# Briefing Note:
# Digital Operational Resilience Act (DORA)
# (Regulation (EU) 2022/2554)

## Overview

- This Briefing Note aims to provide **UK digital businesses** with a summary of **possible impacts** on their activities due to the implementation of **DORA** by **EU *financial entities*** with which they do business.

- DORA is an attempt by the relevant EU authorities to **harmonize** information and communication technology (**ICT**) **risk-management requirements** at EU level in respect of ***financial entities***.

- The EU notes that while ICT keeps our economies running in key sectors, not least the financial sector, **digitalization and interconnectedness** also **increase ICT risk**, rendering society as a whole and the financial sector, in particular, more vulnerable to cyber threats and disruption.

- DORA specifies the authorities' **requirements in detailed lists** – this is *not* a principles-based piece of legislation – aimed at boosting **operational resilience and security capabilities** of firms falling within its scope.

- This is an EU regulation, but **UK digital businesses providing ICT services to EU firms** from the UK or from any other third country, may find they are required to accept **changes in their contractual relationships** with in-scope customers, sub-contractors or affiliates, and **consequent changes in their operational standards**.

- Moreover, their **EU subsidiaries may themselves be *financial entities* caught directly by DORA***.

- Full implementation is due on **17 January 2025**.

## Who is in-scope - who is a "Financial Entity"?

### Within the EU

**Banks and payment institutions**
**Account information service providers**
**Electronic money institutions**
**Investment firms**
**Crypto-asset service providers**
**Central securities depositories and central counterparties**
**Trading venues and trade repositories**
**Managers of alternative investment funds and UCITS management companies**
**Data reporting service providers**
**Insurance and reinsurance undertakings**
**Occupational pension providers**
**Credit rating agencies**
**Administrators of critical benchmarks**
**Crowdfunding service providers**
**Securitisation repositories**
**ICT third-party service providers***

**All of the above are defined as "financial entities"**

## What is meant by "digital operational resilience"?

For the purposes of DORA, the term is defined as the ability of a financial entity to **build, maintain and keep under review, its operational integrity and reliability in respect of the full range of ICT-related capabilities needed to address the security of the *network and information systems*** used by the financial entity to support the continued provision of financial services. This includes the quality of and any disruption to those services.

The term encompasses ***ICT services*** **provided by third party service providers** as well as intra-group service providers.

## What are "network and information systems"?

- Electronic communications networks
- A device or group of interconnected devices programmed to carry out automatic processing of digital data
- Digital data stored, processed, retrieved or transmitted by any of the above for the purposes of their operation, protection and maintenance.

DORA references *ICT assets* in terms of software or hardware assets in the network and information systems used by a financial entity.

Additionally, an *information asset* is defined as a collection of information, either tangible or intangible, that is worth protecting.

## What is an ICT service?

ICT service is **defined as a digital and data service provided through ICT systems to internal or external users**; the term includes hardware as a service and hardware services including the provision of technical support via software or firmware updates by the hardware provider. Analogue telephone services are excluded.

## What constitutes ICT risk?

ICT risk is defined as any **reasonably identifiable** circumstances, which, if they should materialize, might **compromise the security** of:

- the network and information systems
- any technology dependent tool or process
- operations and processes
- the provision of services

by producing adverse effects in the digital or physical environment.

## What does DORA require from in-scope firms?

As mentioned above, the list of requirements is comprehensive and is set out in both DORA itself and in secondary legislation. As an overarching principle, DORA makes it clear that the **management body of the financial entity bears ultimate responsibility for managing ICT risk**. This includes the relevant body "keeping actively up to date with sufficient knowledge and skills to understand and assess ICT risk"

Broadly, requirements applicable to financial entities involve robust structures to be in place in relation to:

- **ICT risk management**
- **Reporting major ICT related incidents and notifying significant cyber threats to the competent authorities**
- **Reporting major operational or security payment related incidents to the competent authorities**

- **Digital operational resilience testing**
- **Information and intelligence sharing in relation to cyber threats and vulnerabilities**
- **Measures for the sound management of ICT third-party risk**

## What does this mean for ICT service providers?

It is in the nature of the services covered by DORA – and the risks it seeks to mitigate – that in-scope firms can only **assure their own compliance by seeking the compliance of their ICT service providers and partners.** Thus, detailed requirements are stipulated in relation to contractual arrangements between ICT third-party service providers and financial entities, including before the contract is entered into.

As part of the financial entity's ICT risk management framework, it must establish a policy specifying contractual arrangements, including risk assessment, due diligence and the requirement for certain contractual clauses setting out mutual obligations.

### Key Pre-contract and Contractual Requirements

- **Detailed due diligence of prospective ICT third-party service providers.**
- **Can the provider demonstrate that it has the desired business reputation, sufficient abilities and expertise?**
- **Does the provider have sufficient financial, human and technical resources, information security standards, appropriate organisational structures, risk management and internal controls?**
- **Is the provider in possession of the relevant authorisations or registrations?**
- **Financial entities are required to specify the right to access information, carry out inspections and audits and perform tests on ICT. The methods to be used by the financial entity are set out in the regulations.**
- **The contract must specify the measures and key indicators to monitor, on an ongoing basis, the performance of the service provider and specify measures that will apply when service level agreements are not met**
- **An exit plan for the financial entity needs to be documented, reviewed and tested.**

6th September 2024

This briefing note is intended for general information purposes only and as a high-level overview of the relevant legislation.

For further information contact:

stephen.sanders@sandersconsultinglimited.com

penny.sanders@sandersconsultinglimited.com

On behalf of Sanders Consulting Limited.