BCLP. Client Intelligent

Insights

THE EU'S DIGITAL OPERATIONAL RESILIENCE ACT 2022/2554 (DORA)

DIGITAL SPEAKS SERIES

Sep 20, 2024

Financial services regulators have long grappled with the complexity of regulating to maintain stability in financial markets, given:

- the dependence of modern financial systems on third party systems, technology and platforms, which has only intensified with the adoption of cloud solutions; and
- the systemic risk posed to the smooth functioning of financial markets if a technology provider suffers a cyber incident.

Long IT sub-contracting chains can make it hard for financial institutions to understand the vulnerabilities in their IT estate and the location of key functions (where these may be located in entities who do not have a direct contractual relationship with the financial institution).

The EU's Digital Operational Resilience Act 2022/2554 (**DORA**) was crafted with this in mind – to require financial institutions to identify those ICT services which support critical or important functions and to ensure the contractual arrangements with the providers of those functions are bolstered to include certain core protections.

DORA came into force in January 2023, and EU financial institutions and IT suppliers providing critical services to financial institutions operating in the EU now have until **January 2025** to comply with its requirements (following which, EU regulators will be empowered to request that financial institutions take steps to remedy security vulnerabilities and can impose fines). It also potentially affects non-EU based companies, to the extent that these companies have functions delegated to them by EU financial institutions, and these functions fall within the concept of 'ICT services'.

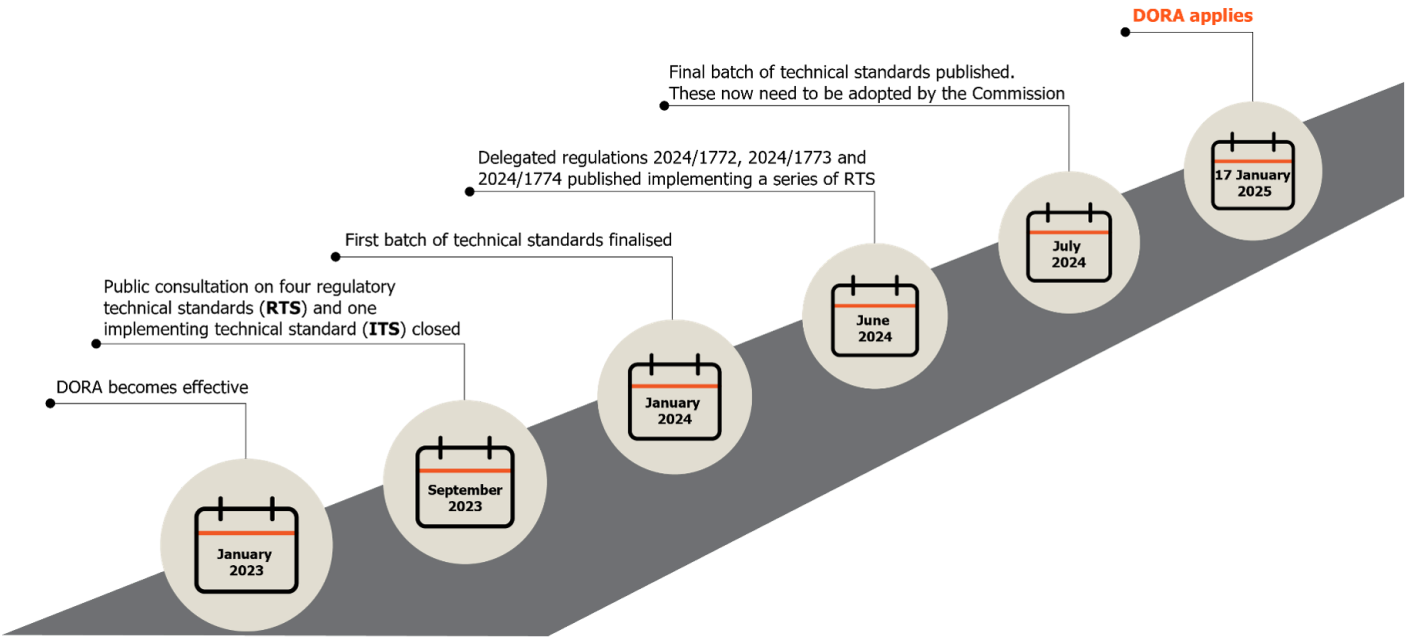
We are working closely with our financial services clients to ensure their readiness for DORA compliance and to ensure their contracts appropriately address the new DORA requirements as failure to comply with the DORA requirements can have serious consequences, including:

- fines;

- sanctions for board members; and
- reputational damage and potentially criminal penalties for non-compliance.

KEY DATES

- January 2023 - DORA becomes effective.
- September 2023 - Public consultation on four regulatory technical standards (**RTS)** and one implementing technical standard (**ITS**) closed.
- January 2024 - First bath of technical standards finalised.
- June 2024 - Delegated regulations 2024/1772, 2024/1773 and 2024/1774 published implementing a series of RTS.
- July 2024 - Final bath of technical standards published. These now need to be adopted by the Commission.
- **17 January 2025 - DORA applies**



WHO WILL BE IMPACTED?

DORA imposes obligations upon:

- a wide range of 'financial entities': including banks, investment firms, pensions companies and asset managers, electronic money institutions, insurance companies and crypto asset firms, amongst others; and

- certain ICT third party service providers: being organisations that provide services to the financial entities that meet certain benchmarking criteria set out in DORA.

Some in-scope ICT providers will be designated critical, and then will be subject to supervision by the European Securities and Markets Authority, the European Insurance and Occupational Pensions Authority or the European Banking Authority (which has the role of lead overseer). As yet, no service providers have been so designated, as this requires a two-step assessment to be conducted. However, recent commentary from the European Banking Authority suggests that providers of network infrastructure services and data centre services are very likely to meet the criticality threshold.

Although DORA is an EU regulation, it can also apply to non-EU third party service providers that provide services to financial entities that are within the EU.

WHAT ARE ICT SERVICES?

ICT services are defined to include 'digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services.'

Criticality for an ICT service provider will be determined by:

- the systemic impact on the stability, continuity or quality of the provision of financial services if the provider suffered a large scale operational failure (based on the number of financial entities and the total value of assets of financial entities to which the relevant ICT third party service provider provides services);
- the systemic character or importance of its financial services customers (taking into account the number of global systemically important institutions or other systemically important institutions that rely on the provider and the interdependence between the institutions which rely on the provider);
- the nature of the financial entities' services which rely on the provider and whether these are critical or important functions; and
- how easy it would be to substitute the services of the provider for a third party (i.e. whether there are any real alternatives in a specific market, the market share of the service provider, the technical complexity or sophistication involved and any likely difficulties which would be encountered partially or fully migrating the relevant data and workloads to another provider, including financial costs/time of migration or increased ICT risk or other operational risks of a migration).

STRUCTURE

DORA is underpinned by a series of regulatory technical standards and implementing technical standards. Of those standards now in final form, the standards in the Delegated Regulations 2024/1773 are important for setting the key obligations on financial entities to observe from an internal standpoint and embed in contractual requirements, requiring each in-scope entity to:

- have a policy in place to assess exposure to third party IT supplier risk including tools in that policy for assessing risks associated with providers who support a 'critical or important' function;
- set standards for pre-contractual due diligence;
- ensure the relevant components from Article 30 of DORA are included in all contracts with third party ICT providers (to the extent it is possible to obtain audit rights over third party providers for example);
- set up a monitoring function to oversee contractual arrangements and performance of the service provider (including ensuring compliance with confidentiality, availability, integrity and authenticity of data requirements and compliance with the entity's own policies and procedures) and steps to be taken if a provider is not meeting relevant service levels; and
- plan for exit / termination (and ensure exit plans are devised, accepted and tested over the life of the contract).

IMPACT

Key deliverables that financial entities need to have in place, internally from a compliance perspective and documented in contractual arrangements include:

ICT RISK MANAGEMENT

This includes:

- having an internal governance and control framework, ensuring effective and up-to-date management of ICT risk;
- having a separate ICT risk management framework that is reviewed, as a minimum, on a yearly basis;
- appropriate ICT systems, protocols and tools in relation to the operations an organisation is carrying out;

- identification and mapping of critical ICT assets, including any processes that depend on ICT third party services providers;
- ongoing monitoring of ICT systems, ensuring continuous protection of ICT systems and therefore also prevention of any threats to security;
- mechanisms to detect any irregular activities and points of failure;
- an ICT business continuity policy, ICT response and recovery plans and ICT business continuity plans that must be tested, at a minimum, on an annual basis;
- the development of backup policies and procedures and the maintenance of adequate recovery restoration and recovery procedures and methods;
- learning by collating information on security threats and determining the points of failure after ICT-related incidents, and then using this learning to develop security awareness programmes and training for staff.

ICT-RELATED INCIDENT MANAGEMENT AND REPORTING

Including maintaining an incident classification and reporting framework, ensuring authorities are reported to accurately and quickly.

ADVANCED DIGITAL OPERATIONAL RESILIENCE TESTING

Including the need to develop a specific, threat-led testing approach.

A THIRD PARTY RISK MANAGEMENT FUNCTION

Which will ensure:

- contracts with third party ICT service providers comply with DORA obligations;
- a register of information relating to the third party ICT service providers is maintained;
- a process for risk concentration management is implemented;
- exit strategies for third party ICT service providers that support critical functions are put in place.

It is not a requirement for financial entities to share information regarding security threats, but DORA encourages them to do so in order to utilise collective knowledge and thereby enhance

capabilities.

THE UK CRITICAL THIRD PARTY (CTP) REGIME

The UK's new regulatory regime will allow the regulators to designate certain third party service providers as 'critical' and bring them directly into the ambit of the financial services regulatory regime. The regime is similar to DORA, but implementation dates are dependent on the outcome of the consultation about designation criteria. This consultation closed in March 2024, so we anticipate we may start to see designations being made by the end of 2024. Available analysis suggests the likely number of CTPs within the remit of the regime will be 20 or less, with expected focus to be on large cloud service providers and SaaS vendors. CTPs will have to meet requirements set out in the Bank of England Rulebook, the PRA Rulebook and the FCA Handbook. The framework will consist of CTP Fundamental Rules (akin to principles – requiring business to be conducted with integrity, requirement to use due care and skill etc), to apply to all CTPs, accompanied by a more granular set of requirements which will apply only to a CTP's **material** services. These cover 8 areas of operational risk and resilience requirements, and include minimum resilience standards, dependency and supply chain risk management, scenario testing requirements and incident notification requirements. These were inspired by and adapted from existing global standards on operational resilience for firms, such as the Basel Committee on Banking Supervision's 'Principles for Operational Resilience'.

The UK's requirements are designed to be interoperable with DORA and the US Bank Service Company Act – and anticipates that UK regulators can ask CTPs for info they have provided to other regulators (or incident notifications given to firms / other regulators). The key thing to note is that the CTP regime **does not** replace the compliance steps expected of regulated firms, with the new rules to '*complement but not blur, eliminate or reduce the accountability and responsibility of firms*'. This regime does not therefore absolve a firm of responsibility for its selection, monitoring and management of its portfolio of third party service providers. The providers themselves (once designated) will be subject to additional requirements, such as the requirement to maintain financial sector incident management playbooks – where the CTP plans, documents, tests and reviews how it manages an incident affecting its material services (and tests this annually).

Separately, firms themselves need to ensure they have identified and met their impact tolerances for their important business services by 31 March 2025 (and ensure there is a process in place to review this continuously, as the risk/threats landscape evolves).

NEXT STEPS

With **less than 6 months** to go before in-scope organisations are required to be compliant, DORA is a pressing issue that should be at the forefront of your compliance plans.

In order to implement all of the DORA-mandated deliverables detailed above, we recommend that affected organisations:

- identify any key stakeholders and consider which business functions are affected by the rules (and ensure all mapping of key contracts relating to critical or important functions is complete as soon as possible);
- review current policies and processes already in place and how these need to be adapted to match the obligations imposed by DORA;
- find any gaps in your current processes and determine how these can be tackled (e.g. to revise resilience testing plan); and
- devise playbooks for negotiations with third party vendors to reflect how the contractual requirements mandated by DORA are to be implemented (particularly to ensure a firm can monitor performance, audit service provision and exit an arrangement as seamlessly as possible).

HOW CAN BCLP HELP?

We have a highly regarded, multi-disciplinary team of lawyers across various jurisdictions who provide advice on complying with DORA and the CTP Regime. If you think your organisation may be affected by either DORA or the CTP Regime, please reach out to Marcus Pearl, Matthew Baker, Geraldine Scali, Benjamin Wheeler or Amelda Henning.

RELATED PRACTICE AREAS

- Data Privacy & Security
- Technology Transactions

MEET THE TEAM

Marcus Pearl

London

marcus.pearl@bclplaw.com
+44 (0) 20 3400 4757

Matthew Baker

London

matthew.baker@bclplaw.com
+44 (0) 20 3400 4902

Geraldine Scali

London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483

Benjamin Wheeler

London

benjamin.wheeler@bclplaw.com
+44 (0) 20 3400 3407
