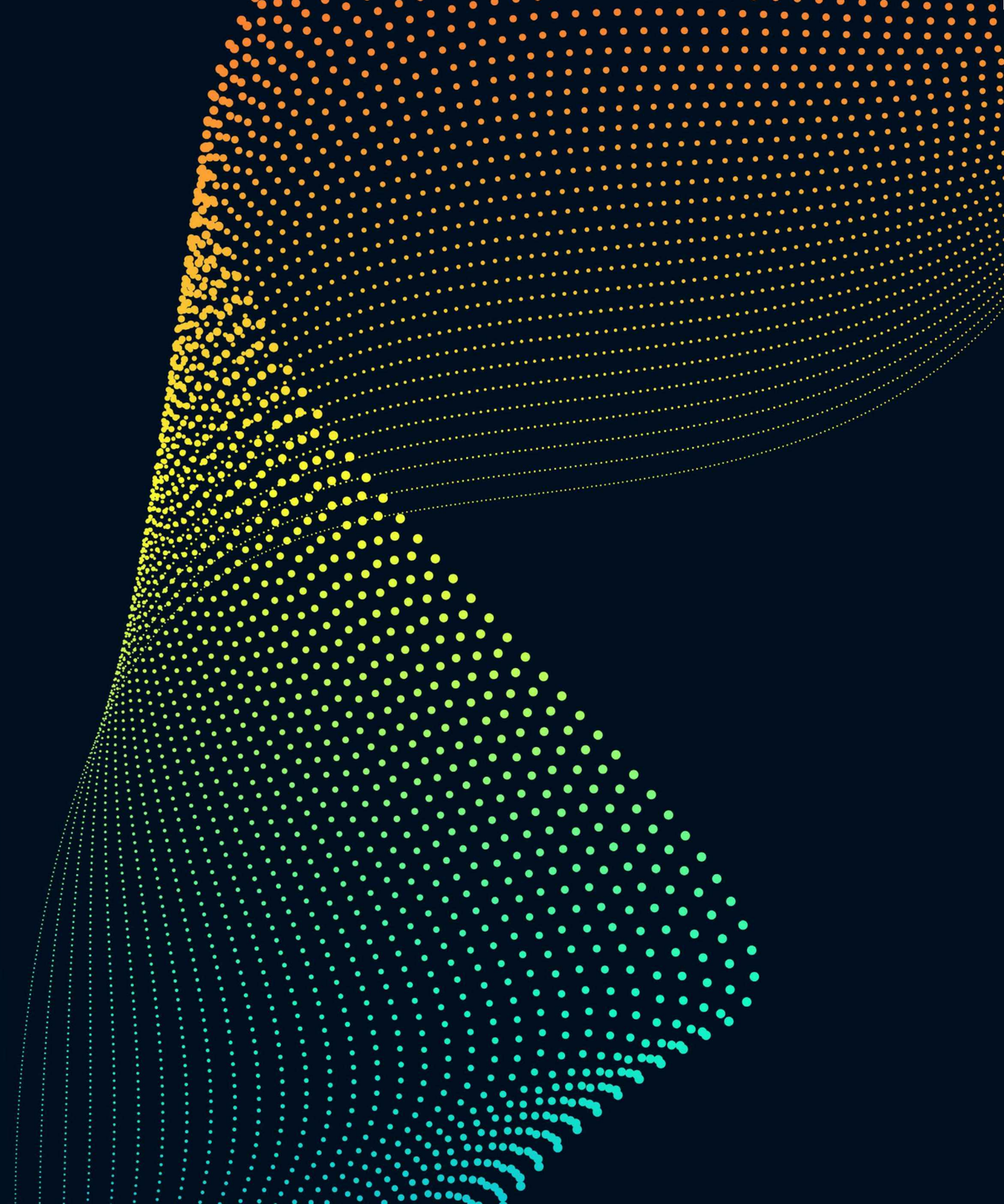
Baker McKenzie.

How will DORA impact financial institutions?

Helping clients navigate and comply with this significant new financial services regulation

March 2023



> “Their ability to handle complex matters and give plain and straightforward advice is invaluable.
>
> “What I rate is the degree of legal technical expertise, commercial approach and behavioural attitude.
>
> **Chambers FinTech Legal – London 2023**

> “Baker McKenzie is a highly regarded global firm with almost unmatched international coverage through its impressive network of offices.
>
> **Chambers FinTech Legal – London 2022**

The financial services sector has experienced significant digital transformation in recent years, accelerated as a result of the pandemic, with more and more institutions outsourcing technology services and moving systems to the cloud. This has resulted in the financial sector becoming increasingly dependent on third party technology providers and this dependency has raised new operational, technological and cyber security risks.

To mitigate these risks, the EU has introduced a new regulatory framework which imposes additional requirements for financial institutions using third party technology providers, along with establishing direct regulatory oversight over critical third parties providing services to financial institutions for the first time.

The UK has announced its own new regulatory framework for ICT providers to the financial services sector.

What is the EU Digital Operational Resilience Act (DORA)?

- DORA establishes a new supervisory framework that will implement a harmonised digital operational resilience regime for a broad range of financial institutions. This includes banks, asset managers, payment institutions, credit rating agencies and a range of other entities.
- DORA will apply to institutions headquartered in the EEA. It will also apply to institutions that have EEA entities within their group. It could also indirectly impact operations outside the may indirectly affect its non-EEA operations.
- DORA introduces new operational resilience requirements on financial institutions. The sector is already subject to operational resilience standards, but DORA marks a step-up with multiple new, granular requirements in what is a more prescriptive regime. Financial institutions will be required to develop a fully comprehensive risk management framework which addresses and mitigates any and all ICT-related risks that the firm has. This will require the firm to revisit and, potentially, revamp existing policies and procedures (or introduce new ones) including, among others, cybersecurity policies, policies to determine whether ICT resources are appropriate to the business, business continuity policies, disaster recovery strategies.
- Overall responsibility with this risk management framework will rest with the financial institution’s management body. This will require the management body to fully understand the ICT services used by the institution, the risks posed by such services and to ensure that the risk profile is continually updated. Regulators will expect to see management fully engaged with the firm’s use of ICT services, receiving appropriate management information, and exercising oversight, scrutiny, challenge and intervention where necessary.
- Additionally, DORA will require financial institutions to carry out certain operational resilience tests, to mitigate service outages and downtimes.
- DORA will also introduce obligations for financial institutions to report ICT related incidents to their local competent regulator. This is very similar to the existing requirements under the GDPR (and the Data Protection 2018 in the UK) to report data breaches to the relevant data protection authority, and also builds on (and ultimately will replace) existing sector-specific standards in the financial services space, notably the payment services incident reporting regime. The extent of these reporting obligations will be further detailed in upcoming regulatory technical standards.
- DORA also introduces and/or codifies a number of contractual requirements for institutions to include in contracts with ICT providers. Financial institutions are already required to include certain provisions in their agreements with third party providers where the relevant arrangement amounts to an “outsourcing”. DORA introduces similar contract requirements for ongoing digital services and data services provided by third party vendors including cloud computing services, as well as certain hardware-related services. For DORA, the ICT arrangement does not need to amount to an outsourcing as such and so DORA covers a broader range of ICT services.
- Firms have a little under two years to get ready for DORA as DORA will apply from 17 January 2025. During the implementation period, the ESAs will develop a very specific set of criteria, templates and instructions.

What is the UK CTP framework?

- The UK CTP framework will enable the UK Treasury, along with the Bank of England, FCA and PRA (the financial regulators), to directly oversee third-party service providers. Under the regime, HM Treasury will consult with the financial regulators before designating certain third parties that provide services to firms as critical (CTPs). It will also be possible for the financial regulators to proactively recommend CTP designation. The regime is expected to take effect later in 2023, once the relevant legislation is finalised and the financial regulators issue their rules and guidance. This marks an expansion from the current designation regime, which currently provides for designation only in respect of service providers to financial market infrastructures. The new UK CTP framework will extend this to capture services provided to a wider range of financial institutions.
- The new UK CTP regime is currently not expected to introduce any significant obligations on financial institutions. However, it may be that some indirect obligations apply to the financial institution as a result of the contract between the firm and the CTP. The CTP may include certain provisions within the agreement to enable it to comply with the UK CTP regime.

What will this mean for financial institutions?

DORA will have a significant impact on financial institutions

DORA: Risk Management Framework

- Financial institutions will need to create a broad risk management framework. The purpose of this framework is to enable firms to address ICT risks quickly, comprehensively and efficiently. The framework will involve a significant number of policies and procedures all of which are designed to ensure that the ICT services a firm uses are appropriate, and to help maintain operational resilience. At a broad level, these include policies for:
  - ensuring that ICT services are appropriate and reliable; carrying out appropriate due diligence and risk management assessments before entering into new contracts with ICT vendors
  - identifying and classifying third party ICT services;
  - reporting ICT services to the competent authority;
  - ensuring that appropriate cyber security tools and other protection methodologies are in place;
  - ensuring the resilience, continuity and availability of ICT systems;
  - detecting anomalous activities;
  - responding to and recovering from ICT-incidents; and
  - back-up and disaster recovery.
- Whilst a number of the above components reflect existing regulatory expectations, DORA is more prescriptive than the current regime in laying down the specific elements that are required in a risk management framework. Regulators will want to see that firms have analysed their existing frameworks against the DORA requirements, and can demonstrate that they meet all of the various elements.
- Overall responsibility for the risk management framework will rest with the firm's management body. The management body is responsible for approving, overseeing and implementing the risk management framework. As such, it bears ultimate responsibility for the framework. The effect of this is that the firm's management will need to have a sufficiently developed understanding of the firm's IT systems, the risks faced by those systems and the tools in place to detect and mitigate risks. Senior management may need to obtain additional subject matter expertise to support its role.

DORA: Operational Resilience Testing

- DORA will require firms to develop a comprehensive testing program to ensure the operational resilience of its ICT systems. Tests to be conducted include both scenario tests of certain risks faced by the firm, as well as cyber tests and gap analyses. Certain firms may also be required to carry out advance testing by means of TLPT. Any issues that are identified by such tests should be rectified and addressed appropriately. Clearly, many financial institutions will already have testing programmes in place but it will be important to perform a gap analysis of current procedures against the DORA framework.

DORA: Incident Reporting

- DORA requires financial institutions to report ICT-related incidents to their local competent authority. This will include an initial notification, an intermediate report during the investigation and a final report once the root cause analysis has been completed. The specific time frames and requirements for these reports will be drafted in upcoming regulatory technical standards. Certain sub-sectors, notably the payment services sector, are already subject to incident reporting regimes which will ultimately be consolidated under DORA.

DORA: Contract Requirements

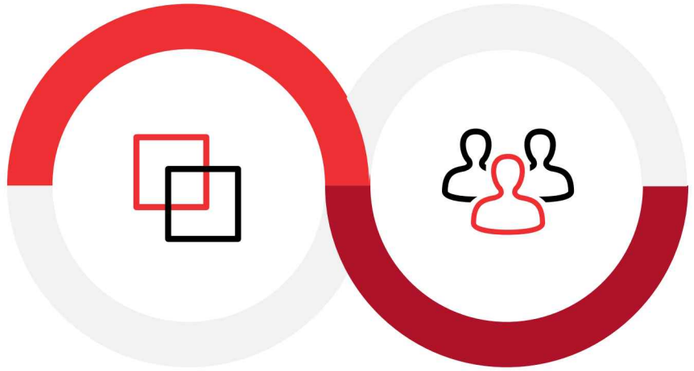
- DORA requires financial institutions to ensure that certain mandatory provisions are included within their agreements with ICT service providers. Many of these requirements are similar to mandatory requirements included in existing rules or standards on outsourcing issued by the financial services regulators in Europe (e.g., the EBA Outsourcing Guidelines). DORA includes additional requirements for contracts where the ICT services support a firm's critical or important functions.

NIS2 requirements

- The EU has recently updated the Network and Information Systems Directive, which applies to financial market infrastructure and banking as a sector of high criticality. NIS2 will need to be considered alongside cyber requirements under DORA. (The UK is also working on its own equivalent version of NIS2.)

How can Baker McKenzie help you?

Baker McKenzie offers an end-to-end solution which provides the right blend of legal expertise and tested process to help you manage the impact of DORA on your business.

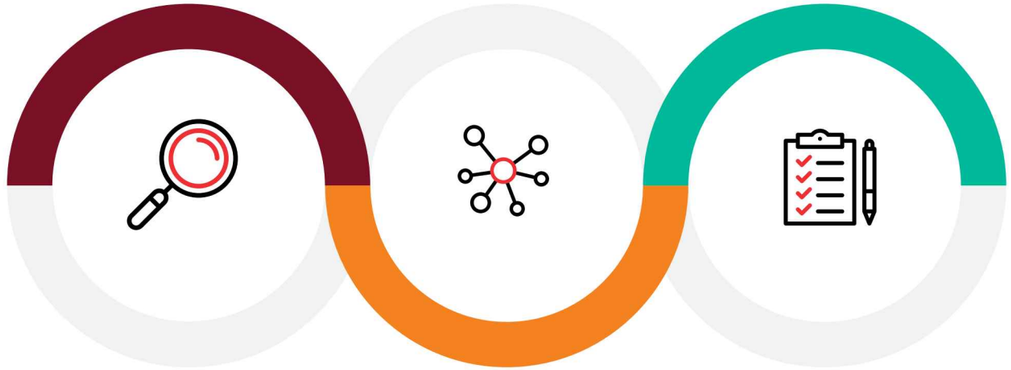


Our dedicated team of financial services, commercial, tech and cyber security specialists will partner seamlessly with your project team and tailor our support to address your specific business needs. We will provide hands-on, practical and clear guidance throughout the transition process, as we work closely with you to ensure your business complies with the new regulation.

Risk assessment as a first step...

1 Assess and review current risk management systems, policies, procedures and ICT controls against regulatory requirements for the purposes of creating a DORA compliant risk management framework.

3 Provide risk assessment report providing a summary of our conclusions, risk rating and our recommended roadmap to address DORA.



2 Analyse FI's current policies around cybersecurity and reporting of data-related incidents to account for new requirements introduced by DORA and review template agreements for ICT services against DORA requirements.

Here you may also want to consider NIS2 and related requirements.

What will the typical scope of an end-to-end solution look like?

Scope	Baker McKenzie support
DORA Risk Management Framework	DORA requires financial institutions to have a robust risk management framework in place to identify and mitigate against certain ICT and other technological risks. Baker McKenzie can assist you in: » Reviewing your current ICT related tools, policies and procedures to assess their level of compliance with DORA and the possible risks that these controls may pose » Supporting the production of any new policies and procedures that are required as part of the risk management framework » Supporting on reviews and updates to the risk management framework once the framework is in place » Providing guidance to boards and management committees, reflecting their responsibility for the risk management framework.
Security	Provide legal support in connection with the cyber-security implications, including: » Contributing to internal operational playbooks concerning security, incident management, pen testing, etc » Supporting/table top IM exercises and cyber-security training » Advising on amendments to security provisions in contract templates and related negotiation playbooks including fall-back clauses etc
Incident Reporting	DORA introduces new or in some cases codifies existing requirements to report cyber and other ICT related incidents to financial services regulators. BM can assist with this by providing legal support in respect of incident reporting, including: » Reviewing, providing and updating data-incident policies and procedures to cover for the reporting obligations imposed by DORA; » Assessing whether an incident is reportable under DORA; and » Assisting in the filing of the report
Operational Resilience	DORA requires firms to carry out various operational resilience tests. We can assist in the preparation of policies and procedures for the purposes of these tests.
Sub-processors / contractors	» Provide legal support in terms of analysis of sub-contractors/outsourcers for in-scope services » Advise on amendments to sub-processor/contractor clauses of templates and related negotiation playbooks including fall-back clauses » Liaise with DP and cyber teams as required to ensure alignment
Contract updates	Advise on amendments to contract templates and related negotiation playbooks (including fall-back clauses) with respect to the following topics: » Sub-contracting » Incident Management » Service Levels » DR/BCP » Audit » Exit » Termination

Other areas of support

Scope	Baker McKenzie support
Vendor Communications and engagement	Provide legal support in connection with communications and materials produced for customers concerning DORA
Training	Support on training your relevant legal, regulatory and business teams on DORAs, including training on roll-out of updated contract templates
Monitoring	Monitoring for DORA developments and equivalent rules in specified countries
Ad hoc advice	Provide support to your DORA Programme teams on legal interpretation and market practice generally
Events and thought leadership (non-chargeable collaboration)	» BM could participate in your events around DORA / Operational Resilience » You could participate in BM events around DORA / Operational Resilience » We could explore partnering with third parties on events » We could collaborate on thought leadership

Key contacts: London

To support your business with its DORA programme, speak to our team at Baker McKenzie.

Caitlin McErlane
Partner
Financial Services Regulatory

+442079191894
Caitlin.Mcerlane@bakermckenzie.com

Sue McLean
Partner,
Technology

+442079191998
Sue.McLean@bakermckenzie.com

Paul Glass
Partner
Cybersecurity & Data Privacy

+442079191288
Paul.Glass@bakermckenzie.com

Mark Simpson
Partner
Financial Services Regulatory

+442079191403
Mark.Simpson@bakermckenzie.com

Baker McKenzie delivers integrated solutions to complex challenges.

Our unique culture, developed over 70 years, enables our 13,000 people to work together across borders and practice areas. We provide seamless advice underpinned by local market knowledge and deep sector expertise so that business leaders can feel confident in driving growth that is both sustainable and inclusive.

bakermckenzie.com