UK COMPLIANCE GUIDE FOR IT

DORA (EU Digital Operational Resilience Act)

Last reviewed: November 2026 · Current version: wise-its.uk/compliance/dora/

Please read first. This guide summarises; it is not legal advice. Rules change: check the current version at **wise-its.uk/compliance/dora/** and the official sources listed, and ask your legal or compliance adviser to confirm what applies to you.

In brief

The EU Digital Operational Resilience Act (Regulation (EU) 2022/2554) has applied to EU financial entities since 17 January 2025. It sets detailed requirements for how banks, insurers, investment firms, payment firms and others manage technology risk. UK businesses are not regulated by it directly unless they are EU entities, but those that supply technology services to EU financial firms will see its requirements written into their contracts.

Who it applies to

- EU financial entities, including banks, insurers, investment firms, payment and e-money institutions and crypto-asset service providers
- ICT third-party service providers to those entities, through contractual requirements
- Critical ICT third-party providers designated by the European Supervisory Authorities, which face direct oversight

What it requires

ICT risk management
A documented framework for identifying, protecting against, detecting, responding to and recovering from ICT risk.

Incident reporting
Classification of ICT-related incidents and reporting of major incidents to regulators within set timescales.

Resilience testing
Regular testing of systems, with advanced threat-led penetration testing for the most significant firms.

Third-party risk
A register of all ICT third-party arrangements and contracts that contain specific provisions.

Information sharing
Voluntary sharing of cyber threat information between financial entities.

What it means for your IT

Contract terms
Expect clauses on service descriptions, data locations, security, incident assistance, cooperation with regulators, termination rights and exit strategies.

Incident notification
Agreed timescales for telling the client about incidents affecting their services, so they can meet their own reporting obligations.

Audit and testing
Rights for the client and its regulator to audit, and participation in the client's resilience testing where the service supports a critical function.

Register information
Clients may ask for identifiers such as a Legal Entity Identifier, details of subcontractors and where data is processed.

Exit plans
A documented, workable plan for transferring the service to another provider.

Evidence to keep

- Security controls and test results
- Incident notification procedures and timescales
- A list of subcontractors and data processing locations
- Business continuity arrangements for the service
- An exit plan

Common gaps we find

- Standard contracts with no incident notification timescale
- Subcontractors and data locations not documented
- No exit plan beyond "we will cooperate"
- Assuming DORA is irrelevant because the business is UK-based

Key dates

When	What
17 January 2025	DORA began to apply to EU financial entities.
Ongoing	Supervisory authorities designate critical ICT third-party providers for direct oversight.

Common questions

We are UK-based. Why does DORA matter?
If your customers include EU financial firms, they must apply DORA's requirements to their technology suppliers, so the requirements reach you through contracts.

Is there a UK equivalent?
The UK has its own operational resilience rules for financial firms and a separate regime for critical third parties to the financial sector. See FCA operational resilience.

What is a Legal Entity Identifier?
A global reference code for legal entities. EU financial firms use it to identify suppliers in their register of ICT arrangements.

Official sources

- EUR-Lex: Regulation (EU) 2022/2554 (DORA): https://eur-lex.europa.eu/eli/reg/2022/2554/oj

- European Banking Authority: DORA: https://www.eba.europa.eu/regulation-and-policy/operational-resilience

Not sure where you stand?

Take the free cyber maturity self-assessment at **wise-its.uk/resources/cyber-maturity-model**, or ask us for an evidence review at **wise-its.uk/contact**. Wise IT Solutions provides the technical controls, the evidence and the advice; compliance decisions stay with you.

© Wise IT Solutions. Free to share in full with this notice. Last reviewed November 2026.