SmartSuite

Framework / Operational Resilience / Other

# DORA (Regulation (EU) 2022/2554)

DORA (Regulation (EU) 2022/2554) requires EU financial entities to manage ICT risk, report major incidents, test resilience and control ICT third-party risk, applying from January 17, 2025.




## What it is

The Digital Operational Resilience Act (DORA, Regulation (EU) 2022/2554) requires EU financial entities to manage ICT risk under a framework approved by their management body, report major ICT-related incidents to their supervisor, test their resilience, and control the risks of ICT third-party service providers through contracts and a register of information. It has applied since January 17, 2025.

The European Parliament and the Council adopted it on December 14, 2022. It applies to banks, payment and e-money institutions, investment firms, crypto-asset service providers, central securities depositories, central counterparties, trading venues, trade repositories, fund managers, insurers, insurance intermediaries, pension institutions, credit rating agencies and other listed financial entities (Article 2), and it sets an oversight regime for critical ICT third-party service providers run by the European Supervisory Authorities (ESAs).

## At a glance

PUBLISHER
European Parliament and Council of the European Union

TYPE
Regulation

VERSION
Regulation (EU) 2022/2554

EFFECTIVE
January 17, 2025 (entered into force January 16, 2023)

DOMAIN
Operational Resilience

FAMILY
Other

REGION
European Union

INDUSTRY
Financial Services

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554&from=EN

## Why it matters

- **Management body accountability** The management body defines, approves and oversees the ICT risk framework and bears ultimate responsibility for ICT risk (Article 5(2)).
- **One incident reporting regime** Major ICT-related incidents are reported to the competent authority as an initial notification, intermediate report and final report using common templates (Articles 19 and 20).
- **Tested resilience** Entities test ICT tools regularly, and those identified by authorities carry out threat-led penetration tests at least every three years (Articles 24 to 26).
- **Third-party risk is contractual** Financial entities keep a register of information on all ICT contracts and include key provisions in every contract (Articles 28 and 30).


Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

## How SmartSuite supports EU DORA

### ICT Risk Framework and Governance

Record the management body approvals, the framework, roles and review dates (Articles 5 and 6).

### Asset and Dependency Register

Map critical or important functions to ICT assets, providers and dependencies (Article 8).

### Incident Classification and Reporting

Classify incidents, track the initial notification, intermediate and final reports and the supervisory templates (Articles 17 to 20).

### Resilience Testing Program

Plan tests, threat-led penetration test cycles, findings and remediation with owners (Articles 24 to 26).

### Register of Information

Maintain contracts with ICT providers, their functions, locations and critical or important flags for the yearly report (Article 28(3)).

### Contract Terms and Concentration Review

Check each contract against Article 30 provisions and record concentration risk assessments and exit plans (Articles 29 and 30).

## Common framework mappings

EBA GL/2019/04 | ISO 22301 | ISO 27001:2022 | NIS2 (EU 2022/2555) | NIST CSF 2.0 | NIST 800-53 Rev.5 | SWIFT CSCF | EBA GL/2019/02

## Official resources

### EU Digital Operational Resilience Act (DORA)

Provides the full legal text of the Digital Operational Resilience Act for financial sectors.

eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554&from=EN

### European Commission DORA Guidelines

Outlines official guidance on implementing the Digital Operational Resilience Act for financial entities.

eiopa.europa.eu/digital-operational-resilience-act-dora_en

### European Union Financial Resilience Framework

Describes the regulatory framework enhancing digital resilience of financial institutions in the EU.

eiopa.europa.eu/digital-operational-resilience-act-dora_en

## Frequently asked questions

### Who must comply with DORA?

The financial entities in Article 2(1): credit institutions, payment and e-money institutions, investment firms, crypto-asset service providers, central securities depositories and counterparties, trading venues, fund managers, insurers and intermediaries, pension institutions, credit rating agencies and others. ICT third-party service providers are covered through contracts and, if critical, ESA oversight.

### When does DORA apply?

DORA entered into force on January 16, 2023 and has applied since January 17, 2025 (Article 64). It is a regulation, so it applies directly in every Member State.

### What must entities report to their supervisor?

Major ICT-related incidents, through an initial notification, an intermediate report and a final report using common templates, within time limits set under Article 20 (Article 19). Significant cyber threats can be notified voluntarily.


Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

### What is the register of information?

A register, kept at entity and consolidated levels, of all contractual arrangements for ICT services from third-party providers, separating those that support critical or important functions. Entities report on it to competent authorities at least yearly and give the full register on request (Article 28(3)).

### What are threat-led penetration tests?

Advanced tests (TLPT) on live production systems that support critical or important functions, carried out at least every three years by entities identified by their competent authority (Article 26). Testers must meet the requirements of Article 27.

License included / downloadable: Yes The Regulation is EU law published in the Official Journal and is included with the platform for reference.

Full framework page and mappings: smartsuite.com/frameworks/eu-dora-digital-operational-resilience-act


Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.