REGULATION DORA

DORA in 5 minutes

The EU Digital Operational Resilience Act, on one page: what it is, who it covers, what it requires.

Updated August 2026 · share freely within your organisation

WHAT IT IS

Regulation (EU) 2022/2554 sets digital operational resilience rules for the EU financial sector. It has applied since **17 January 2025**, directly in every Member State, with no national transposition. It consolidates ICT risk, incident, testing and third-party requirements into one rulebook, detailed by RTS and ITS technical standards.

THE FIVE PILLARS

1 **ICT risk management** (Art. 5–16)
Governance, protection, detection, response and recovery. The management body owns the framework.

2 **ICT incident management and reporting** (Art. 17–23)
Classify every ICT-related incident; report major ones: initial notification within 4 hours of classification (at latest 24 hours after detection), intermediate report at 72 hours, final report within one month.

3 **Digital operational resilience testing** (Art. 24–27)
A testing programme for all entities; threat-led penetration testing (TLPT) at least every 3 years for entities designated by their authority, aligned with TIBER-EU.

4 **ICT third-party risk** (Art. 28–30, oversight Art. 31–44)
Mandatory contractual provisions, concentration risk, and a Register of Information kept available to the competent authority.

5 **Information sharing** (Art. 45)
Voluntary exchange of cyber threat information and intelligence between financial entities.

WHO IS IN SCOPE

21 categories of financial entities (Art. 2): credit institutions, payment and e-money institutions, investment firms, insurance and reinsurance undertakings, crypto-asset service providers, central counterparties, trading venues and more.

ICT third-party service providers are **not directly subject**: DORA reaches them through mandatory contract provisions (Art. 30). Providers designated as critical (CTPPs) by the European Supervisory Authorities come under direct Union oversight (Art. 31).

PENALTIES, WITHOUT THE MYTH

DORA sets **no EU-wide fine cap** for financial entities. Art. 50 leaves administrative penalties to national law, so ceilings differ by Member State. The widely repeated «2% of worldwide turnover» is not in the regulation.

The only turnover figure DORA itself sets: periodic penalty payments of **1% of average daily worldwide turnover**, for designated CTPPs only (Art. 35(8)). Member States may also provide criminal penalties (Art. 52).

WHERE TO START

1. Map your **critical or important functions** and the ICT assets and providers behind them.
2. Dry-run one incident through your **classification criteria** and the 4h/24h, 72h and one-month reporting clocks.
3. Complete your **Register of Information** and re-paper ICT contracts against Art. 30.

Free tools, the full RTS/ITS library and an interactive gap analysis: **www.regulation-dora.eu**