Bird & Bird

The Digital Operational Resilience Act (DORA)

An Overview

Contents

The operational context

Introduction

The digital transformation of the financial sector depends on the availability of a secure, efficient, affordable and high-quality information and communications technology (ICT) infrastructure. ICT services enable business expansion and scalability in the deployment of financial activities consistently with demand evolution, while driving cost reduction in financial intermediation and allowing ICT tools to manage complex internal processes.

Since cutting-edge technology is more and more key-competitive advantage and its evolution is speeding up, technology catching up means a constant flow of investments in digitalisation, data collection and analysis as well as security, alongside technological development.

This is the reason why financial institutions increasingly rely on external providers of ICT services, especially of cloud services. While cloud solutions bring opportunities, they also expose financial institutions to operational risks (e.g., loss or alteration of data, fraud, cyber threats, ICT risks)

In addition, the market of cloud services is dominated by few big-techs, which together hold a market share of over 70%. The use of a small number of cloud service providers by a large number of financial institutions and financial market operators can generate systemic concentrations that could adversely impact financial stability in case one or more of them experienced a major disruption in the provision of services.

Moreover, the high level of interconnectedness existing between financial entities, financial markets and financial market infrastructures, and in particular the interdependencies of their ICT systems, may potentially constitute a systemic vulnerability.

Furthermore, it is worth mentioning that financial institutions operating across borders and holding multiple licences face operational challenges in managing ICT risks and mitigating the adverse effects of ICT incidents due to non-uniform legal frameworks and different enforcement policies.

The digital resilience of financial market participants is a key issue that needs to be addressed by harmonised rules across the EU to maintain the technical safety, smooth functioning and stability of the EU financial system.

The legal background

ICT security and digital resilience have been less in the focus of the post-crisis regulatory agenda, not yet sufficiently built in their operational frameworks.

Changes to the EU financial services legislation, which introduced a Single Rulebook regulating much of the financial risks associated with financial services, did not fully address digital operational resilience. The measures taken in relation to this topic were often devised as minimum harmonisation directives or principled-based regulations, leaving substantial room for diverging approaches across the Member States. In addition, there has been only some limited or incomplete focus on ICT risks in the context of the operational risk coverage.

Current EU rules on managing ICT risks vary significantly between financial services sectors, being developed at differing moments over the past decade. They only partly address ICT risks, with a few exceptions (e.g. payments and post-trading services), often only as a matter of secondary concern. National requirements and supervisory guidelines have tried to fill the gaps, though not necessarily in a consistent manner.

This situation has been deemed to fragment the single market, undermine the stability and integrity of the EU financial sector, and put consumer and investor protection at risk.

The European Commission has therefore advocated the need to establish a detailed and comprehensive framework on digital operational resilience for EU financial entities.

Institutional inputs

In the EU Fintech Action Plan (March 2018), even under pressure from the European Parliament, cyber resilience of the financial sector was identified as a political priority since "*operational and cyber risks pose a mounting threat to the stability of the financial system and undermine the confidence that is vital for our financial markets*". It was recognised that "*at EU level, current financial services legislation, in particular covering financial market infrastructures and payments, already contains specific requirements on the integrity of IT resources and systems and their governance. In other areas, requirements are more general, for example in the case of business continuity or general operational risk requirements*". The Fintech Action Plan pointed out, inter alia, the need for closer cooperation and coordination of threat intelligence sharing across the EU financial sector also with regard to penetration and resilience test results. The Commission invited the ESAs to map, by Q1 2019, the existing supervisory practices across financial sectors around ICT security and governance requirements, and where appropriate: a) to consider issuing guidelines and, b) if necessary, provide the Commission with technical advice on the need for legislative improvements.

Bird & Bird retains its leading position for advice on complex IT and digitalisation projects and technology-driven transactions and advises on the entire spectrum of high tech, including IoT, blockchain, AI and machine learning, cloud and big/smart data.

Legal 500 EMEA, 2020

The ESAs - in their Joint Advice to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector [JC 2019 26 (2019)] - highlighted that the requirements for firms to address ICT risk are fragmented and inconsistent across the financial sector. Specifically, the ESAs called for a more coherent approach in addressing ICT risk in finance and recommended the Commission to strengthen, in a proportionate way, the digital operational resilience of the financial services industry through an EU sector-specific initiative. The ESAs advice was a response to the Commission's 2018 Fintech action plan.

Moreover, the High-Level Forum on Capital Markets Union (June 2020) recommended in its final report, among others, that the Commission develops (i) voluntary standard clauses in contractual arrangements between financial institutions and providers of cloud services to

enable financial institutions to better assess and manage risks related to their reliance on third party services providers; (ii) a new harmonised legislative framework to strengthen the digital operational resilience of the EU financial sector and to make secure outsourcing critical and important functions by financial institutions to cloud services providers, including an appropriate mechanism for the supervision of these ICT service providers; and (iii) digital competitiveness of the EU by encouraging the development of EU cloud providers.

On Sept. 24, 2020, the European Commission had published a proposal for a new Digital Operational Resilience Regulation, with the aim of consolidating and updating ICT risk requirements across the financial sector to ensure that all financial system participants were subject to a common set of rules to prevent and mitigate ICT risks, particularly cyber threats, to their operations.

This proposal brought together, for the first time, the rules related to ICT risk in the financial sector into one single legislative act to fill gaps and address current inconsistencies in sectoral legislation.

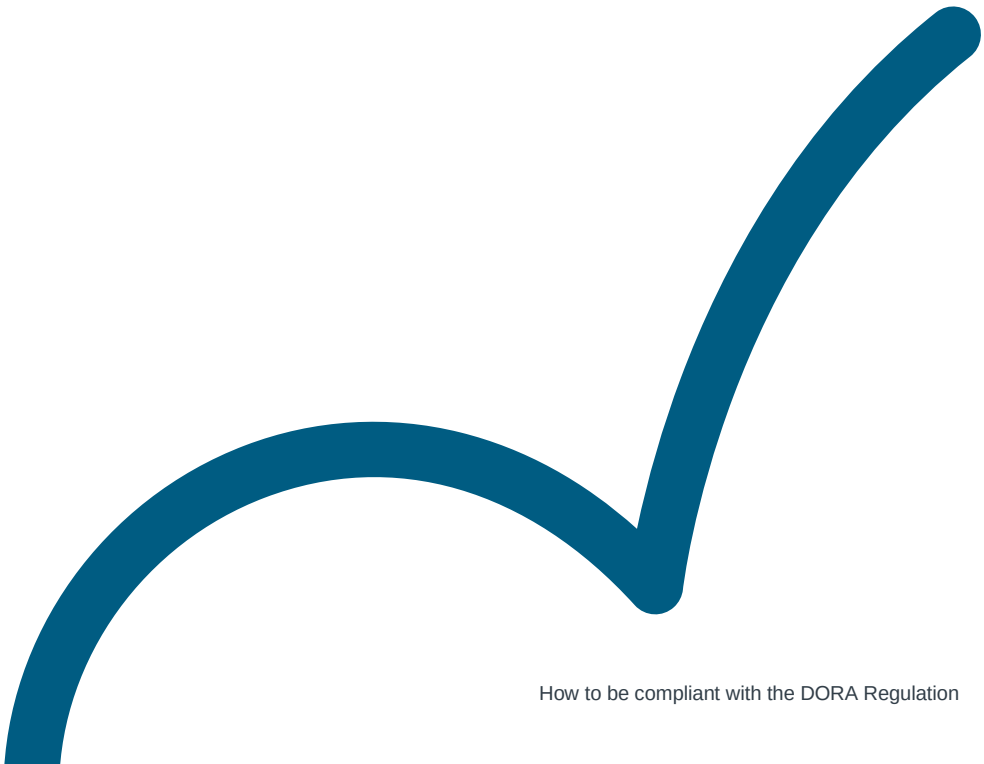
Trilogues between the EU co-Legislators started on 25 January 2022 and ended in a provisional agreement on 10 May 2022.

On November 10, 2022, the European Parliament adopted its first reading position on DORA. On November 28, 2022, the Council approved the European Parliament's DORA text.

In accordance with the ordinary legislative procedure, the proposal for Regulation was formally adopted on 14 December 2022 with the signatures of the President of the European Parliament and the President of the Council.

This will apply 24 months after the date of its entry into force, i.e., after the 20th day of its publication in the Official Journal of the European Union. Therefore, **DORA will apply at the beginning of 2025.**

It shall be binding in its entirety and directly applicable in all EU Member States.



The Digital Operational Resilience Act (DORA)

- DORA is part of the EU's Digital Finance Package, which aims to develop a harmonized European approach to digital finance to facilitate the secure adoption of technology by financial institutions.
- DORA includes:
  a. a Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (broadly defined) (hereafter, DORA Regulation or the Regulation), in order to ensure that detailed requirements be effectively and directly applicable in a uniform manner within the EU. It also innovates certain risk management requirements of various sectoral legal measures: (a) Regulation (EC) n° 1060/2009 on credit rating agencies; (b) Regulation (EU) n° 648/2012 on OTC derivatives, central counterparties and trade repositories; (c) Regulation (EU) n° 909/2014 on improving securities settlement in the European Union and on central securities depositories; (d) Regulation (EU) n° 600/2014 on markets in financial instruments; (e) Regulation (EU) 2016/1011 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds;
  b. a Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending the following Directives: 2009/65/EC (UCITS), 2009/138/EC (Solvency II), 2011/61/EU (AIFMD), 2013/36/EU (CRD IV), 2014/59/EU (BRRD), 2014/65/EU (MiFID II), (EU) 2015/2366 (PSD2) and (EU) 2016/2341 (EPAP / IORPs) as regards digital operational resilience for the financial sector.
- Regulatory Technical Standards should be developed - on the basis of Technical Advices made by the ESA, in consultation with the European Union Agency on Cybersecurity (ENISA) - in the areas of ICT risk management security policies, reporting, testing and key requirements for a sound monitoring of ICT third-party risks.
- Implementing Technical Standards should be developed - on the basis of Technical Advices made by the ESAs - to establish standardised templates, forms and procedures for financial entities to report a major ICT-related incident, as well as standardized templates for the register of information.
- The DORA Regulation establishes uniform requirements for the security of networks and information systems supporting the business processes of financial entities, while requiring full alignment and overall consistency between their business strategies and ICT risk management.
- The management body of the financial institution maintains a central and active role in adopting and steering the digital operational resilience strategy and governance (including tools, people, processes, and policies), taking full and ultimate responsibility for it.
- Specifically, the Regulation introduces common targeted rules for financial entities on ICT risk-management, incident reporting, digital operational resilience testing, information sharing and ICT third-party risk monitoring.
- Financial institutions implement the DORA rules in accordance with the principle of proportionality, i.e., taking into account their size, overall risk profile and nature, scale, and complexity of their services, activities and operations.
- DORA provides simplified ICT risk management rules for small financial entities. It does not apply in case of relationship with certain third-party ICT service providers (e.g., ICT service providers operating only within a group or in an EU member state).
- It also establishes a Union "oversight framework" for all critical ICT third-party services providers to financial institutions, including service providers of cloud computing, software, hardware, data analytics and data centre.

Scope

The Regulation covers a wide range of regulated financial entities at EU level and also ICT third-party service providers, in order to ensure that ICT-risks are managed in a homogeneous and consistent way, namely:

a credit institutions

b payment institutions and electronic money institutions

c account information service providers

d investment firms

e crypto-asset service providers (authorised under the Regulation on markets in crypto-assets - MiCAR) and issuers of asset-referenced tokens

f trading venues

g central securities depositories, central counterparties, trade repositories, data reporting service providers

h managers of alternative investment funds and management companies

i insurance and reinsurance undertakings, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries

j institutions for occupational retirement provisions

k credit rating agencies

l administrators of critical benchmarks

m crowdfunding service providers and

n securitisation repositories

o ICT third-party service providers*

* *ICT service providers designated as critical for financial entities by European Supervisory Authorities.*

Key areas of the DORA Regulation

The Regulation sets out important rules applicable to financial entities in the following key areas:

1. Governance and Organization requirements (Article 5)

- full alignment and overall consistency between financial entities' business strategies and the conduct of ICT risk management;
- internal governance and control frameworks ensuring an effective and prudent management of all ICT risks;
- full responsibility of the management body in defining, approving, and overseeing the implementation of all provisions related to the ICT risk management framework.
- In bearing ultimate responsibility for managing ICT risks, the financial entities' management body shall, *inter alia*:
  - a set and approve the Digital Operational Resilience Strategy;
  - b set clear roles and responsibilities for all ICT-related functions and establish appropriate governance arrangements to ensure effective and timely communication, cooperation and coordination among those functions;
  - c approve, oversee and periodically review the implementation of the financial entity's ICT Business Continuity Policy and ICT Response and Recovery Plans;
  - d approve and periodically review the financial entity's policy on arrangements regarding the use of ICT services provided by ICT third-party service providers;
  - e be duly informed of the arrangements concluded with ICT third-party service providers on the use of ICT services and of any relevant planned material changes;
  - f establish a role in order to monitor the arrangements concluded with ICT third-party service providers on the use of ICT services or designate a member of senior management as responsible for overseeing the related risk exposure and relevant documentation.

2. ICT risk management requirements (Articles 6 to 16)

- The DORA Regulation requirements revolve around specific activities in ICT risk management (risk identification, protection and prevention, detection, response and recovery, backup policies, learning and evolving and communication).
- Digital operational resilience is rooted in a set of key principles and requirements of the ICT Risk Management Framework, including strategies, policies, procedures and tools necessary to ensure that all information and ICT assets (including computer software, hardware, and infrastructure) are duly and adequately protected from risks such as damage, unauthorized access and illicit use.
- ICT systems, protocols, and tools have sufficient capacity to accurately process the data needed to carry out activities and provide services in a timely manner and are technologically resilient under stressed market conditions or other adverse situations.
- Responsibility for managing and overseeing ICT risk is assigned to a control function with an appropriate level of segregation and independence.
- The Digital Operational Resilience Strategy includes "*a holistic ICT multi-vendor strategy, at group or entity level, showing key dependencies on ICT third-party service providers and explaining the rationale behind the procurement mix of ICT third-party service providers*" (Art.6, 9).
- Moreover, among other things, financial entities are required to:
  - identify and map all information and ICT assets, specifying which are considered critical and their links and interdependencies;
  - carry out specific ICT risk assessments on all legacy ICT systems on a regular basis, at least annually;
  - continuously monitor and control the security and functioning of ICT systems and tools;

- devote sufficient resources and capabilities to monitor user activity, the occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks;
- put in place, maintain and periodically test **appropriate ICT business continuity** [and ICT response and recovery] **plans**, notably with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers (Art.11, 4);

- The DORA Regulation itself does not set a specific methodology for ICT risk management, but rather relies on recognised European and international technical standards and industry best practices.

3. ICT-related incident management, classification and reporting (Articles 17 to 23)

- General obligation for financial entities to establish and implement a management process to monitor and record all ICT-related incidents and significant cyber threats, followed by the obligation to classify them according to the criteria detailed in the Regulation and further developed by the ESAs.
- Reporting at least ICT-related incidents that are deemed major to the relevant senior management and management body.
- Reporting major ICT-related incidents to the relevant competent authority. After an initial report, the submission of an interim report, if the status of the original incident has changed significantly, and a final report, when the root cause analysis has been completed.
- To set off a dialogue between financial entities and competent authorities that would help minimising the impact and identifying appropriate remedies, the reporting of major ICT related incidents should be complemented by supervisory feedback and guidance.

4. Digital operational resilience testing (Articles 24 to 27)

- Establishing, maintaining, and reviewing a robust and comprehensive testing program for digital operational resiliency as part of the ICT risk management framework to identify weaknesses, deficiencies and gaps and implement timely corrective actions.
- Setting up procedures and policies to address all issues identified through the testing exercise.
- Digital operational resilience testing should include
  - **appropriate assessment based on the application of the proportionality principle** (e.g., vulnerability assessments and scans, open-source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing or end-to-end testing);
  - **advanced testing** covering several or all critical or important functions, such as Threat-Led Penetration Testing (TLPT), for large financial entities (identified by competent authorities as significant and ICT mature).

    Credit institutions classified as significant should use only certified external verifiers to conduct TLPT.

5. Managing ICT third-party risk (Articles 28 to 30)

- The Regulation is designed to ensure a **sound monitoring of ICT third-party risks**, rebalancing relationship of big ICT service providers with financial entities and making the use of cloud services more secure and appropriately supervised to preserve the financial system's resilience ("*Financial entities shall manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework*").
- The use of ICT services by third parties shall not affect the financial operator's overall responsibility for compliance with and performance of all obligations under the DORA Regulation and applicable financial services legislation.
- This objective is pursued by DORA through principle-based rules that financial institutions must apply when monitoring risks arising from the provision of ICT services by third parties.
  - adoption and regularly review of **a strategy on ICT third-party risk**
  - maintenance and updating a **Register of Information on all contractual arrangements** for the use of ICT services provided by ICT third-party service providers;

- **adoption of Exit strategies and Transition Plans** for ICT services supporting critical or important functions (art. 28, 8 DORA Regulation).

  Exit plans shall be comprehensive, documented, sufficiently tested and reviewed periodically. Financial entities shall identify alternative solutions and develop transition plans […] to […] securely and integrally transfer [the contracted ICT services and the relevant data from the ICT third-party service provider] to alternative providers or reincorporate them in-house.

- regularly review of the risks identified in respect of outsourcing of critical or important functions;
- *in exercising access, inspection and audit rights over the ICT third-party service provider, financial entities shall on a risk-based approach pre-determine the frequency of audits and inspections and the areas to be audited […].*

- A thorough **pre-contracting analysis** (art.28, 4) should underpin and precede the formal conclusion of contractual arrangements to identify the likelihood for systemic risk to emerge, including by means of in-depth analyses of sub-outsourcing arrangements, notably when concluded with ICT third-party service providers established in a third country: "[…] *financial entities shall*:

  a assess whether the contractual arrangement covers a critical or important function;

  b assess if supervisory conditions for contracting are met;

  c identify and assess all relevant risks in relation to the contractual arrangement;

  d undertake all due diligence and ensure throughout the selection and assessment processes that the ICT third-party service provider is suitable;

  e identify and assess conflicts of interest that the contractual arrangement may cause".

  Preliminary assessment of ICT concentration risk (Art. 29, 1). Before concluding a contractual arrangement with an ICT third-party service provider, financial entities shall take into account (a) the ease of its replacement; or (b) the risks of having multiple contractual arrangements with the same ICT third-party service provider or with closely connected ICT third-party service providers.

  Preliminary assessment of sub-outsourcing arrangements (art.29, 2): "financial entities shall weigh benefits and risks that may arise in connection with such possible subcontracting, in particular in the case of an ICT sub-contractor established in a third-country. […] Financial entities shall assess whether and how potentially long or complex chains of sub-contracting may impact their ability to fully monitor the contracted functions".

- **Definition of contractual arrangements between the financial entity and ICT third-party service providers** (Art. 30 DORA Regulation).

  The full contract between a financial entity and a third-party ICT service provider shall be documented in one **written document**".

  The Regulation introduces **harmonisation on the key contractual elements** considered crucial to enable full monitoring by financial entities with a view to ensuring their digital resilience by relying on the stability and security of ICT services.

- The contractual arrangements on the use of ICT services of a third-party provider shall include at least the following elements:

  a a complete description of all functions and services to be provided by the ICT third-party service provider;

  b indication **whether sub-contracting of a critical or important function**, or material parts thereof, **is permitted** and, if so, the conditions applying to such sub-contracting;

  c indication of locations where the contracted or sub-contracted functions and services are to be provided and where data is to be processed, including the storage location;

  d iv. relevant provisions on accessibility, availability, integrity, security and protection of personal data;

  e in the case of ICT services supporting critical or important functions:

  - **full-service level descriptions** with precise quantitative and qualitative performance targets to allow an effective monitoring by the financial entity and enable appropriate corrective actions when agreed service levels are not met;
  - **notice periods and reporting obligations** of the ICT third-party service provider;

- requirements for the ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies;
- the right to monitor, on an ongoing basis, the ICT third-party service provider's performance;

f the obligation of the ICT third-party service provider to assist in the event of an ICT incident;

g rights of access, inspection and audit by the financial entity or an appointed third-party;

h the obligation of the ICT-third party service provider to fully cooperate with the competent authorities and resolution authorities of the financial entity;

i termination rights and related minimum notices period

j dedicated exit strategies with indication of a mandatory adequate transition period.

- Moreover, Dora Regulation promotes the **voluntary use of standard contractual clauses** developed by public authorities for specific services when financial entities and ICT third-party service providers negotiate contractual arrangements.

6. Information-sharing arrangements (Article 45)

To raise awareness on ICT risk, minimise its spread, support financial entities' defensive capabilities and threat detection techniques, the regulation allows financial entities to set-up arrangements to exchange amongst themselves cyber threat information and intelligence.

Oversight framework for critical ICT third-party service providers to financial entities

- The Regulation also requires critical ICT third-party service providers - large technology companies that supply many of the digital technology solutions used to support financial services by the financial sector - to be subject to a Union Oversight Framework (Articles 31 to 44).
- The ESAs, through the Joint Committee, shall designate ICT third-party service providers that are critical for financial entities.

  The European Commission will adopt a delegated act specifying qualitative and quantitative criteria to be used for designation of third-party ICT service providers as "critical" for ESA oversight.
- In order to ensure proper pan-European supervision of all technology service providers that play a key role in the functioning of the financial sector, one ESA is designated as a Lead Overseer for each critical third-party ICT service provider.
- Lead Overseers should enjoy the necessary powers to conduct investigations, onsite and offsite inspections at critical ICT third-party service providers, access all relevant premises and locations and obtain complete and updated information to enable them to acquire real insight into the type, dimension and impact of the ICT third-party risk posed to the financial entities and ultimately to the Union's financial system.
- In addition, **Lead Overseers should be able to submit recommendations on ICT risk matters** and suitable remedies, including opposing certain contractual arrangements ultimately affecting the stability of the financial entity or the financial system.
- To avoid duplications and overlaps, competent authorities should refrain from individually taking any measures aimed at monitoring the critical ICT third-party service provider's risks. Any such measures should be previously coordinated and agreed in in the context of the Oversight Framework.
- The Joint Committee of the ESAs ensures cross-sectoral coordination in relation to all maters on ICT risk, in accordance with its tasks on cybersecurity, supported by the relevant subcommittee (Oversight Forum) carrying out preparatory work for individual decisions and collective recommendations to CTPPs (Critical Third-Party Providers).
- This oversight framework should be without prejudice to Member States' competence to conduct own oversight missions in respect to ICT third-party service providers which are not critical under this Regulation but could be deemed important at national level.
- A regime of voluntary "opt-in" to the Oversight Framework is envisaged for ICT third-party service providers which are not automatically designated as critical by ESAs.
- ICT third-party service providers - already subject to oversight mechanism frameworks supporting the fulfilment of the tasks of the European System of Central Banks – are exempted.

How to be compliant with the DORA regulation

- Compliance with DORA's regulatory requirements is a complex process of mapping current structures and processes, planning decisions and implementing measures by the Board of Directors (and senior management) of a financial institution.
- **Mapping**. First, financial institutions should map out all current strategies, policies and processes for managing ICT-related risks, along with roles and responsibilities for all ICT-related functions and coordination structures within their organization.
- **The DORA framework**. DORA requirements should be properly classified and systematized by relevance and priority in order to have a clear picture of the overall measures, tools, and processes involved, as well as their interdependencies, necessary to establish a solid action plan for compliance.
- **GAP Analysis**. The management body of financial entities should task senior management to undertake a comprehensive GAP analysis between DORA requirements, on the one hand, and the ICT risk strategy and governance measures and tools already adopted and in place, on the other.

  GAP analysis should identify any deficiencies in professional skills and competences.
- **Bridging the DORA GAP**. Senior management of the financial institution, with the possible assistance of legal advisers and ICT risk management experts, should take into account the previous GAP analysis and develop an action plan proposing to the management body all structural and organisational measures necessary to ensure full compliance with the DORA framework.
- **Implementation of the Action Plan**. The management body should discuss and approval the action plan (with its timetable) to make the financial entity compliant with DORA requirements, giving due consideration to the application of the proportionality principle.
- **Monitoring and reporting on the implementation of the Action Plan**. It is important that the Board of Directors receive from the senior management responsible for the Action Plan detailed periodic reports on the status of DORA's implementation, as well as on any significant problems encountered and any organizational constraints or limitations to be overcome.

Bird & Bird has a comprehensive understanding of your business and uses experts from various disciplines and sectors to assist you with the legal and contractual aspects of implementing DORA requirements in accordance with your chosen ICT risk strategy.

Key contacts

Scott McInnes - Belgium

Partner

+3222826059
scott.mcinnes@twobirds.com

Ivan Sagál – Czech Republic & Slovakia

Partner

+420226030509
ivan.sagal@twobirds.com

Annette Printz Nielsen - Denmark

Partner

+4539141660
annette.nielsen@twobirds.com

Kristiina Lehvilä - Finland

Counsel

+420226030516
kristiina.lehvila@twobirds.com

Cathie-Rosalie Joly - France

Partner

+33142686742
cathie-rosalie.joly@twobirds.com

Johannes Wirtz, LL.M. - Germany

Partner

+4969742226000
johannes.wirtz@twobirds.com

Dr. Michael Jünemann - Germany

Partner

+4969742226000
michael.juenemann@twobirds.com

Konrad Siegler - Hungary

Of Counsel

+3613018916
konrad.siegler@twobirds.com

Giuseppe D'Agostino - Italy

Of Counsel

+390230356078
giuseppe.dagostino@twobirds.com

Stefano Febbi - Italy

Partner

+390230356030
stefano.febbi@twobirds.com

Slawomir Szepietowski - Poland

Partner

+48225837913
slawomir.szepietowski@twobirds.com

José Luis Lorente Howell - Spain

Partner

+34917906022
jose.luis.lorente.howell@twobirds.com

Hans Svensson - Sweden

Partner

+46850632048
hans.svensson@twobirds.com

Gidget Brugman – The Netherlands

Partner

+31703538925
gidget.brugman@twobirds.com