Sample audit programme

IT projects

12 audit steps · ISO 27001, GDPR, GoBD

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

ISO 21502:2020 · ISO/IEC 27001:2022 Annex A 5.8 · ISO/IEC 27001:2022 Annex A 5.8 and 8.26 · Art. 25 and 35 GDPR · ISO/IEC 27001:2022 Annex A 8.29 · GoBD para. 142 · ISO/IEC 27001:2022 Annex A 8.32

Audit objective and scope

The audit assesses whether an IT project is run with a clear mandate, a suitable organisation and effective control of time, budget, scope and risks. It also assesses whether information security and data protection requirements are included, tests and acceptance are documented, data is migrated completely and correctly and operations are handed over properly.

SCOPE

- One selected ongoing or recently completed IT project
- Project mandate, project organisation, planning, reporting and change control
- Security and data protection requirements, testing, acceptance, data migration and handover to operations
- Out of scope: the technical correctness of individual design decisions

Audit steps 1 to 3

Step 01 — ISO 21502:2020; ISO/IEC 27001:2022 Annex A 5.8

A binding method with phases and decision points applies to projects.

Procedure Read the method and check for the selected project whether the defined decision points were passed.

Evidence Project management handbook, evidence of phase decisions

Step 02 — ISO 21502:2020

An approved project mandate describes objective, benefit, scope, budget and deadlines.

Procedure Read the mandate and business case and check approval by the sponsor.

Evidence Project mandate, business case, approval note

Step 03 — ISO 21502:2020

The project organisation with sponsor, steering committee and project management is defined and works demonstrably.

Procedure Check the project organisation chart and steering committee minutes for decisions and escalations.

Evidence Project organisation chart, steering committee minutes

Audit steps 4 to 6

Step 04

ISO/IEC 27001:2022 Annex A 5.8 and 8.26

Information security is anchored in the project: protection needs and security requirements are determined early.

Procedure Check whether protection needs and security requirements are documented and assessed by the security officer.

Evidence Protection needs assessment, security requirements, information security statement

Step 05

Art. 25 and 35 GDPR

Data protection by design is considered; where required, a data protection impact assessment has been carried out.

Procedure Trace the involvement of data protection and review the threshold check or impact assessment.

Evidence Statement of the data protection officer, threshold check, impact assessment

Step 06

ISO 21502:2020; ISO/IEC 27001:2022 Annex A 5.8

Project risks, including information security risks, are recorded, assessed and followed up with actions and owners.

Procedure Check the risk list for currency and trace actions and status for three risks.

Evidence Risk list, status reports

Audit steps 7 to 9

Step 07 — ISO 21502:2020

Progress, budget and deadlines are measured regularly and reported to the sponsor.

Procedure Analyse status reports with planned versus actual comparison of costs and dates.

Evidence Status reports, project plan, budget overview

Step 08 — ISO 21502:2020

Changes to project scope are requested, assessed and approved.

Procedure Check change requests for assessment of cost, time and risk and for approval.

Evidence Change requests, approvals

Step 09 — ISO/IEC 27001:2022 Annex A 8.29

Testing and acceptance follow documented criteria; security testing is included.

Procedure Review test concept, test results and acceptance record and assess open defects at acceptance.

Evidence Test concept, test records, acceptance record

Audit steps 10 to 12

Step 10 — GoBD para. 142

Data migrations are checked for completeness and correctness; legacy data remains analysable for the retention period.

Procedure Check the migration concept and reconciliation evidence such as totals and record counts and clarify the handling of the legacy system.

Evidence Migration concept, reconciliation records, legacy data concept

Step 11 — ISO/IEC 27001:2022 Annex A 8.32

Handover to operations goes through the change process with operating documentation and owners.

Procedure Check the handover record and the change request for go-live.

Evidence Handover record, operations manual, change request

Step 12 — ISO 21502:2020

The project is formally closed; lessons learned and benefit realisation are evaluated.

Procedure Read the closure report and check whether a benefit review is planned or done.

Evidence Closure report, lessons learned, benefit review

Document request list

Request these 8 documents before you start

1. Project management handbook
2. Project mandate and business case
3. Steering committee minutes and status reports
4. Risk list and change requests
5. Protection needs assessment and security requirements
6. Data protection statement and, where applicable, impact assessment
7. Test concept, test records and acceptance record
8. Migration concept with reconciliation evidence

TYPICAL FINDINGS

- The project mandate was never formally approved.
- The steering committee meets rarely and takes no documented decisions.
- Security and data protection are involved only shortly before go-live.
- Scope changes are implemented without assessment.
- Acceptance is given despite open severe defects.
- The data migration is not reconciled, legacy data cannot be read after shutdown.

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