CHECKLIST

ISO 27001 Evidence-Request Pack

An auditor's-eye list of the evidence requested per ISMS clause (4–10) and per Annex A theme, with why each artefact is wanted plus a readiness checklist — genericised, no engagement data.

Published by
Compliance Enablers LLP

Last Updated
March 2026

Pages
~10 pages

Introduction

When an ISO/IEC 27001 auditor arrives, they do not ask whether you "have security" — they ask to see the evidence that your Information Security Management System (ISMS) is established, operating, and improving. Knowing exactly what an auditor will request, and having it ready, is the single biggest determinant of a smooth Stage 1 and Stage 2 audit.

This Evidence-Request Pack is a genericised, auditor's-eye list of the artefacts typically requested, organised by ISMS clause (Clauses 4-10 of ISO/IEC 27001:2022) and by Annex A theme. For each item it states the evidence requested and why the auditor wants it. Use it to run an internal readiness check, to brief control owners on what to prepare, and to assemble an evidence pack before Stage 1.

There is no client, audit, or engagement data in this pack. Every item is framework-driven and generic — it describes the kind of artefact an auditor asks for, not any specific organisation's records.

How Auditors Sample Evidence

Auditors work by sampling. They will pick a handful of controls and follow the trail end to end: policy, procedure, evidence of operation, and evidence of review. Strong evidence shares four traits — it is **current** (recently dated), **attributable** (you can show who did it), **complete** (it covers the period under review), and **traceable** (it links back to the requirement or risk it satisfies). As you prepare each item below, test it against those four traits.

Part 1 — ISMS Clauses (4-10)

Clause 4 — Context of the Organization

Evidence Requested	Why the Auditor Wants It
Documented ISMS scope statement	To confirm the boundaries of the ISMS and that they are deliberate and justified
List of interested parties and their requirements	To show you understand who relies on your ISMS and what they expect
Internal and external issues analysis	To demonstrate the ISMS is grounded in your actual context

Clause 5 — Leadership

Evidence Requested	Why the Auditor Wants It
Information security policy approved by top management	To confirm leadership commitment and a mandate for the ISMS
Defined and communicated security roles and responsibilities	To show accountability is assigned, not assumed
Evidence of management engagement (meeting minutes, decisions)	To prove leadership actively directs the ISMS

Clause 6 — Planning

Evidence Requested	Why the Auditor Wants It
Risk assessment methodology and results	To confirm risks are identified and assessed consistently
Risk treatment plan	To show how risks are being addressed and by whom
Statement of Applicability (SoA)	To map every Annex A control to its applicability, justification, and status
Information security objectives and plans to achieve them	To demonstrate the ISMS drives toward measurable goals

Clause 7 — Support

Evidence Requested	Why the Auditor Wants It
Competence and training records	To confirm people doing security work are competent
Awareness programme evidence	To show staff understand their security responsibilities
Documented information control procedure (versioning, approval)	To prove documents are controlled, current, and approved

Clause 8 — Operation

Evidence Requested	Why the Auditor Wants It
Evidence that planned processes are operating	To confirm the ISMS runs in practice, not just on paper
Records of risk assessments performed at planned intervals	To show risk is reassessed as the environment changes
Change management records	To demonstrate changes are controlled and assessed for risk

Clause 9 — Performance Evaluation

Evidence Requested	Why the Auditor Wants It
Monitoring and measurement results (metrics, KPIs)	To show the ISMS effectiveness is measured
Internal audit programme, reports, and findings	To confirm the ISMS is independently checked internally
Management review minutes and outputs	To prove leadership reviews ISMS performance and acts on it

Clause 10 — Improvement

Evidence Requested	Why the Auditor Wants It
Nonconformity and corrective action records	To show issues are tracked to root cause and closure
Evidence of continual improvement	To demonstrate the ISMS gets better over time

Part 2 — Annex A Themes

A.5 Organizational — Sample Evidence Requested

Evidence Requested	Why the Auditor Wants It
Approved suite of security policies and review dates	To confirm policies exist, are approved, and are kept current (A.5.1)
Supplier security assessments and contract security clauses	To show third-party risk is managed (A.5.19-A.5.23)
Incident register with classification and response records	To prove incidents are detected, triaged, and handled (A.5.24-A.5.28)
Business continuity and ICT readiness test results	To demonstrate continuity is planned and exercised (A.5.29-A.5.30)
Records retention and legal/regulatory requirements register	To confirm legal obligations are identified and met (A.5.31-A.5.34)

A.6 People — Sample Evidence Requested

Evidence Requested	Why the Auditor Wants It
Background screening records (metadata, no sensitive PII)	To show new joiners are screened appropriately (A.6.1)
Signed terms of employment and confidentiality agreements	To confirm security obligations are contractual (A.6.2, A.6.6)
Awareness and training completion records	To prove ongoing awareness is delivered and tracked (A.6.3)
Joiner/mover/leaver access change records	To show responsibilities and access change with employment (A.6.5)

A.7 Physical — Sample Evidence Requested

Evidence Requested	Why the Auditor Wants It
Physical access logs and visitor records	To confirm physical entry is controlled (A.7.2)
Clear desk and clear screen policy and checks	To show information is protected in the workplace (A.7.7)
Secure media handling and disposal records	To prove media is protected and disposed of securely (A.7.10, A.7.14)

A.8 Technological — Sample Evidence Requested

Evidence Requested	Why the Auditor Wants It
Access reviews and privileged access records	To confirm access is least-privilege and reviewed (A.8.2-A.8.3)
Multi-factor authentication configuration evidence	To show strong authentication is enforced (A.8.5)
Vulnerability scan and patch management records	To prove vulnerabilities are managed in time (A.8.8)
Backup configuration and restore test evidence	To demonstrate backups exist and are recoverable (A.8.13)
Logging and monitoring configuration and sample logs	To confirm security events are captured and reviewed (A.8.15-A.8.16)
Encryption standards and key management records	To show cryptography is used and managed correctly (A.8.24)
Secure development and code review records	To prove security is built into development (A.8.25-A.8.29)

Building Your Evidence Pack — A Checklist

- [ ] **Assemble Clause 4-10 records** into a single, indexed pack before Stage 1.
- [ ] **Confirm the SoA reconciles** with the risk treatment plan.
- [ ] **Date-stamp every artefact** and remove anything stale or superseded.
- [ ] **Assign an owner** to each evidence item so the auditor can talk to the right person.
- [ ] **Dry-run a sample trail** — pick a control and follow it from policy to operating evidence.
- [ ] **Redact sensitive PII** from screening and personnel evidence; provide metadata only.
- [ ] **Capture the period of operation**, not just a point-in-time snapshot.

How the Platform Supports Audit Readiness

The Compliance Enablers platform keeps your evidence audit-ready by linking each Annex A control and ISMS clause to the live artefacts that prove it — policies, access reviews, backup restore tests, incident records, and training completion — with version history and ownership built in. Evidence is reusable across frameworks, so the same artefact satisfies ISO 27001, SOC 2, and other standards at once. An auditor portal lets you grant scoped, redacted access without handing over the whole system. Sage, our AI assistant built on Anthropic Claude with every interaction disclosed and audited, can pre-check evidence freshness and flag gaps for human review ahead of Stage 1 — so you walk into the audit knowing exactly what the auditor will find.