# The ISO 27001 evidence chain

One risk, twelve links. An auditor can pull on any of them. Can you show it?

**Example risk: ransomware on the file server**

Backbone · Proof · Expected · Often missing

1. **Scope** — DOCUMENT · 4.3
   **Auditor asks** *Is this system inside your boundary?*
   **Keep ready** Scope document: what is in, what is out and why, interfaces.
2. **Risk assessment methodology** — DOCUMENT · 6.1.2
   **Auditor asks** *How did you score this risk?*
   **Keep ready** Scales, risk matrix, acceptance line, risk owners.
3. **Risk register entry** — RECORD · 8.2
   **Auditor asks** *Where is this risk recorded, and who owns it?*
   **Keep ready** Dated register row: scenario, score, owner, treatment decision.
4. **Statement of Applicability row** — DOCUMENT · 6.1.3
   **Auditor asks** *Why is this control applicable?*
   **Keep ready** SoA row: reason, status, link to the evidence.
5. **Risk treatment plan entry** — DOCUMENT · 6.1.3 / 8.3
   **Auditor asks** *What did you decide to do, and by when?*
   **Keep ready** Action, owner, due date, status, risk owner’s sign-off on the residual risk.
6. **Security objective** — DOCUMENT · 6.2
   **Auditor asks** *How will you know it works?*
   **Keep ready** Objective with KPI, target, owner and deadline.
7. **Policy or procedure for the control** — DOCUMENT · 7.5.1
   **Auditor asks** *What is the rule?*
   **Keep ready** For example the backup policy: scope, frequency, retention, restore testing.
8. **Operational evidence** — RECORD · 8.1 — WHERE CHAINS SNAP
   **Auditor asks** *“Show me the last restore test.”*
   **Keep ready** Backup logs and dated restore-test records.
9. **Monitoring result** — RECORD · 9.1
   **Auditor asks** *What did the measurements say?*
   **Keep ready** Dated KPI results (for example restore success rate) with a short analysis.
10. **Internal audit report** — RECORD · 9.2
    **Auditor asks** *Did you check this independently?*
    **Keep ready** Audit programme, scope, findings, evidence, report to management.
11. **Management review minutes** — RECORD · 9.3
    **Auditor asks** *What did management decide?*
    **Keep ready** Minutes showing the inputs reviewed and decisions with owners.
12. **Corrective action log** — RECORD · 10.2
    **Auditor asks** *What did you fix, and did it work?*
    **Keep ready** Finding, root cause, action, effectiveness check.

**Your homework** **Take one risk from your own register and walk it along these twelve links. The first link you can’t show is your next task.**

# Every document and record, field by field

What the standard asks for, and a practical structure for each. Use it as a checklist.

## 1 THE BACKBONE: documents the standard requires you to have

| Document | Must show | Typical fields |
|---|---|---|
| **ISMS scope** Clause 4.3 | Boundaries and applicability; interfaces and dependencies; what is out, and why | Purpose · organisation and context · in scope · out of scope with reason · interfaces · owner, version, approval |
| **Information security policy** Clause 5.2 | Fits your organisation; frames objectives; commits to requirements and improvement | Purpose · principles · commitments · responsibilities · review cycle · management signature (1–2 pages) |
| **Risk assessment methodology** Clause 6.1.2 | Acceptance and assessment criteria; consistent, comparable results; risk owners | Approach · likelihood and impact scales with definitions · risk matrix and acceptance line · roles · when to reassess |
| **Risk treatment methodology** Clause 6.1.3 | How treatment options are chosen; who approves; owner accepts the residual risk | Options (reduce, avoid, share, accept) · how controls are chosen · approval |
| **Statement of Applicability** Clause 6.1.3 d | Every necessary control, why it is included, whether implemented; a reason for each exclusion | Control · applicable (yes/no) · reason · status · link to evidence. Annex A (2022): 93 controls |
| **Risk treatment plan** Clause 6.1.3 e–f | Actions per risk; the risk owner approves the plan and the residual risk | Risk ID · action · owner · resources · due date · status · residual risk and approval |
| **Information security objectives** Clause 6.2 | Consistent with the policy; measurable where practicable; monitored | Objective · KPI · baseline · target · owner · deadline · how it is measured |

## 2 THE PROOF: records the standard requires you to keep

| Record | Must show | Typical fields |
|---|---|---|
| **Competence records** Clause 7.2 | People are competent for the roles you gave them | Role · required skills · evidence (training, certificate, CV) · date · next due |
| **Risk assessment results (risk register)** Clause 8.2 | Assessments at planned intervals and on significant change | ID · scenario · threat and vulnerability · impact · likelihood · score · owner · controls · decision · residual risk · status · date |
| **Risk treatment results** Clause 8.3 | The plan was actually carried out | Updated register and plan status, with a link to the evidence |
| **Monitoring and measurement results** Clause 9.1 | Performance and effectiveness are evaluated | KPI definitions (what, how, when, who) · dated results · short analysis |
| **Internal audit programme and reports** Clause 9.2 | Planned, independent checks by objective and impartial auditors | Programme · scope and criteria · findings · evidence · report to management |
| **Management review minutes** Clause 9.3 | Required inputs reviewed; decisions and changes recorded | Date and attendees · inputs · discussion · decisions with owners · next review |
| **Nonconformity and corrective action log** Clause 10.2 | What went wrong, why, what you did, and whether it worked | Finding · source · root cause · action · owner · due date · effectiveness check |

# What auditors expect, and what is nice to have

Not named in the mandatory list, but your Statement of Applicability and clause 7.5.1 make them necessary in practice.

## 3 THE EXPECTATIONS: optional on paper, mandatory in practice

| Document | Typical fields | Watch out |
|---|---|---|
| **Asset inventory**<br>Annex A 5.9 | ID · asset · owner · type · classification · location · criticality | IT assets only; no owners |
| **Supplier list and assessments**<br>Annex A 5.19–5.22 | Supplier · service · data or systems accessed · criticality · security terms in the contract · assessment · next review | No review; no security terms |
| **Access control policy**<br>Annex A 5.15 | Principles (need-to-know, least privilege) · request and approval · periodic review · removal · privileged access | No records of access reviews |
| **Incident response procedure**<br>Annex A 5.24–5.27 | Roles · detect and report · classify · respond · communicate (incl. legal duties) · preserve evidence · lessons learned | Never exercised; tickets not kept |
| **Backup policy**<br>Annex A 8.13 | Scope · frequency · locations · retention · protection · restore testing · roles | No restore-test evidence |
| **Change management procedure**<br>Annex A 8.32 | Request · impact and risk assessment · approval · test · implement · roll back · record | Emergency changes skip the process |
| **Business continuity plan**<br>Annex A 5.29–5.30 | Critical processes · recovery targets · roles and contacts · strategies · communication · test schedule | Written once, never tested |
| **External documents**<br>Clause 7.5.3 | Laws (for example GDPR, NIS2 where it applies), customer contracts and SLAs, supplier agreements, standards: each with version, location, owner | Unknown versions; no list |
| **Operational evidence**<br>Clause 8.1 | Change tickets · access logs · backup logs · incident tickets: dated, retrievable, tied to the procedure | Procedures exist, traces do not |

## 4 ADD-ONS: not required, but they save time

| Add-on | Why it helps | Related |
|---|---|---|
| Roles and responsibilities matrix (RACI) | Shows who does what, and who owns what | Annex A 5.2 |
| Document and record control procedure | Naming, versions, approval and retention keep the set consistent | Clause 7.5.2 / 7.5.3 |
| Information classification guideline | One shared language for assets and controls | Annex A 5.12 / 5.13 |
| Security awareness plan | Turns “we did a training” into a planned programme with records | Clause 7.3 / Annex A 6.3 |
| ISMS map on a page | One diagram showing how documents and records link | — |

*If your SoA marks the matching control “applicable”, some add-ons move up into the expectations group, for example vulnerability management, cryptography or acceptable use.*

**Want your evidence chain built together with your team?**

We build practical ISMS, mainly ISO/IEC 27001, with your people, and hand over the knowledge to run it yourself.

**feldmanncyber.com** · New guides in your inbox: **feldmanncyber.com/newsletter**