DORA · INCIDENT REPORTING AND RESILIENCE

DORA: Report incidents. Manage resilience.

A practical two-page guide for financial entities: confirm scope, connect the main work areas and prepare reporting for major ICT-related incidents.

DORA has applied since 17 January 2025 - but not to every business.

Check the specific legal entity against Article 2, including exclusions and simplified requirements. A customer contract does not automatically make an ICT provider a financial entity under DORA; contractual duties and the oversight framework for critical ICT third-party providers may create additional obligations.

Five connected work areas

ICT risk management

Organise accountability, inventories, protection, detection, response and recovery.

Incidents

Record, classify and escalate incidents internally; report major cases.

Resilience testing

Maintain a proportionate testing programme that includes critical functions and dependencies.

ICT third parties

Manage registers, contracts, concentration risks, monitoring and exit options.

Learning and sharing

Use incident lessons; information on cyber threats may be shared.

Reporting timeline for a major ICT-related incident

4 h / 24 h

Initial notification

As early as possible; within 4 h of classification as major and no later than 24 h after awareness.

72 h

Intermediate report

No later than 72 h after the initial notification, even if there is no status change.

1 month

Final report

No later than one month after the intermediate report or its latest update.

If an incident is classified as major more than 24 hours after the entity became aware of it, the initial notification is due within 4 hours of that later classification. Submit required updates without undue delay; check the competent authority’s process and applicable exceptions.

Assess severity against defined criteria

Apply the criteria and thresholds in Regulation (EU) 2024/1772, including impact on critical services, duration, clients or transactions, geographic spread, data loss and economic impact. Record the classification rationale and timestamp.

FROM THE RULES TO A CLEAR INCIDENT RESPONSE

Six steps to prepare for an incident

A rehearsed process reduces searching and coordination loops when several teams and ICT providers need to establish reliable facts quickly.

01 · Ownership

Name an incident lead, deputy, management contact and reporting owner for each legal entity.

02 · Classification

Assess affected critical services, duration, clients, transactions, countries, data loss and economic impact against the applicable thresholds.

03 · Timeline

Record discovery, awareness, classification decisions and each submission with its time zone.

04 · Gather facts

Document affected functions, impacts, known causes, containment, providers and recovery estimates.

05 · Follow-up reports

Prepare the 72-hour report and updates. Clearly identify estimates and information still being verified.

06 · Close and learn

Complete root-cause analysis, actual impacts and remedial actions; feed lessons into testing and supplier oversight.

Keep these facts ready for the first report

Incident ID and timestamps · affected critical or important function · initial classification rationale · affected countries, clients or transactions · downtime and data impact · immediate measures · key ICT providers · contact and next update time. Use the required forms and reporting channel of the competent authority.

Two important distinctions

Record and classify ICT-related incidents using DORA criteria; major ICT-related incidents must be reported to the authority. A significant cyber threat may be reported voluntarily under Article 19. Check data protection, contract and other sectoral reporting duties separately.

Official sources · legal status checked 8 October 2026

DORA, Regulation (EU) 2022/2554 (notably Arts. 2, 5-19, 28-30, 64) · Delegated Regulation (EU) 2024/1772 (classification criteria) · Delegated Regulation (EU) 2025/301 (timelines) · Implementing Regulation (EU) 2025/302 (reporting forms) · EIOPA, DORA overview.

Official texts: 2022/2554 · 2024/1772 · 2025/301 · 2025/302 · EIOPA

Scope limits

General working aid, not legal advice, technical investigation, conformity assessment or a report to an authority. Check scope, classification, competent authority, reporting channel and exceptions for the specific legal entity.