The ISO 27001:2022 Starter Checklist

Get audit-ready in 9 steps

ISO/IEC 27001:2022 is the international standard for an Information Security Management System (ISMS). **Who this is for:** founders, IT/security leads, and small teams starting their first ISO 27001 effort and wanting a clear path from zero to audit.

> **Honest note:** a checklist and good templates dramatically speed up the documentation work — but they do not make you certified. Certification is issued only by an accredited certification body after it audits your *operating* ISMS (Stage 1 + Stage 2). Use this as a roadmap, not a guarantee.

Step 1 — Define scope & context (Clause 4)

Scope sets the boundary the auditor measures you against — too broad wastes effort, too narrow risks gaps.

- [ ] Identify internal/external issues relevant to your information security
- [ ] List interested parties (customers, regulators, staff) and their requirements
- [ ] Define the ISMS scope boundary (sites, systems, services, teams) in writing
- [ ] Note any exclusions and the justification for each

Step 2 — Secure leadership & write the ISMS policy (Clause 5)

ISO 27001 requires demonstrable top-management commitment — auditors look for it first.

- [ ] Get documented leadership sign-off and resource commitment
- [ ] Publish a top-level Information Security Policy
- [ ] Assign ISMS roles, responsibilities, and authorities
- [ ] Confirm security objectives align with business goals

Step 3 — Run a risk assessment (Clause 6)

Every control decision and your Statement of Applicability flow from this — it is the engine of the ISMS.

- [ ] Define a repeatable risk assessment methodology (criteria, scoring, acceptance)
- [ ] Identify the risks to confidentiality, integrity, and availability in scope
- [ ] Assess likelihood and impact; rank the risks
- [ ] Record results in a risk register (this feeds the SoA)

Step 4 — Build the risk treatment plan (Clause 6.1.3)

It shows auditors how you will actually reduce each risk and by when.

- [ ] Choose a treatment per risk: mitigate, accept, transfer, or avoid
- [ ] Map each mitigated risk to specific Annex A controls
- [ ] Assign owners and target dates for each action
- [ ] Obtain risk-owner approval for residual and accepted risks

Step 5 — Produce the Statement of Applicability (SoA) (Clause 6.1.3)

The SoA is the single document auditors return to most — it justifies every control in or out.

- [ ] Review all 93 Annex A controls across the 4 themes: Organizational, People, Physical, Technological
- [ ] Mark each control applicable or not — with a written justification
- [ ] Note each control's implementation status
- [ ] Cross-check the SoA against your risk treatment plan for consistency

Step 6 — Implement & document the applicable controls (Clause 8)

Auditors verify controls exist and are evidenced — undocumented work does not count.

- [ ] Write the policies and procedures for each applicable control
- [ ] Operationalize controls (access, backups, logging, supplier security, etc.)
- [ ] Establish records/evidence that controls run as designed
- [ ] Maintain version control and document approval

Step 7 — Train staff & run awareness (Clause 7)

People are a common cause of incidents — competence and awareness are explicit clause requirements.

- [ ] Deliver security awareness training to all in-scope staff
- [ ] Provide role-specific training where needed
- [ ] Keep attendance/competence records as evidence
- [ ] Run reminders (e.g., phishing tests, policy refreshers)

Step 8 — Internal audit + management review (Clause 9)

ISO 27001 requires you to check yourself before the certification body does — skipping this is a common audit failure.

- [ ] Plan and conduct an internal audit of the ISMS against the standard
- [ ] Log findings, nonconformities, and corrective actions
- [ ] Hold a documented management review of performance and risks
- [ ] Close out actions and capture continual-improvement decisions

Step 9 — Certification audit: Stage 1 then Stage 2 (Clause 9 → certification)

This is the only step that produces an actual certificate — and only an accredited certification body can.

- [ ] Select an accredited certification body
- [ ] Stage 1 (documentation review): confirm your ISMS documents and readiness
- [ ] Remediate any Stage 1 gaps
- [ ] Stage 2 (implementation audit): demonstrate the ISMS operating in practice with evidence
- [ ] Address findings; receive the certification decision