Sample audit programme

# Cloud use and outsourcing

## 12 audit steps · ISO 27001, DORA, BSI

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

ISO/IEC 27001:2022 Annex A 5.23 · BSI OPS.2.2 · DORA Art. 28(4) · DORA Art. 30(2) · ISO/IEC 27001:2022 Annex A 5.20 · DORA Art. 28(3) · ISO/IEC 27001:2022 Annex A 8.2 · § 30(2) no. 10 BSIG · ISO/IEC 27001:2022 Annex A 5.23 and 8.9 · ISO/IEC 27001:2022 Annex A 5.22 · DORA Art. 30(3)(a) and (b) · DORA Art. 29 · DORA Art. 28(8) · ISO/IEC 27001:2022 Annex A 5.30

## Audit objective and scope

The audit assesses whether the organisation governs its use of cloud services: from the decision and risk assessment through contract design and the division of tasks with the provider to secure configuration, ongoing monitoring and an orderly exit. It also assesses whether the additional requirements for financial entities are taken into account where they apply.

### SCOPE

- Software, platform and infrastructure services used by the organisation, including shadow IT that comes to light
- Decision, contract and operating processes for cloud services
- Configuration and access of the organisation's tenants at the provider
- Out of scope: internal security of the provider's data centres, unless considered separately through certificates or reports

## Audit steps 1 to 3

Step 01 — ISO/IEC 27001:2022 Annex A 5.23; BSI OPS.2.2

### A cloud strategy or policy defines for which data and processes cloud services may be used and by which criteria providers are selected.

**Procedure** Read the strategy and policy, check approval and compare them with the services actually used.

**Evidence** Cloud policy with approval, list of cloud services in use

Step 02 — ISO/IEC 27001:2022 Annex A 5.23; DORA Art. 28(4)

### Before use, the protection requirement of the data concerned is established and the risk is assessed, including whether the function is critical or important.

**Procedure** For three cloud services, review the risk assessment made before introduction and trace the classification of the function.

**Evidence** Risk assessments, protection requirement determinations, decision papers

Step 03 — ISO/IEC 27001:2022 Annex A 5.23; BSI OPS.2.2

### Tasks between organisation and provider are delimited in writing, so that it is clear who is responsible for configuration, access, backup and logs.

**Procedure** Read the responsibility matrix and contract documents and check for two services whether the tasks are actually performed.

**Evidence** Responsibility matrix, contracts and service descriptions

## Audit steps 4 to 6

Step 04 — DORA Art. 30(2); ISO/IEC 27001:2022 Annex A 5.20

### Contracts contain provisions on information security, location of data, subcontractors, incident reporting, audit rights and termination.

**Procedure** Review contracts of the essential cloud providers against a checklist covering these points.

**Evidence** Contracts, annexes on security and data processing, completed checklist

Step 05 — DORA Art. 28(3)

### A register records all outsourced services with contract data and classification and is kept current.

**Procedure** Compare the register with procurement records and invoices to find services that are not recorded.

**Evidence** Register of outsourcing, invoice analysis, list of procurements

Step 06 — ISO/IEC 27001:2022 Annex A 8.2; § 30(2) no. 10 BSIG

### Access to cloud consoles is limited to authorised people and protected by multi-factor authentication; privileged roles are reviewed regularly.

**Procedure** Read administrator roles in two tenants and trace authentication and the last review.

**Evidence** Role and user extracts, authentication policy, review record

## Audit steps 7 to 9

**Step 07** ISO/IEC 27001:2022 Annex A 5.23 and 8.9; BSI OPS.2.2

### Cloud resources are configured according to defined standards; deviations are detected and corrected.

**Procedure** Compare configuration standards with the settings of one tenant, in particular public exposure and encryption.

**Evidence** Configuration standards, results of configuration checks, extract of settings

**Step 08** ISO/IEC 27001:2022 Annex A 5.23

### Data is protected at rest and in transit; keys are managed under control.

**Procedure** Check encryption settings and key management for two services.

**Evidence** Configuration extracts, key management concept

**Step 09** ISO/IEC 27001:2022 Annex A 5.22; DORA Art. 30(3)(a) and (b)

### Performance, availability and security incidents of providers are monitored; reports and certificates are evaluated.

**Procedure** Review reports of the last twelve months and check whether deviations were followed up.

**Evidence** Performance reports, certificates and audit reports, meeting minutes

## Audit steps 10 to 12

Step 10

DORA Art. 28(4); DORA Art. 29

### Concentration risks, for example from depending on one provider for several essential services, are identified and assessed.

**Procedure** Analyse the distribution of essential services across providers and review the assessment of concentration risk.

**Evidence** Analysis by provider, risk assessment, management decisions

Step 11

DORA Art. 28(8); ISO/IEC 27001:2022 Annex A 5.23

### For critical services there are documented and tested exit and repatriation plans.

**Procedure** Read exit plans and trace whether data export and alternatives have been checked or tried.

**Evidence** Exit plans, test records, evidence of data export

Step 12

ISO/IEC 27001:2022 Annex A 5.30

### Continuity and recovery plans take the failure of a cloud provider into account.

**Procedure** Check continuity plans for the cloud services covered and review the results of the last exercise.

**Evidence** Continuity plans, exercise records, recovery times

Document request list

# Request these 8 documents before you start

1. Cloud strategy or policy on the use of cloud services
2. Register of services in use and outsourced, with classification
3. Contracts, service descriptions and annexes on data processing
4. Risk assessments and decision papers for the services in the sample
5. Responsibility matrix between organisation and provider
6. Role and configuration extracts from the tenants
7. Reports, certificates and audit reports of the providers
8. Exit and continuity plans

## TYPICAL FINDINGS

- Business units procure cloud services without involving information security, and they are not in the register.
- Responsibility for backup and logs is not clarified between organisation and provider.
- Contracts contain no audit rights and no provision on subcontractors.
- Public exposure or weak configurations are not detected by ongoing checks.
- Administrator access to the cloud console is not protected by multi-factor authentication.
- An exit plan is missing or has never been tried; data export is unclear.

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