CYBERSECURITY 101 · eBuilder Security

# DORA

The EU rulebook that makes banks, insurers and other financial firms prove they can keep running through any technology failure.

## WHAT IT IS

DORA, the Digital Operational Resilience Act, is an EU law requiring financial firms to withstand, respond to and recover from every kind of ICT disruption. It has applied across the EU since 17 January 2025 and sets one binding standard for ICT risk in the financial sector.

## WHY IT MATTERS

**19**

critical ICT suppliers placed under direct EU oversight in the first designation

ESAs, 18 November 2025

**4 hours**

the deadline to notify a major ICT incident after classifying it

DORA Article 19, RTS 2025/301

**8.5 million**

Windows devices crashed by one supplier's faulty update in July 2024

Microsoft, 2024

## WHAT HAPPENED

In January 2023 ransomware attributed to the LockBit group hit ION Cleared Derivatives, whose software runs derivatives trading for banks and brokers. At least 42 clients had to process trades by hand, according to Bloomberg, and the Futures Industry Association coordinated the response. One supplier's outage rippled across the market, the exact risk DORA's third-party rules address.

## RED FLAGS TO WATCH FOR

### Signs your firm is not yet DORA ready

- No single register of your ICT third-party contracts
- Critical supplier contracts with no audit rights or exit plan
- No rehearsed way to classify and report an incident inside four hours
- Resilience testing that never touches your most critical systems
- ICT risk treated as an IT topic the board never sees

> THE ONE RULE THAT STOPS IT
>
> **Know exactly where you depend on a single technology supplier, and hold a tested plan for the day it fails.**

## THEN BUILD THE HABIT AROUND IT

- Keep the register of information current, not a once-a-year scramble

- Rehearse the four-hour and 72-hour reporting clocks
- Test the systems behind your critical functions, including threat-led testing where it applies

## MYTHS AND FACTS

MYTH

DORA is only about cyberattacks.

FACT

It covers every ICT disruption, including a faulty update or a failed migration.

MYTH

Outsourcing IT moves the DORA risk to the provider.

FACT

The financial firm stays responsible for its third-party risk.

MYTH

DORA compliance is the IT department's job.

FACT

Article 5 makes the board accountable, with personal liability for directors.

### THE LEGAL DUTY

In Sweden, Finansinspektionen supervises DORA and receives incident reports. For financial entities DORA takes precedence over NIS2, and national rules allow fines of up to 10 percent of turnover. Directors are personally accountable under Article 5.

---

## GET HELP

**Talk to eBuilder Security about mapping your DORA obligations.**

Read the Full Article →