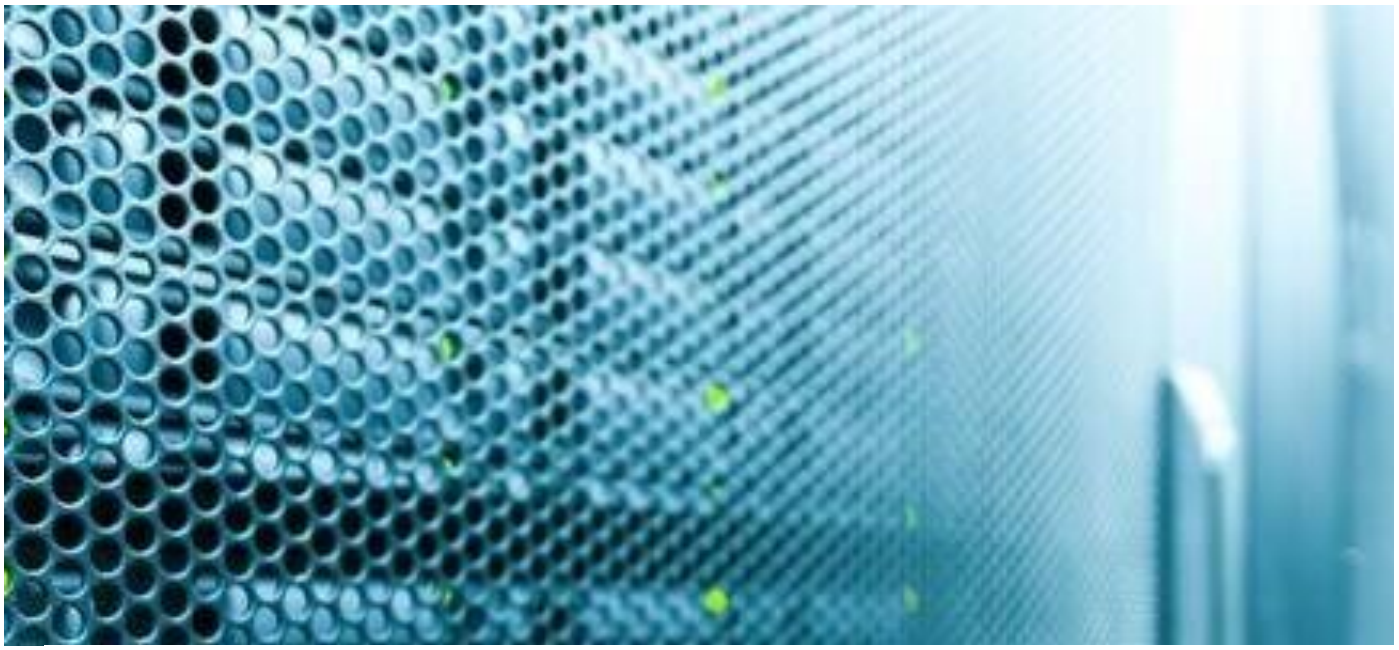
EVERSHEDS
SUTHERLAND



The EU's Digital Operational Resilience Act (DORA)

Unlocking European Cybersecurity Regulation

July 23, 2024

Global

The EU's Digital Operational Resilience Act (DORA) applies from January 2025, harmonising digital resilience and cybersecurity requirements across the financial sector. Financial entities now face a tight deadline to review ICT risk management, third-party risk, and update new and existing agreements with ICT service providers.

Executive summary

With the January 17, 2025 deadline for application of the EU's Digital Operational Resilience Act ("DORA") rapidly approaching, financial entities and their ICT service providers face a crucial period of preparation. As these entities navigate the complexities of DORA—addressing ICT risk management, reporting mechanisms, and third-party risk— they encounter significant challenges due to the uncertainties surrounding this new regulation. While DORA demands substantial effort and adaptation by the financial entity and its management body, it also offers an opportunity to strengthen resilience, build customer trust, and gain a competitive advantage in today's market. This article provides an overview and insights into the challenges of the EU's latest cybersecurity regulation.

EVERSHEDS
SUTHERLAND

Background

The European Union has introduced several new regulations and directives to harmonise operational resilience requirements across its member states. DORA was introduced as a sector-specific legal act for the financial sector and takes precedence over the more general network and information security directive (“NIS2”).

DORA’s goal is to ensure the uninterrupted provision of financial services to the end customer, even during serious disruptions. The regulation aims to achieve this by mandating ICT-risk management as part of financial entities’ governance requirements, reporting requirements, digital operational resilience testing, information sharing, and comprehensive management of ICT third- party risk.

Financial entities are now assessing which DORA obligations apply to them, how they may benefit from DORA’s principle of proportionality, and which aspects may need to be considered at the group level.

The regulation also introduces a new oversight framework for specific ICT services to financial entities which are considered systemically important.

1. Challenging timeline

Financial entities in scope (see 2. below) are currently navigating regulators’ strict expectations regarding the implementation timeline. Although DORA takes effect in January 2025, many of the regulation’s requirements are still being detailed by European Supervisory Authority (“ESA”) guidance. The ESAs, which are the EBA, EIOPA, and ESMA, have drafted Regulatory Technical Standards (“RTS”) and Implementing Technical Standards (“ITS”) essential for implementing DORA requirements. During this drafting process, financial entities have been given the opportunity to provide feedback in open consultations. However, this drafting is taking place just months before DORA requirements take effect. This leaves financial entities and their ICT service providers with a tight timeline to implement requirements and update their contractual obligations. E.g., when reviewing the ESA requirements for subcontracting (see 3.4).

DORA timeline

- **16 January 2023: DORA regulation comes into force**
- **13 March 2024: Batch 1 RTS adopted by EU Commission**
- **17 July 2024: Batch 1 RTS and ITS submitted to EU Commission**
- **[delayed]: ESAs finalize subcontracting RTS**
- **17 January 2025: DORA applies (including pre-existing agreements)**

2. Entities in scope of DORA

The DORA regulation applies to a range of financial institutions, including the insurance sector. The Financial Entities ("FE") in scope of DORA are:

- **Credit, payment, and electronic money institutions**
- **Investment firms**
- **Crypto asset service providers**
- **Central securities depositories**
- **Trading venues**
- **Managers of alternative investment funds**
- **Data reporting service providers**
- **Insurance and reinsurance undertakings**
- **Insurance intermediaries**
- **Occupational retirement provision**
- **Credit rating agencies**
- **Crowdfunding service providers**

For a full list please see Article 2 (1) of DORA. DORA equally imposes direct and indirect obligations for ICT third-party service providers (see 3.3 and 5.).

3. Roadmap to resilience

Under DORA, the management body of the FE is required to define, approve, oversee and take responsibility for the implementation of the ICT risk management. This includes appropriate planning for the implementation of DORA itself as part of the resilience strategy and the FE's governance. FEs are now assessing requirements on a case-by-case basis, where obligations under DORA may vary depending on the type of FE in question. E.g., if the obligation to perform advanced testing applies, or not (see 3.5 below).

FEs must ensure that their management body fully understands ICT risks, as both the FE and its management body may face administrative penalties and remedial measures under national law (Article 50 (5) DORA). To support stakeholders in fulfilling their responsibilities, FEs should develop a detailed implementation plan, covering key areas including, but not limited to, the following core issues.

3.1 ICT risk management framework

DORA mandates that FEs implement an internal governance and control framework ("ICT Risk Management Framework"), which integrates multiple resilience aspects. This framework is central to DORA and must be documented and audited regularly. FEs are required to review and determine to what degree they must update their policies, ICT systems, protocols and tools so that they may be sufficiently reliable to manage ICT risks.

3.2 Incident management

The DORA regulation outlines requirements for responses and recovery from incidents, including effective Business Continuity Management ("BCM"). In preparation, FEs should review their internal processes and identify the new reporting obligations. This particularly includes identifying which scenarios must be monitored, how the DORA reporting may interact with other existing reporting obligations and what effective incident management may look like. Updating incident management procedures can pose a challenge, as this is also subject to the RTS draft guidance. The ESAs have so far suggested that reports must be submitted to the supervisory authority within 4 hours, but no later than 24 hours for an initial report. This must be followed by an intermediate report within 72 hours and a final report within 1 month. Additionally, FEs will also need to review which form requirements apply to them and identify stakeholders, such as customers, who may need to be notified or provided with appropriate support.

3.3 ICT service providers

Since DORA's core objective is to mitigate risks from ICT incidents, ICT services to an FE are directly involved in implementing DORA obligations. Many FEs have recently completed extensive projects related to outsourcing following the EBA guidelines. However, ICT Services in scope of DORA extend to ICT providers beyond the narrow lens of material outsourcing.

ICT Services according to DORA include all *"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 technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone"* (Article 3 (21) DORA).

FEs now face the challenge of classifying which of their service providers are actually in scope of the ICT Service definition and which ICT Services support their critical or important functions. The resulting list of ICT Services must then be documented in a detailed register, subject to specific requirements and provided to the supervisory authorities by the time DORA applies.

It's worth noting that despite the terminological overlap, the ICT service provider classified as supporting a critical or important function is not to be confused with the critical ICT third-party service provider. Under DORA, critical ICT service providers are subject to a distinct designation process and DORA's oversight framework (see 5.).

3.4 Contractual uplift

Depending on the type of ICT Service, DORA also requires specific contractual requirements (e.g., Article 30 DORA). These apply to the direct contractual relationship between the FE and its ICT Service provider, including audit or termination rights. Entities in scope must therefore review the respective agreements and addenda by the time DORA applies.

In a strict interpretation of the regulation, supervisory authorities, such as the German BaFin, have indicated that the regulator expects both new and existing agreements to be DORA compliant by January 17, 2025. This presents significant implementation challenges for FEs, especially since the ESA RTS on contractual requirements for subcontractors are still in draft form. Whilst the ESAs have finalised the second batch of RTS and ITS guidance and submitted these drafts to the EU Commission on July 17, 2024, the RTS on subcontracting are delayed and will be published in the weeks after the deadline, according to ESA sources.

3.5 Testing resilience

A key aspect for FEs and their ICT Service providers is the requirement to regularly assess and test resilience, including ICT tools and systems, to identify weaknesses and vulnerabilities. Certain FEs will need to conduct advanced testing in the form of Threat-Led Penetration Testing ("TLPT"). This advanced testing framework is based on the European TIBER-EU testing framework and is also specified by ESA Guidance.

FEs must closely assess the scope of this obligation, as the TLPT process requires significant time and resources. E.g., where FEs must provide access and facilitate the simulation of an attack on live systems. Additionally, legal considerations are required, where conflicting interests, such as confidentiality or data protection may be at stake. It does not come as a surprise that engaging in early discussions about detailed options will be beneficial to FEs and ICT Service providers alike. Both the entities in scope and their ICT Services are now assessing potential paths to comply with the extensive requirements and to accommodate varying interests, e.g., when implementing pooled testing.

4. Proportionality principle

DORA's principle of proportionality (Article 4 DORA) is fundamental to implementing DORA and allows for certain exceptions that simplify DORA obligations. For instance, FEs must implement an ICT risk management in light of their *"size and overall risk profile, and the nature, scale and complexity of their services, activities and operations"*.

FEs must now assess the extent to which they may benefit from a proportionate approach to their ICT-risk management process, testing and third-party risk management in their operations.

5. The new oversight framework

To improve digital resilience throughout the sector, DORA introduces a new oversight framework for ICT service providers which are critical to FEs (Article 31 DORA). These Critical ICT Third-Party Service Providers ("CTPP") will need to undergo specific assessments and be subject to recommendations from one of the ESAs acting as lead overseer. To determine which ICT Services may be critical, the ESAs will collect and assess the registers submitted by the FEs. The ESAs will map the ICT Services offered throughout the sector to determine which providers have e.g., a systemic impact on the provision of financial services (e.g., 10% market share among FEs). The designation of CTPPs will therefore only take place after DORA applies to the FEs. Additionally, certain ICT Services may opt-in to the oversight framework on a voluntary basis.

Next steps

FEs and their ICT Service providers are now facing a tight implementation schedule leading up to January 17, 2025. Our experienced team of international experts is here to guide you through the required DORA implementation steps and lay out a roadmap for you and your team. E.g., where helpful to you, support you with your internal gap analysis, the resulting action items or training sessions, including practical boardroom briefings covering DORA obligations and C-suite responsibilities.

To ensure our service excellence to you, our Eversheds Sutherland team works with a full range of experts across EU member states and with cybersecurity technical expert partner firms at your disposal.

For further details, please reach out to your contacts below.

EVERSHEDS
SUTHERLAND

The materials on the Eversheds Sutherland website are for general information purposes only and do not constitute legal advice. While reasonable care is taken to ensure accuracy, the materials may not reflect the most current legal developments. Eversheds Sutherland disclaims liability for actions taken based on the materials. Always consult a qualified lawyer for specific legal matters. To view the full disclaimer, see our Terms and Conditions or Disclaimer section in the footer.

Services

- Cybersecurity →
- Data Privacy, Security and Technology →

Industries

- Financial Services →

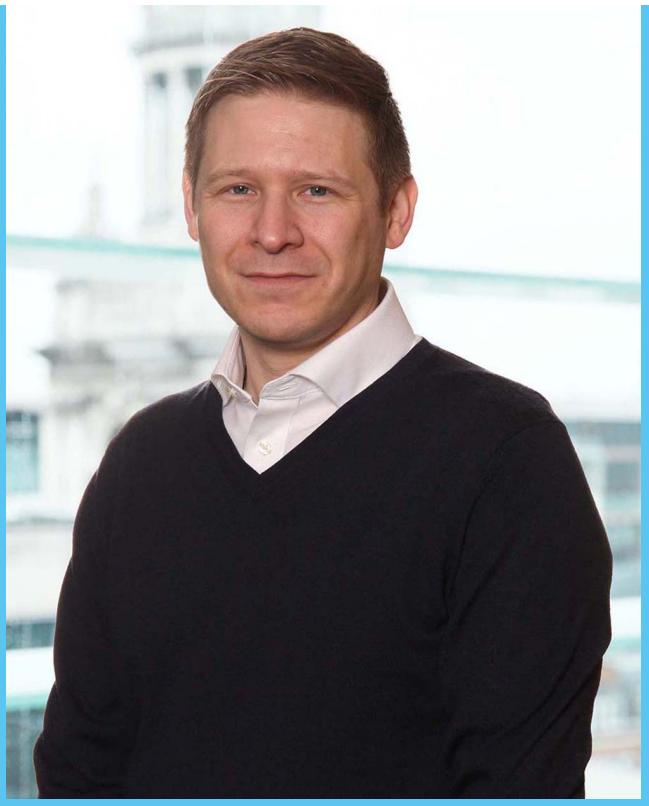
Key contacts

EVERSHEDS
SUTHERLAND

Simon Gamlin

Partner

United Kingdom



Simon Lightman

Partner

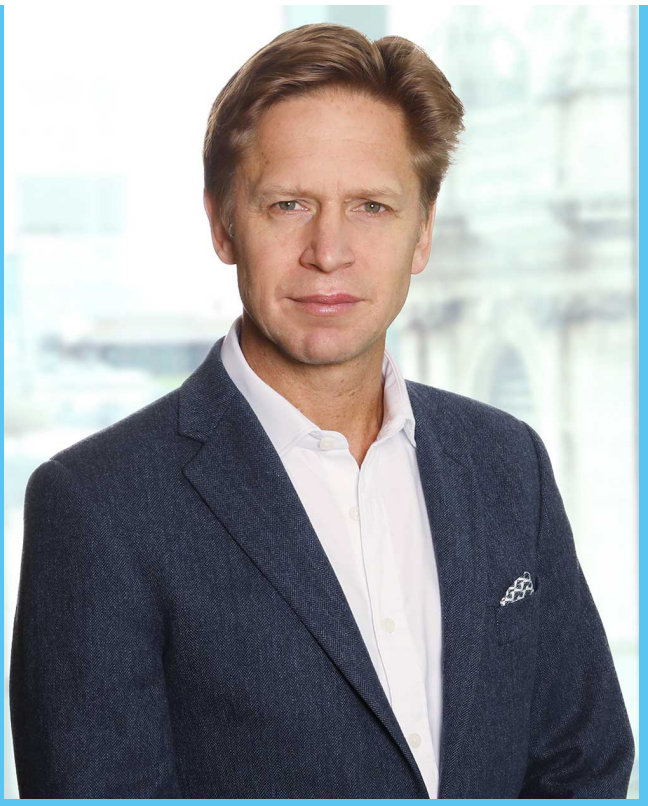
United Kingdom

EVERSHEDS
SUTHERLAND

Joanne Veitch

Partner

United Kingdom



Craig Rogers

Partner

United Kingdom

EVERSHEDS
SUTHERLAND

Nils Müller

Partner

Munich, Germany

Stephanie Shepherd

Senior Associate

United Kingdom

EVERSHEDS
SUTHERLAND

Isabella Norbu

Associate

Munich, Germany