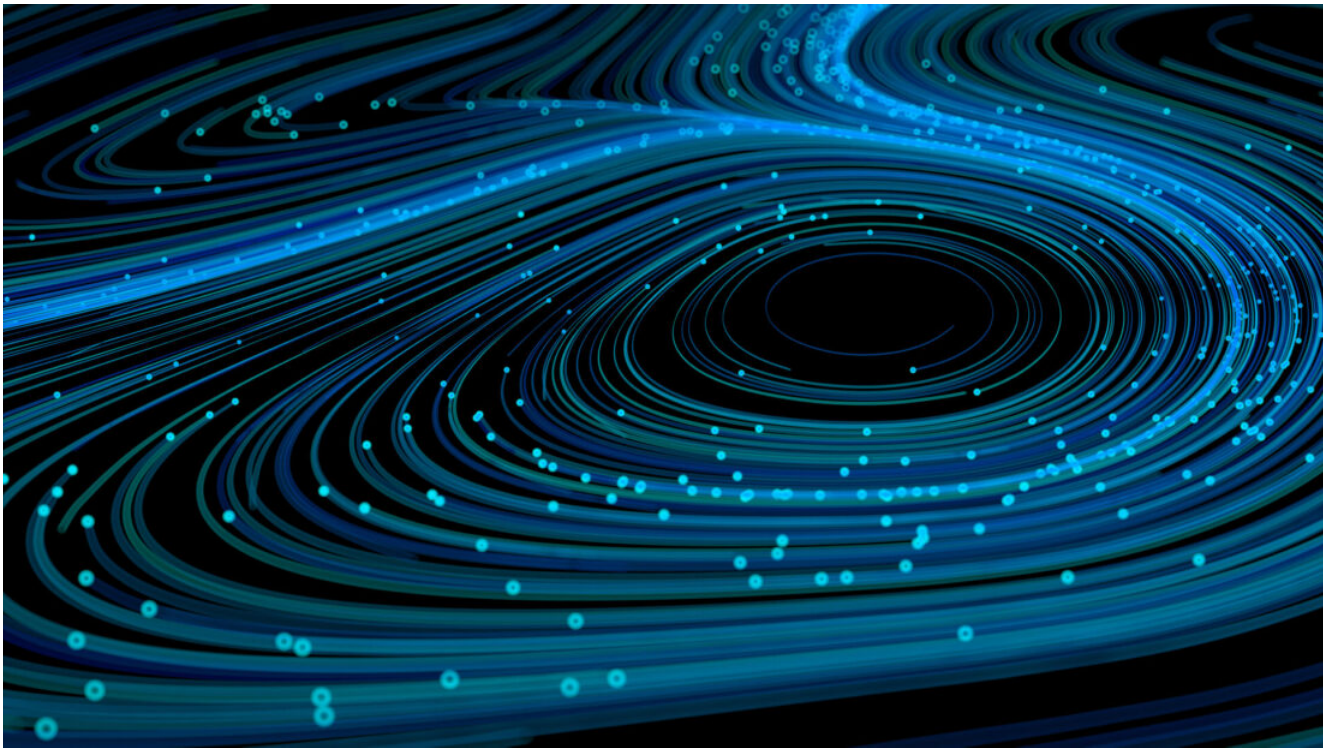
LATHAM & WATKINS LLP
Global Fintech & Digital Assets Blog
Exploring innovative financial services: tech, regulations, and market trends

DORA: Just Over Three Months Until Take Off

Posted on September 27, 2024



The deadline is fast approaching for in-scope financial entities and their ICT service providers to conform to the EU's new digital operational resilience regulation.

By **Christian F. McDermott** and **Alain Traill**

With effect from 17 January 2025, a broad range of EU financial entities will be subject to the new EU regulation on digital operational resilience for the financial sector (DORA), with significant impact for firms and their third-party ICT service providers. As the new landscape takes shape, below is an overview of some of the key changes and steps that impacted financial entities and providers should be

taking ahead of the deadline.

Reminder: What Is DORA and Who Does It Apply to?

DORA entered into force on 16 January 2023, and takes effect from 17 January 2025. It represents the EU's attempt to mitigate the digital operational resiliency risks (for example, the impact of cyberattacks and software malfunctions) arising from the increasing reliance of the financial services sector on technology and in particular, a small number of core ICT providers.

DORA directly applies to most financial entities operating in the EU market, including banks, insurers, payments providers, and alternative investment fund managers, among others. It also indirectly impacts a broad range of third-party providers of technology-related services — from software to technology infrastructure — which will be required to take steps to facilitate compliance by financial entity customers that are subject to DORA. Finally, a small group of third-party ICT service providers designated as "critical" will be directly subject to a dedicated regulatory regime under DORA.

The territorial scope of DORA is broad and extends to organisations based outside the EU, where, for example, they (in the case of financial entities) offer certain financial services in the EU market or (in the case of ICT providers) contract with financial entities that are in-scope of DORA.

New Obligations on Financial Entities

The requirements for financial entities are broken down into five pillars, and should be applied proportionally taking into account the financial entity's overall risk profile and the nature, scale, and complexity of its services.

1. **ICT risk management**, involving operational and procedural controls such as governance frameworks and internal policies
2. **ICT incident management, classification, and reporting**, including requirements to notify of certain ICT-related incidents within set timescales
3. **Resilience testing**, i.e., requirements to carry out regular operational

resilience tests including in some cases, threat-led penetration testing

4. **ICT third-party risk management**, including diligencing and managing ICT providers and flowing down certain contractual requirements
5. **Information sharing**, whereby in-scope financial entities are encouraged to share information on cyber threats and intelligence

As part of the fourth pillar, all contracts between financial entities and ICT providers must contain certain provisions. This will involve updating existing contracts and entering into new contracts. While some of these elements will be familiar to organisations from the EBA's Guidelines on outsourcing arrangements (EBAG), others are new or will require a compliance uplift. Examples of the latter include the requirement for the full contract to be set out in one, written document, available on paper or in a document with another downloadable, durable, and accessible format, and for the ICT provider to assist the financial entity in the event of ICT-related incidents either at no additional cost, or based on forecasted/*ex-ante* costs. Additionally and depending on the particular arrangement, financial entities may need to flow further obligations down to ICT providers in order to meet their own compliance responsibilities, including the ongoing provision of information (to enable financial entities to maintain required registers) as well as support and/or participation in business continuity plan testing.

In a split that will again be familiar to those accustomed to EBAG, DORA distinguishes between two categories of arrangements with ICT providers, by adopting the concept of "critical or important functions". These are functions that, if disrupted, would materially impair the financial institution's (i) financial performance; (ii) soundness or continuity of services and activities; or (iii) ability to comply with its conditions or obligations of authorisation or regulatory obligations. Contracts for services that support such functions are subject to more stringent requirements, such as the inclusion of specific audit and exit assistance related provisions.

Direct Regulation of "Critical" ICT Providers

In a marked change from pre-existing regulation in this field, DORA establishes a

direct oversight regime by the European Supervisory Authorities (ESAs) for “critical” ICT providers. These providers will be provisionally designated by the ESAs and will then have just six weeks from the date of notification to challenge their designation. Once designation is confirmed, a “Lead Overseer” (the EBA, ESMA, or EIOPA) will be appointed for each critical ICT provider and granted a range of supervisory, investigatory, and sanctioning powers, including the power to access documents, conduct on-site inspections, and implement remedial measures for breaches. Lead Overseers will adopt an oversight plan tailored to each critical ICT provider and an oversight fee will be payable. Critical ICT providers must also maintain an adequate business presence in the EU, meaning that those not already located within the EU must effectively incorporate an EU subsidiary within 12 months of their designation.

Impacts on Other ICT Providers

For ICT providers not designated as “critical”, the key impact of DORA will be a flow-down of various contractual provisions and other requirements from customers that are in-scope financial entities. A key change to existing regulation is that arrangements between these ICT providers and in-scope financial entities will be impacted by DORA regardless of whether or not the services constitute an *outsourcing* for the purposes of pre-existing financial services outsourcing regulation (e.g., EBAG). This means that a far broader range of service providers will be impacted by DORA than existing regulation such as EBAG. It also increases the scope of the compliance exercise for in-scope financial entities, as they will need to consider and potentially remediate a greater number of third-party relationships than under existing requirements.

Consequences of Non-Compliance

There are significant financial and other consequences for non-compliance with DORA. Specific monetary penalties for non-compliance by financial entities are not set out in DORA, rather EU Member States have the freedom to introduce appropriate penalties and criminal sanctions. However, these are expected to be substantial. Critical ICT providers may be fined for non-compliance by way of a

daily penalty, applied for up to six months and calculated as 1% of their average daily worldwide turnover. Competent authorities may also temporarily suspend the use of services provided by a critical ICT provider.

Next Steps

With just over three months remaining before DORA takes effect, both financial entities and ICT providers — particularly those anticipating designation as a critical provider — should by now have developed and be implementing compliance programmes. For financial entities, this will include a gap analysis of existing operational resilience measures against the requirements in the Regulation (including based on the technical standards published under DORA such as those regarding the **classification of ICT incidents and cyber threats**), the updating of policies, processes, and procedures, and completion of a contract inventory and remediation exercise (likely prioritising arrangements that support critical or important functions).

ICT providers anticipating "critical" designation also face a potentially large-scale compliance exercise, including a gap analysis against the new requirements, preparation for engagement with the Lead Overseer, updates to contract terms, and potentially the establishment of an EU entity. Meanwhile, ICT providers that will not be designated as "critical" but that count EU financial entities as customers should by now be implementing the approach they will take to the flow-down of DORA requirements from customers, including by communicating the compliance activities they will take or support, implementing contractual updates, and providing further information to customers to justify their approach.

This post was prepared with the assistance of Sidney Chin in the London office of Latham & Watkins.