CLIFFORD
CHANCE

DORA: WHAT THE NEW EUROPEAN FRAMEWORK FOR DIGITAL OPERATIONAL RESILIENCE MEANS FOR YOUR BUSINESS

— THOUGHT LEADERSHIP

NOVEMBER 2022

DORA: WHAT THE NEW EUROPEAN FRAMEWORK FOR DIGITAL OPERATIONAL RESILIENCE MEANS FOR YOUR BUSINESS

On 10 November 2022, the European Parliament voted to adopt a new EU regulation on digital operational resilience for the financial sector (DORA). With obligations under DORA coming into effect late in 2024 or early 2025 at the latest, in this briefing we take a closer look at its impact and consider what the regulation will mean for firms, their senior managers and operations and what firms should be doing now in preparation for day one compliance.

What is DORA?

Aimed at harmonising national rules around operational resilience and cybersecurity regulation across the EU, DORA establishes uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provide services related to information communication technologies (ICT), such as cloud platforms or data analytics services. DORA creates a regulatory framework on digital operational resilience whereby all in-scope firms need to make sure that they can withstand, respond to, and recover from, all types of ICT-related disruptions and threats. ICT is defined broadly to include digital and data services provided through ICT systems to one or more internal or external users, on an ongoing basis.

DORA forms part of the EU's Digital Finance Package (DFP), which aims to develop a harmonised European approach to digital finance that fosters technological development and ensures financial stability and consumer protection. The DFP also includes legislative proposals on markets in cryptoassets (MiCA), distributed ledger technology and a digital finance strategy.

Who will need to comply with DORA?

DORA will apply to financial entities, including: credit institutions, payment institutions, e-money institutions, investment firms, cryptoasset service providers (authorised under MiCA) and issuers of asset-referenced tokens, central securities depositories, central counterparties, trading venues, trade repositories, managers of alternative investment funds and management companies, data reporting service providers, insurance and reinsurance undertakings, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, institutions for occupational retirement pensions, credit rating agencies, administrators of critical benchmarks, crowdfunding service providers and securitisation repositories (Financial Entities).

DORA will also apply to ICT third-party service providers which the European Supervisory Authorities (the European Banking Authority (EBA), the European Securities and Markets Authority and the European Insurance and Occupational Pensions Authority, acting through their Joint Committee) (ESAs) designate as "critical" for Financial Entities (Critical ICT Third-Party Providers) through a newly established oversight framework. The ESAs would make this designation based on a set of qualitative and quantitative criteria, including:

- the systemic impact on the stability, continuity or quality of financial services in the event that the ICT third-party provider faced a large-scale operational failure to provide its services;
- the systemic character or importance of Financial Entities that rely on the ICT third-party service provider;
- the degree of reliance of those Financial Entities on the services provided by the ICT third-party service provider in relation to critical or important functions of those Financial Entities; and
- the degree of substitutability of the ICT third-party service provider.

Any ICT third-party service provider not designated as critical would have the option to voluntarily "opt in" to the oversight.

The ESAs may not make a designation in relation to certain excluded categories of ICT third–party service providers, including where Financial Entities are providing ICT services to other Financial Entities, to ICT third–party service providers delivering services predominantly to the entities of their own group or to those providing ICT services solely in one Member State to financial entities that are active only in that Member State.

What are the key obligations?

DORA introduces targeted rules on ICT risk management capability, reporting and testing, in a way which enables Financial Entities to withstand, respond to and recover from ICT incidents. In principle, some of the requirements imposed by DORA, such as for ICT risk management, are already reflected to a certain extent in existing EU guidance (for example, the EBA Guidelines on ICT and security risk management).

The proposals include requirements relating to:

- **ICT risk management**
  DORA sets out key principles around internal controls and governance structures. A Financial Entity's management body will be expected to be responsible for defining, approving, overseeing and being continuously accountable for a firm's ICT risk management framework as part of its overall risk management framework. As part of the ICT risk management framework, Financial Entities need to maintain resilient ICT systems, revolving around specific functions in ICT risk management such as identification of risks, protection and prevention, detection, response and recovery and stakeholder communication.
- **Reporting of ICT-related incidents**
  DORA aims to create a consistent incident reporting mechanism, including a management process to detect, manage and notify ICT-related incidents.

  Incidents deemed "major" would need to be reported to competent authorities within strict time frames, including initial notifications "without delay" on the same day or next day by using mandatory reporting templates. In some cases, communication to service users or customers may be required.
- **Testing**
  As part of the ICT risk management framework, DORA requires Financial Entities to adopt a robust and comprehensive digital operational resilience testing programme covering ICT tools, systems and processes.

  Certain Financial Entities must carry out advanced testing of their ICT tools, systems and processes at least every three years using threat-led penetration tests.
- **Information sharing**
  DORA contains provisions which should facilitate the sharing, among Financial Entities, of cyber threat information and intelligence, including indicators of compromise, tactics, techniques and procedures, cyber security alerts and configuration tools to strengthen digital operational resilience.
- **Localisation**
  Financial Entities will only be permitted to make use of the services of a third-country Critical ICT Third-Party Provider if such provider establishes a subsidiary in the EU within 12 months following its designation as a Critical ICT Third-Party Provider.

A simplified set of ICT risk framework requirements will apply to certain Financial Entities, including small and non-interconnected investment firms and payment institutions exempted under the Second Payment Services Directive. Such entities will need to comply with a reduced set of requirements under DORA, including the requirement to put in place and maintain a sound and documented risk management framework that details the mechanisms and measures aimed at a quick, efficient and comprehensive management of all ICT risks, including for the protection of relevant physical components and infrastructures.

Documentation impact

DORA also sets out a number of requirements for contracts between Financial Entities and ICT third-party service providers in relation to ICT services. These will affect both existing and new contracts.

DORA sets out requirements for all contractual arrangements on the use of ICT services, with more extensive requirements applying to those contracts which support critical or important functions. All relevant contracts must be in writing and clearly allocate the rights and obligations of the Financial Entity and the ICT third-party service provider.

The contractual requirements in DORA are closely aligned to the EBA guidelines on outsourcing arrangements. Additions for all contracts include requirements for providers to assist when certain ICT-related incidents impact the service "at no additional cost or at a cost that is determined ex-ante". There is also a requirement for providers to participate "in the financial entities' ICT security awareness programs and digital operational resilience trainings".

DORA is not as prescriptive as the existing EBA guidelines on outsourcing in relation to subcontracting requirements. At the pre-contractual stage, Financial Entities are to engage in an in-depth analysis of subcontracting arrangements, notably when concluded with ICT third-party service providers established in a third country. For critical or important functions, Financial Entities are to assess whether and how potentially long or complex chains of subcontracting may impact their ability to monitor fully the contracted functions, and the ability of the competent authority to supervise the entity effectively.

The only contractual requirements relating to subcontracting set out in DORA are for the contract to specify whether subcontracting is permitted, the conditions of subcontracting and the locations of subcontracted functions, ICT services and data processing activities.

Management Responsibility

In order to ensure full alignment between a Financial Entity's business strategy and the management of ICT risks relevant to it, the management body of the entity will be required to maintain an active and central role in steering and adapting the entity's ICT risk framework and overall digital resilience strategy. Relevant requirements broadly reflect those in existing EU guidelines, including the EBA Guidelines on ICT and security risk management and Guidelines on outsourcing arrangements.

The management body will bear ultimate responsibility for managing a Financial Entity's ICT risks and is required to set clear roles and responsibilities for all ICT-related functions and establish appropriate governance arrangements to ensure effective and timely communication, co-operation and co-ordination between such functions.

Financial Entities (other than those that qualify as a microenterprise) must establish a dedicated role to monitor arrangements with ICT third-party providers or designate a member of senior management as responsible for overseeing the related risk exposure and relevant documentation.

In order to discharge their duties competently, the members of the management body will be required to have and maintain sufficient knowledge and skills to understand and assess ICT risks and their impact on the operations of the Financial Entity. This will mean that entities need to have in place a programme of regular training, not just for their staff directly engaged in the management of ICT risks and overseeing arrangements with ICT third-party providers, but also for members of the management board.

What should firms be doing now to prepare?

Although it is not expected that DORA will apply to in-scope entities until late 2024 (see below), firms should now begin considering the steps that they will need to take to ensure day one compliance. These include:

- **Scope out impact**
  Taking a risk-based approach reflective of their size, nature, scale and the complexity of their services and operations, Financial Entities should begin to scope out the impact of DORA on their business. Firms should carry out a comprehensive gap analysis of their existing ICT-risk management processes against the new requirements introduced by DORA to identify any aspects of their existing processes that will be impacted by the new requirements and develop detailed implementation plans setting out the steps that will need to be taken to effect relevant changes. As part of this, Financial Entities should ensure that they have in place appropriate: (i) capabilities to enable a strong and effective ICT risk management environment; (ii) mechanisms and policies for handling all ICT-related incidents and reporting major incidents; and (iii) policies for the testing of ICT systems, controls and processes and the management of ICT third-party risk. This process will be iterative as some of the more detailed requirements of DORA will be further developed through technical standards to be published by the ESAs in due course.

- **Critical ICT Third-Party Providers**
  Critical ICT Third-Party Providers will be required to have in place comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risks which they may pose to Financial Entities.

  Although DORA provides that the designation mechanism (pursuant to which the ESAs may designate an ICT third-party service provider as "critical") must not be used until the Commission has adopted a delegated act specifying further details on the criteria to be used in making such an assessment (to be adopted within 18 months after the date on which DORA enters into force), it is expected that certain categories of providers, such as cloud computing service providers who provide ICT services to Financial Entities, will be designated as Critical Third-Party Providers.

  Consequently, such providers may wish to begin the task of benchmarking their existing systems, controls and processes against existing guidelines, such as the EBA Guidelines on ICT and security risk management and Guidelines on outsourcing arrangements, to the extent required, to identify areas that require further investment and maturity. They will also need to consider whether new and existing contracts give them sufficient flexibility to comply with new regulatory rules, orders and directions, even if this would otherwise be inconsistent with their contractual obligations.

  As set out above, certain categories of ICT third-party service providers are expressly excluded from the designation mechanism, including Financial Entities providing ICT services to other Financial Entities, ICT intra-group service providers and ICT third-party service providers providing ICT services solely in one Member State to Financial Entities that are only active in that Member State.

- **Third Country Critical ICT Third-Party Providers – Subsidiarisation**
  The EU subsidiarisation requirement that will apply to third country Critical ICT Third-Party Providers is one that will necessitate early engagement between such providers and the Financial Entities that they serve. While it is not clear what role the EU subsidiary must play in the provision of services to the relevant Financial Entity (e.g. whether the provider must act as contractual counterparty), Recital 58 of DORA indicates that the requirement to set up a subsidiary in the EU does not prevent ICT services and related technical support from being provided from facilities and infrastructures located outside the EU. Nevertheless, where a relevant third country ICT third-party provider that is likely to be designated as "critical" indicates that it does not intend to establish a subsidiary in the EU, even following a designation as such by the ESAs, Financial Entities may wish to commence the process of identifying alternative providers, since they will not be permitted to obtain ICT services from a third country Critical ICT Third-Party Provider that fails to establish a subsidiary in the EU within 12 months following its designation as critical.

Companies that consider they are likely to be classified as Critical ICT Third-Party Providers that do not already have an establishment or subsidiary located in the EU should begin to consider now which Member State would be most appropriate to establish a new subsidiary in, taking into account their business operations and the various applicable legal requirements.

- **Documentation impact**
  As noted above, DORA sets out core contractual rights in relation to several elements in the performance and termination of contracts with a view to enshrine certain minimum safeguards underpinning the ability of Financial Entities to monitor effectively all risk emerging at ICT third-party level. Some contractual requirements set out in DORA are mandatory and will need to be included in contracts, if not already reflected. Others take the form of principles and recommendations and may require negotiation between the relevant parties. Early mapping and engagement in this respect will be important. Additionally, parties may wish to consider benchmarking their existing contractual arrangements against relevant requirements set out in DORA, as well as existing standard contractual clauses developed by EU institutions. For example, Recital 55 of DORA notes that "the voluntary use of contractual clauses developed by the Commission for cloud computing services may provide comfort for Financial Entities and ICT third-party providers by enhancing the level of legal certainty on the use of cloud computing services in full alignment with requirements and expectations set out by the financial services regulation".

As the industry awaits more detailed technical standards to be developed and published by the relevant ESAs, as well as DORA compromise/Level 1 text, in-scope entities may consider using existing guidelines such as the EBA Guidelines on ICT and security risk management and Guidelines on outsourcing arrangements as useful benchmarking tools in preparation for day one compliance.

How does DORA interact with NIS2?

The second iteration of the Security of Network and Information Systems Directive (NIS2) aims to strengthen security requirements and provide further harmonisation of Member States' cybersecurity laws, replacing the original NIS Directive of 2016 (NIS1). Its timeline is similar to that for DORA, with a provisional agreement among EU institutions reached in May 2022, and a vote by the European Parliament anticipated by the end of 2022. NIS2 significantly extends the scope of NIS1 by adding new sectors, including "digital providers" such as social media platforms and online marketplaces, for example, but importantly also introduces uniform size criteria for assessing whether certain financial institutions (and other entities) fall within its scope. NIS2 sets out cybersecurity risk management and reporting obligations for relevant organisations, as well as obligations on cybersecurity information sharing, so there is some overlap in coverage with DORA. However, this has been addressed during the legislative process to ensure that financial entities will have full clarity on the different rules on digital operational resilience that they need to comply with when operating within the EU. NIS2 specifically provides that any overlap will be addressed by DORA being considered as lex specialis (ie a more specific law that will override the more general NIS2 provisions).

How does DORA compare with international developments?

The introduction of DORA in the EU reflects a global focus on operational resilience and strengthening cybersecurity standards in the wake of ever-increasing digitalisation of financial services and increasingly sophisticated cyber incidents. For example, in March 2021, the Basel Committee on Banking Supervision issued its **Principles for operational resilience**, as well as an updated set of **Principles for the sound management of operational risk** (PSMOR), which aim to make banks better able to withstand, adapt to and recover from severe adverse events.

In October 2022, following a G20 request, the Financial Stability Board (FSB) published a **consultation on Achieving Greater Convergence in Cyber Incident Reporting**, recognising that timely and accurate information on cyber incidents is crucial for effective incident response and recovery and promoting financial stability and with a view to ensuring that financial institutions operating across borders are not subject to multiple conflicting regimes. The FSB proposals include recommendations to address the challenges to achieving greater international convergence in cyber incident reporting, work on establishing common terminologies related to cyber incidents and a proposal to develop a common format for incident reporting exchange.

Following its departure from the EU, the UK has introduced a Financial Services and Markets Bill (the UK Bill) which includes proposals to regulate cloud service providers and other critical third parties supplying services to UK regulated firms and financial market infrastructures. HM Treasury would have powers to designate service suppliers as 'critical' and the UK regulators would have new powers to directly oversee designated suppliers, which would be subject to new minimum resilience standards. While the proposals have the same ambitions as, and there are similarities with, the requirements under DORA, there are a number of key differences between them.

For example, the proposed enforcement regime under DORA for Critical ICT Third-Party Providers is very different from the equivalent regime proposed by the UK Bill. Under DORA, the ESAs will be designated as "Lead Overseers", but with the power only to make 'recommendations' to Critical ICT Third-Party Providers, in contrast to the ability for UK regulators to make rules applying to, or to give directions to, critical third parties subject to the UK Bill, with the ability to issue sanctions for non-compliance. Under DORA, non-compliance by a Critical ICT Third-Party Provider with recommendations gives the Lead Overseer the ability to notify and publicise such non-compliance and "as a last resort" the option to require Financial Entities to temporarily suspend services provided by such provider until the relevant risks identified in the recommendations have been addressed.

This means that the liability and contractual issues for Critical ICT Third-Party Providers providing services in the EU will be different than for those providing services in the UK, and that contracts for each will need to be considered and negotiated carefully.

Please see **our briefing on the UK proposals** for further details, including a detailed comparison of obligations under DORA and the UK Bill.

Next steps and legislative timeline

Following adoption of DORA by the European Parliament plenary session on 10 November 2022, the regulation is now passing through the final technical stages of the formal procedure for European legislation. The text still needs to be formally approved by the EU Council before being published in the Official Journal, which is expected in December 2022 or January 2023.

DORA will come into effect on the twentieth day following the day on which it is published in the Official Journal. It will apply, with direct effect, 24 months from the date on which it enters into force. Therefore, it is expected that DORA will apply to in-scope firms from late 2024 or early 2025 at the latest.

AUTHORS

Kikun Alo
Senior Associate
London
T: +44 207006 4067
E: kikun.alo@cliffordchance.com

Marc Benzler
Partner
Frankfurt
T: +49 69 7199 3304
E: marc.benzler@cliffordchance.com

Christian Hissnauer
Counsel
Frankfurt
T: +49 69 7199 3102
E: christian.hissnauer@cliffordchance.com

Monica Sah
Partner
London
T: +44 207006 1103
E: monica.sah@cliffordchance.com

Laura Nixon
Knowledge Director
London
T: +44 207006 8385
E: laura.nixon@cliffordchance.com

CONTACTS

Belgium

Lounia Czupper
Partner
Brussels
T: +32 2 533 5987
E: lounia.czupper@cliffordchance.com

France

Pierre d'Ormesson
Avocat
Paris
T: +33 1 4405 5135
E: pierre.dormesson@cliffordchance.com

Frédérick Lacroix
Partner
Paris
T: +33 1 4405 5241
E: frederick.lacroix@cliffordchance.com

Hélène Kouyaté
Counsel
Paris
T: +33 1 4405 5226
E: helene.kouyate@cliffordchance.com

Germany

Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com

Gregor Evenkamp
Partner
Munich
T: +49 89 21632 8800
E: gregor.evenkamp@cliffordchance.com

Thomas Voland
Partner
Düsseldorf
T: +49 211 4355 5642
E: thomas.voland@cliffordchance.com

Italy

Riccardo Coassin
Lawyer - Counsel
Milan
T: +39 02 8063 4263
E: riccardo.coassin@cliffordchance.com

Andrea Tuninetti Ferrari
Lawyer - Counsel
Milan
T: +39 02 8063 4435
E: andrea.tuninettiferrari@cliffordchance.com

Luxembourg

Steve Jacoby
Regional Managing Partner CE
Luxembourg
T: +352 48 50 50 219
E: steve.jacoby@cliffordchance.com

Oliver Zwick
Counsel
Luxembourg
T: +352 48 50 50 476
E: oliver.zwick@cliffordchance.com

The Netherlands

Marian Scheele
Senior Counsel
Amsterdam
T: +31 20 711 9524
E: marian.scheele@cliffordchance.com

The Netherlands

Jaap Tempelman
Senior counsel and co-head of Tech Group
Amsterdam
T: +31 20 711 9192
E: jaap.tempelman@cliffordchance.com

Wouter van den Bosch
Senior Associate
Amsterdam
T: +31 20 711 9407
E: wouter.vandenbosch@cliffordchance.com

Poland

Anna Biała
Counsel
Warsaw
T: +48 22429 9692
E: anna.biala@cliffordchance.com

Spain

Jaime Denis
Abogado
Madrid
T: +34 91 590 7521
E: jaime.denis@cliffordchance.com

Eduardo García
Partner
Madrid
T: +34 91 590 9411
E: eduardo.garcia@cliffordchance.com

Carlos Zabala
Counsel
Madrid
T: +34 91 590 7515
E: carlos.zabala@cliffordchance.com

UK

Zayed Al Jamil
Partner
London
T: +44 207006 3005
E: zayed.aljamil@cliffordchance.com

Kate Scott
Partner
London
T: +44 207006 4442
E: kate.scott@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

2211-003471