



Community Library

ISO 27001 Preparation Checklist

Every step, and the proof an auditor will ask for.

37

Organizational

8

People

14

Physical

34

Technological

1.0 · 2026-10

itrygg.com

How to use this checklist

A checked box is not evidence. Most ISO 27001 checklists tell you what to do. This one also tells you what proof you will need to show for it, and where in the standard that requirement lives.

1. Work the phases in order. They follow a 12-week implementation, with a pre-kickoff stage before and certification and sustain stages after.
2. For each task, the Proof line is what an auditor will ask to see. If you cannot produce it, the task is not done.
3. References point to ISO/IEC 27001:2022 clauses (e.g. 6.1.2) or Annex A controls (e.g. A.5.9).

Before kickoff	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Certification	Sustain
Week 0	Weeks 1–2	Weeks 3–4	Weeks 5–6	Weeks 7–9	Weeks 10–12	After week 12	Ongoing

Sponsorship and scope

Projects that go live survive on dedicated sponsorship. Secure it before any work starts.

- ☐ Name an executive sponsor who owns the ISMS outcome and can commit budget and people. 5.1, 7.1
Proof: Signed charter or sponsor memo naming the sponsor and their authority.
- ☐ Document the internal and external issues that affect information security. 4.1
Proof: Context of the organization record.
- ☐ List interested parties (clients, regulators, insurers, suppliers) and what each requires of you. 4.2
Proof: Interested parties register with requirements.
- ☐ Define the ISMS scope: locations, business units, systems, and the interfaces with what sits outside it. 4.3
Proof: Approved scope statement, including boundaries and exclusions.
- ☐ Communicate the scope to the people and suppliers inside it. 7.4
Proof: Dated communication record or meeting minutes.

Kickoff, data assessment and risk review

Know what you are protecting and where the truth about each control lives.

- ☐ Build an inventory of information and associated assets: data, people, devices, cloud services, locations, and intangibles. A.5.9
Proof: Asset register with an owner on every row.
- ☐ Classify each asset and define how each classification is handled. A.5.12, A.5.13
Proof: Classification scheme and labeled asset register.
- ☐ Identify the source system for each control area: identity, mail, endpoints, backup, and logging. A.5.15, A.8.7, A.8.13, A.8.15
Proof: Data source map showing which system enforces and reports each control.
- ☐ Assess data quality in those systems: stale accounts, unmanaged devices, missing owners. A.5.18, A.8.1
Proof: Data assessment findings with counts and dates.
- ☐ Document a risk assessment method: criteria for likelihood, impact, and acceptance. 6.1.2
Proof: Risk methodology document approved by management.
- ☐ Review or build the risk register: each risk scenario with its owner, likelihood, impact, and rating. 6.1.2, 8.2
Proof: Risk register with dated assessment.
- ☐ Draft the Statement of Applicability against all 93 Annex A controls. 6.1.3 d
Proof: Draft SoA listing every control as included or excluded.

Gap analysis and project plan

Score each control from system data, not self-rating, then plan the work to close the gaps.

- ☐ Score each applicable control from the data in the system that enforces it. 9.1
Proof: Gap analysis showing each score, how it was calculated, and when the data was pulled.
- ☐ Record constraints and exclusions with a justification for each. 6.1.3 d
Proof: Final SoA with justification for every inclusion and exclusion.
- ☐ Choose a treatment for each risk: modify, avoid, share, or accept. 6.1.3, 8.3
Proof: Risk treatment plan with owner and target date per action.
- ☐ Get risk owners to formally accept residual risk. 6.1.3 f
Proof: Signed or recorded residual risk acceptance.
- ☐ Set measurable information security objectives. 6.2
Proof: Objectives with metric, owner, target, and review date.
- ☐ Build the project plan with milestones through the first release. 6.2, 8.1
Proof: Project plan or work breakdown with owners and dates.

Policy development and roles review

Write policies people can follow, and give every control a named owner.

- ☐ Publish an information security policy approved by top management. 5.2
Proof: Approved policy with version, date, and approver.
- ☐ Write topic-specific policies for access, acceptable use, suppliers, incidents, and continuity. A.5.1
Proof: Approved policy set, each mapped to its Annex A controls.
- ☐ Assign roles, responsibilities, and authorities for the ISMS and every applicable control. 5.3, A.5.2
Proof: RACI or roles matrix; every control has one named owner.
- ☐ Set up document control: versioning, approval, review cycle, and retention. 7.5
Proof: Document control procedure and a master document list.
- ☐ Define supplier security requirements and review key suppliers and cloud services. A.5.19, A.5.20, A.5.23
Proof: Supplier register with assessments and contract security clauses.
- ☐ Document incident management and business continuity procedures. A.5.24, A.5.29, A.5.30
Proof: Incident response procedure and continuity plan with test schedule.
- ☐ Identify the legal, regulatory, and contractual requirements that apply. A.5.31
Proof: Legal and regulatory register with owners.

Training and awareness

Make sure people know the policies, the threats, and their part in the ISMS.

- ☐ Define the competence each ISMS role needs and close the gaps. 7.2
Proof: Competence matrix and training or certification records.
- ☐ Run security awareness training for all personnel in scope. 7.3, A.6.3
Proof: Completion records by person and date.
- ☐ Train people on the threats you actually face, such as phishing and business email compromise. A.6.3
Proof: Simulation or assessment results over time.
- ☐ Collect policy acknowledgments from every person in scope. A.5.10, A.6.2
Proof: Signed acknowledgment records.
- ☐ Establish a disciplinary process for security policy violations. A.6.4
Proof: Documented disciplinary process referenced in HR policy.
- ☐ Build security into onboarding and offboarding. A.6.1, A.6.5, A.5.18
Proof: Onboarding checklist and access removal records.
- ☐ Plan what gets communicated, to whom, when, and by whom. 7.4
Proof: Communication plan.

First release walkthrough

Prove the ISMS runs: measure it, audit it, review it, and fix what you find.

- | | |
|--|------|
| ☐ Walk the live registers end to end with control owners: assets, risks, SoA, suppliers, incidents. | 8.1 |
| Proof: Walkthrough record with attendees and actions. | |
| ☐ Report on objectives and control performance from current data. | 9.1 |
| Proof: Monitoring report showing each measure and its data date. | |
| ☐ Run an internal audit with auditors who did not build the area they audit. | 9.2 |
| Proof: Audit program, plan, and report with findings. | |
| ☐ Hold a management review covering every required input. | 9.3 |
| Proof: Minutes with decisions, actions, and resource commitments. | |
| ☐ Log every nonconformity with root cause and corrective action. | 10.2 |
| Proof: Corrective action log with closure evidence. | |
| ☐ Plan how changes to the ISMS will be controlled from here on. | 6.3 |
| Proof: Change planning record. | |

External audit

Let an accredited certification body confirm what your evidence already shows.

- ☐ Select an accredited certification body.

Proof: Signed certification agreement.

- ☐ Complete the Stage 1 audit: documentation and readiness review.

Proof: Stage 1 report with any areas of concern addressed.

- ☐ Complete the Stage 2 audit: auditors test that controls are implemented and operating.

Proof: Stage 2 report.

- ☐ Close each nonconformity with root cause analysis and evidence the fix works.

Proof: Accepted corrective action plan and closure evidence.

10.2

Continual improvement

Certification is the start. Keep the data current and the ISMS improving.

- ☐ Prepare for surveillance audits in years one and two, and recertification in year three.
Proof: Three-year audit calendar.
- ☐ Refresh control data on a set cadence so no score goes stale. 9.1
Proof: Each control shows when its data last updated.
- ☐ Reassess risk at planned intervals and when significant changes occur. 8.2
Proof: Dated risk register revisions.
- ☐ Run management reviews and internal audits on schedule. 9.2, 9.3
Proof: Annual audit program and review minutes.
- ☐ Track improvements as well as fixes. 10.1
Proof: Improvement log.

Want to know where you stand today?

Start with a Gap Assessment. We score your controls from the systems that run them, so you see the gaps before an auditor, insurer, or attacker does.

[Start with a Gap Assessment](https://itrygg.com/#demo) (itrygg.com/#demo)

[Book a demo](https://itrygg.com/#demo) (itrygg.com/#demo)

Portal demos follow a mutual NDA.

isms@itrygg.com

This checklist is guidance, not a substitute for the ISO/IEC 27001:2022 standard. Purchase the standard from ISO or your national standards body. Certification decisions are made only by accredited certification bodies.

© 2026 Trygg, Inc.