

DORA (Regulation (EU) 2022/2554)

DORA is an EU regulation requiring financial firms to manage ICT risks, report incidents, test security, and oversee third-party providers.



What it is

The EU Digital Operational Resilience Act (DORA) is a regulatory framework that helps financial organizations enhance their cybersecurity, manage ICT-related risks, and ensure operational resilience across the European Union. DORA aims to strengthen the digital defenses of the financial sector and protect against cyber threats, system failures, and operational disruptions.

Published by the European Union, DORA applies to a broad spectrum of financial entities, including banks, investment firms, payment service providers, and ICT third-party service providers. The regulation mandates comprehensive requirements around ICT risk management, incident reporting, security testing, third-party risk management, and information sharing, creating a unified approach to digital operational resilience.

At a glance

PUBLISHER European Union	TYPE Regulation	VERSION Regulation (EU) 2022/2554
EFFECTIVE January 17, 2025	DOMAIN Operational Resilience	FAMILY Other
REGION European Union	INDUSTRY Financial Services	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY Very High		

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

Why it matters

- Strengthen digital risk governance** Establish clear processes and oversight for identifying, managing, and mitigating technology and cybersecurity risks in financial operations.
- Enhance regulatory alignment** Support consistent compliance with EU-wide regulations, simplifying ongoing reporting obligations and reducing the complexity of managing multiple regimes.
- Promote operational resilience** Enable organizations to maintain essential services during cyberattacks or IT failures, minimizing business interruptions and client impact.
- Improve incident response readiness** Mandate robust planning and testing for detecting, managing, and recovering from cybersecurity incidents and technology outages.

How SmartSuite supports EU DORA

ICT Asset and Service Inventory

Catalog ICT assets, critical services, and dependencies with clear traceability.

ICT Risk Management Controls

Track risk controls, owners, and evidence across ICT governance and operations.

Incident Reporting Workflows

Manage classification, escalation, and reporting steps with decision documentation.

Resilience Testing Program

Schedule testing, capture results, and track remediation for resilience gaps.

Third-Party Risk and Exit Planning

Oversee critical providers with contracts, monitoring, and documented exit plans.

DORA Readiness Reporting

Report program status, open gaps, and evidence coverage across requirements.

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

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

What is DORA used for?

DORA is designed to strengthen the digital operational resilience of financial institutions in the European Union by ensuring robust management of ICT-related risks, incident response, and operational continuity. It establishes mandatory requirements for financial organizations to effectively prevent, detect, and respond to cyber threats and ICT disruptions.

Is DORA mandatory for financial institutions?

Yes, compliance with DORA is mandatory for a wide range of EU-based financial entities, including banks, investment firms, payment service providers, and critical ICT third-party service providers. Organizations are required to demonstrate ongoing adherence to the regulation's provisions and are subject to regulatory oversight.

What organizations or activities fall within the scope of DORA?

DORA applies to nearly all financial entities operating within the EU, such as banks, insurance companies, investment firms, payment processors, and ICT third-party service providers. The regulation covers ICT risk management, service continuity, incident reporting, and third-party provider oversight, regardless of an organization's size.

What are the key requirements or controls specified by DORA?

DORA introduces requirements in five main domains: ICT risk management, incident reporting, digital operational resilience testing, management of ICT third-party risks, and governance arrangements. Organizations must establish risk assessment processes, maintain incident logs, test resilience through regular exercises, and monitor vendor security controls.

How should organizations implement DORA requirements?

Organizations should integrate DORA's requirements into existing risk management and compliance frameworks by mapping regulatory obligations to specific security controls, updating governance policies, conducting regular ICT risk assessments, and developing robust incident response plans. Continuous control monitoring, documented testing, and clear reporting processes are essential for compliance.

How does DORA relate to other frameworks like ISO 27001 or NIS Directive?

DORA is complementary to standards such as ISO 27001 and the NIS Directive, but it is tailored specifically for the financial sector and focuses on operational resilience in addition to information security. Entities can leverage existing controls from other frameworks, but must ensure that all DORA-specific requirements are fully addressed.

What are the ongoing compliance obligations under DORA?

Ongoing compliance with DORA requires continuous risk monitoring, regular testing of operational resilience, timely incident reporting, periodic review of ICT third-party relationships, and documentation of governance actions. Organizations should maintain updated records and be prepared for regulatory audits or supervisory reviews.

How would SmartSuite support EU DORA (Digital Operational Resilience Act)?

SmartSuite can help organizations manage DORA compliance by centralizing risk tracking, aligning control management with regulatory requirements, and facilitating evidence collection through a centralized repository. The platform supports audit readiness by organizing compliance artifacts, automates monitoring and reporting, and streamlines remediation activities to ensure effective oversight and regulatory reporting.

License included / downloadable: Yes The Digital Operational Resilience Act is European Union legislation and is publicly available through official EU regulatory publications.

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