Sample audit programme

DORA

ICT third-party risk

14 audit steps · DORA

14 audit steps with criterion, reference, procedure and expected evidence. 8 documents to request and the typical findings.

DORA Art. 28(1) · DORA Art. 28(2) · DORA Art. 28(3) · DORA Art. 28(4) · DORA Art. 28(4), Art. 29 · DORA Art. 28(5) · DORA Art. 30(2) · DORA Art. 30(3) · DORA Art. 28(6) · Art. 30(3)(e) · DORA Art. 28(7) · DORA Art. 28(8) · DORA Art. 30(3)(a) and (b)

Audit objective and scope

The audit assesses whether the financial entity manages the risk from using ICT service providers as part of its ICT risk management and remains responsible for complying with its obligations. The focus is on strategy, register of information, selection, contract design, ongoing monitoring and exit planning.

SCOPE

- All contractual arrangements for ICT services, with emphasis on services supporting critical or important functions
- Procurement, contract management, information security, business units and management as participants in the process
- Entities within the scope of Regulation (EU) 2022/2554; clarify applicability and proportionality beforehand
- Out of scope: oversight of critical ICT third-party providers by the European supervisory authorities

Audit steps 1 to 3

Step 01 DORA Art. 28(1)

Responsibility for third-party risk remains with the financial entity and is part of the ICT risk management framework.

Procedure Read the framework and responsibilities and establish the roles for steering, monitoring and escalating provider relationships.

Evidence ICT risk management framework, role descriptions, organisation chart

Step 02 DORA Art. 28(2)

A strategy for ICT third-party risk exists, includes a policy on services supporting critical or important functions and is reviewed regularly; the management body regularly reviews the risks arising from the contracts.

Procedure Check strategy and policy for approval, currency and content, and trace how the management body dealt with them.

Evidence Strategy, policy, decisions and minutes of the management body

Step 03 DORA Art. 28(3)

A register of information on all contractual arrangements for ICT services is maintained and complete.

Procedure Compare the register with the contract inventory, the creditor list and procurement data and identify missing providers.

Evidence Register of information, contract inventory, creditor master data

Audit steps 4 to 6

Step 04 DORA Art. 28(3)

Contracts for critical or important functions are traceably identified in the register.

Procedure Read the classification method and re-perform the classification for a sample of services.

Evidence Classification method, register with flags, assessment documents

Step 05 DORA Art. 28(3)

The register is kept up to date, provided on request, and new or changed arrangements for critical functions are reported to the supervisor in time.

Procedure Review the maintenance process, the latest update and the reports to the supervisor, and compare deadlines with the requirements.

Evidence Process description, change history of the register, reports to the supervisor

Step 06 DORA Art. 28(4)

Before a contract is concluded, the entity assesses whether a critical or important function is affected, what risks exist and whether conflicts of interest arise.

Procedure Select a sample of contracts from the last year and go through the pre-contract assessment and due diligence.

Evidence Assessments before signing, due diligence results, approvals

Audit steps 7 to 10

Step 07 — DORA Art. 28(4), Art. 29

Concentration risks arising from single providers or from linked providers are assessed.

Procedure Review the assessment method and the latest analysis and check whether dependencies on single providers and locations are identified.

Evidence Concentration analysis, dependency overview, results for management

Step 08 — DORA Art. 28(5)

Contracts are concluded only with providers that meet appropriate information security standards.

Procedure For a sample, inspect the provider evidence, such as certificates or audit reports, and review the assessment of that evidence.

Evidence Certificates, audit reports, assessment of the evidence

Step 09 — DORA Art. 30(2)

Contracts contain the minimum elements required for all ICT services.

Procedure Derive a checklist from Art. 30(2) and compare a sample of contracts against it.

Evidence Contracts with annexes, completed checklist

Step 10 — DORA Art. 30(3)

Contracts for services supporting critical or important functions contain the additional provisions.

Procedure Check the sample against the additional requirements for these contracts, including service levels, contingency plans and exit arrangements.

Evidence Contracts, service level agreements, checklist for critical functions

Audit steps 11 to 14

Step 11 — DORA Art. 28(6); Art. 30(3)(e)

Access, information and audit rights are agreed; the frequency and scope of audits at the provider follow the risk.

Procedure Review the provider audit plan and trace the audits performed and their results.

Evidence Provider audit plan, reports, follow-up of actions

Step 12 — DORA Art. 28(7)

Termination rights for the cases provided for are agreed in contracts and their exercise is organised.

Procedure Check termination clauses in the sample and ask who decides on exercising them.

Evidence Contract clauses, decision process

Step 13 — DORA Art. 28(8)

For services supporting critical or important functions, exit strategies are documented, tested and reviewed regularly.

Procedure Read the exit plans and check test evidence and transition plans for data and services.

Evidence Exit plans, test records, transition concepts

Step 14 — DORA Art. 30(3)(a) and (b)

Performance and security incidents at providers are monitored and reported on an ongoing basis.

Procedure Review regular reports and service level evaluations of the last twelve months and follow up the response to deviations.

Evidence Performance reports, incident notifications, action lists

Document request list

Request these 8 documents before you start

1. Strategy and policy for ICT third-party risk
2. Register of information with change history
3. Contract inventory, creditor list and list of providers for critical or important functions
4. Sample of contracts with annexes and service level agreements
5. Pre-contract assessments, due diligence and concentration analyses
6. Audit plan and audit reports on providers
7. Exit plans with test evidence
8. Reports and decisions of the management body on the topic

TYPICAL FINDINGS

The register is incomplete because contracts were concluded outside central procurement.

The classification of critical or important functions is not justified or not consistent.

Pre-contract assessments are missing for existing contracts and were not made up for at renewal.

Existing contracts lack some minimum elements, for example on subcontractors or return of data.

Exit plans exist on paper but have never been tested.

Concentration risks are not evaluated even though several services run with the same provider.

Sample audit programme library

29 sample audit programmes online

proauditmap.com/en/audit-programs/

Full audit package in ProAuditMap

proauditmap.com

ProAuditMap

Sample provided without warranty and not legal advice. Laws, regulations and standards appear only as references, no normative text is reproduced. Adapt scope and depth to your organisation, your risks and the current version of the provisions that apply to you before use.
Last updated: 13 October 2026