sosafe

DORA Compliance Checklist

DORA has applied since 17 January 2025 and harmonises the rules on digital operational resilience for financial organisations across the EU.

This checklist helps IT leaders review their current state of DORA implementation in a structured way. It doesn't replace legal advice or a formal audit procedure. It serves as a practical preliminary review of the key areas that need to be reliably managed, documented, and demonstrable in day-to-day IT operations. DORA has applied since 17 January 2025 and harmonises the rules on digital operational resilience for financial organisations across the EU.

How to Use This Checklist

Review each point using three questions:

- ☑ Is this properly governed from a technical standpoint?
- ☑ Does the implementation hold up in daily operations?
- ☑ Is there current evidence to support it?

Rate each point as, for example, "met," "partially met," "open," or "not applicable." This quickly builds a realistic picture of maturity, gaps, and priorities.

1 Executive Governance and Risk Management

Under DORA, senior management remains accountable for oversight and governance. For a Head of IT, what matters most is that governance, reporting lines, and control mechanisms aren't just defined on paper, but actually work in daily operations.

CHECKPOINTS

- ☑ Are roles, responsibilities, and escalation paths for ICT risks clearly defined?
- ☑ Is it documented which bodies make which decisions?
- ☑ Does senior management receive regular, reliable reports on ICT risks, incidents, and measures?
- ☑ Are risk tolerances, protection goals, and minimum requirements clearly established?
- ☑ Is it clearly defined who prioritises, approves, and tracks measures?
- ☑ Are core policies current, approved, and known to the relevant teams?
- ☑ Is there a documented process for reviewing controls regularly and adjusting them as needed?

EVIDENCE

- Governance documents and organisational charts
- Risk reports and management reports
- Policies, approvals, and minutes
- Control plans and review schedules

2 ICT Risk Management

Structured ICT risk management sits at the centre of DORA's requirements. Risks must be identified, assessed, treated, and reviewed regularly. This covers not just technology, but also processes, data, dependencies, and people.

CHECKPOINTS

- [x] Is there a complete picture of critical systems, applications, data flows, and interfaces?
- [x] Are ICT risks assessed and prioritised using consistent criteria?
- [x] Are risks linked to specific measures, deadlines, and owners?
- [x] Are changes to the system landscape reflected in the risk assessment?
- [x] Are contingency planning, recovery, and protective measures part of risk management?
- [x] Are risks reassessed regularly, for example after incidents, tests, or major changes?
- [x] Is it documented which residual risks were accepted, and by whom?

EVIDENCE

- Risk inventory and risk register
- Protection needs or criticality assessments
- Action plans with owners and deadlines
- Review records and approvals

3 Incident Reporting and Detection

DORA devotes a dedicated chapter to the management, classification, and reporting of ICT-related incidents. Major incidents require established processes, clear responsibilities, and harmonised reporting to the relevant authorities.

CHECKPOINTS

- ☑ Is there a documented process for detecting, assessing, escalating, and handling ICT incidents?
- ☑ Are criteria defined for classifying an incident as major?
- ☑ Do IT, security, compliance, and other relevant teams know when they need to be involved?
- ☑ Are internal and external reporting channels formally established?
- ☑ Can teams gather the information needed for initial notifications, intermediate reports, and final reports in good time?
- ☑ Are causes, impacts, measures taken, and lessons learned documented in a traceable way?
- ☑ Are reporting obligations regularly rehearsed so they hold up under time pressure?

EVIDENCE

- Incident response process and escalation matrix
- Incident classification criteria
- Reporting forms, templates, and contact lists
- Incident documentation and post-incident reviews

4 Digital Operational Resilience Testing

DORA requires regular testing of ICT tools, systems, and processes. The goal isn't just proof of testing, but evidence that controls, response procedures, and recovery actually deliver when it counts.

CHECKPOINTS

- ☑ Is there a documented testing programme covering scope, frequency, and responsibilities?
- ☑ Are technical controls, recovery procedures, and contingency processes tested regularly?
- ☑ Are critical systems and processes included in the testing scope?
- ☑ Are results, deviations, and remediation measures systematically documented?
- ☑ Are there clear deadlines for fixing identified weaknesses?
- ☑ Are test results fed back into risk analyses and improvement measures?
- ☑ Has it been assessed whether additional advanced testing requirements apply to your institution?

EVIDENCE

- Test plans and testing calendars
- Results from contingency tests, recovery tests, or technical reviews
- Action lists with status
- Management reports on test findings

5 Third-Party Risk and Information Registers

Robust management of ICT third-party risk is a core part of DORA. This includes maintaining a comprehensive register of contractual arrangements with ICT third-party providers that supervisory bodies and internal governance can rely on.

CHECKPOINTS

- ☑ Is it fully documented which ICT third-party providers are used for which services?
- ☑ Are critical or important functions clearly identified?
- ☑ Are dependencies, subcontractors, and concentration risks visible?
- ☑ Are current contracts in place with the necessary provisions on security, access, audit, support, and exit?
- ☑ Is there a clear process for selecting, assessing, approving, and continuously monitoring providers?
- ☑ Is the information register updated regularly and quality-checked?
- ☑ Are exit strategies for critical services documented and realistically achievable?

EVIDENCE

- Register of information and contractual relationships
- Provider assessments and risk classifications
- Contract documentation and control evidence
- Exit plans and overviews of subcontractors

6 Human Risk Management and Security Awareness

DORA is primarily concerned with governance, risk, incidents, testing, and third parties. In practice, though, controls often fail because of human error, unclear responsibilities, or unsafe decisions. For a Head of IT, this area is operationally relevant even though DORA doesn't treat it as a dedicated chapter.

CHECKPOINTS

- ☑ Do employees know how to recognise phishing, social engineering, and suspicious requests?
- ☑ Do they know the correct channel for reporting security incidents and irregularities?
- ☑ Are awareness measures tailored to target groups, risks, and roles?
- ☑ Are particularly exposed groups trained specifically, such as helpdesk, finance, or admin teams?
- ☑ Are training sessions, phishing simulations, or communication measures evaluated?
- ☑ Do common failure patterns feed back into technical and organisational safeguards?
- ☑ Is it clearly defined how security awareness works together with incident response and risk management?

EVIDENCE

- Training concepts and participation rates
- Results from simulations or learning formats
- Communication plans and reporting guidance
- Measures derived from lessons learned

7 Documentation and Evidence Readiness

In practice, DORA compliance often fails not just due to missing measures, but due to a lack of evidence readiness. What counts in an audit is whether requirements are documented in a traceable way, kept up to date, and readily available when needed.

CHECKPOINTS

- ☑ Are core policies, processes, and evidence complete and up to date?
- ☑ Are there clear owners for documents and registers?
- ☑ Are versions, approvals, and changes tracked in a traceable way?
- ☑ Can evidence be provided within a short timeframe?
- ☑ Is it documented how decisions on measures, exceptions, and residual risks were made?
- ☑ Are overlaps between IT, security, risk, and compliance clearly coordinated?

EVIDENCE

- Document control and approval lists
- Process documentation and procedural instructions
- Audit trails, review histories, and action records

Prioritising Your First Gap Analysis

Not every gap carries the same weight. Three priority questions help with an initial assessment:

- ☑ Does the gap affect a critical process or an important function?
- ☑ Does the gap increase the risk of a major ICT incident or a delayed report?
- ☑ Is evidence missing that would be immediately relevant in an audit?

If you answer yes to any of these questions, the item should be prioritised for short-term action.

Internal Assessment Template

Checkpoint Area	Status	Risk if Gap Exists	Next Action	Owner	Target Date
Governance					
ICT Risk Management					
Incident Management					
Resilience Testing					
ICT Third-Party Providers					
Human Risk Management					
Documentation					

In Practice

This checklist works best when it isn't filled out by a single team in isolation. The strongest results come from IT, information security, risk management, compliance, and other relevant teams looking at the same state of implementation together. That way, gaps surface earlier and measures become verifiable faster.