs), collate existing contracts with ICT TPPs, engage with ICT TPPs and amend ICT TPP contracts in line with DORA requirements by 17 January 2025.

ICT TPPs:

- Pro-actively prepare for financial entities amending existing contractual terms, which may include ICT TPPs issuing their own standard amendment documentation to financial entities.
- Consider whether CTPP designation is likely, and if so, understand the actions needed to be taken to comply with DORA.

Key contact

Rowan Armstrong

Partner

rowan.armstrong@brownejacobson.com

+44 (0)330 045 2737

Related expertise

Services

Cyber liability and data security insurance

Data protection and privacy

Digital and sourcing

Financial institutions

Financial services and insurance advisory

Financial services regulation