ISO 27001 Checklist:

UK Audit Prep by Clause and Evidence Type

An ISO 27001 checklist helps UK organisations prepare for audits by mapping ISO/IEC 27001 clauses to the evidence a certification body is likely to sample. It also groups evidence by type so you can prepare both documented information and operational records.

Use this as an audit prep guide, not a “tick-box” substitute for risk-based decisions in your ISMS.

SURECLOUD®

GDPR Compliant

teiss Awards Winner Best Security Compliance Product

ISO 27001 Checklist Contents

How to Use This ISO 27001 Checklist

Use this checklist to confirm two things before an audit:

- Required documented information exists, is approved, and is controlled
- There is recent evidence showing the ISMS and controls operate in practice

Auditors assess effectiveness over time, not just whether documents exist. Work clause by clause, assign an owner, and gather evidence in one place. If something exists but you cannot show recent records (tickets, logs, minutes, reviews), treat it as a gap and fix it before the audit.

ISO 27001 Clause 4: Context of the Organisation

This section checks that your ISMS scope and business context are clear and consistent.

Checklist items:

- [ ] Define the ISMS scope (services, systems, locations, data types, key suppliers)
- [ ] Identify interested parties and relevant requirements
- [ ] Describe boundaries and interfaces (shared platforms, group functions, outsourced services)

Typical evidence auditors expect:

- Approved ISMS scope statement (current, version-controlled)
- Interested parties/context analysis updated when the business changes
- High-level service or process maps showing dependencies and interfaces

ISO 27001 Clause 5: Leadership

This section checks that leadership ownership is visible and evidenced.

Checklist items:

- [ ] Information security policy approved and communicated
- [ ] Roles, responsibilities, and authorities defined (including risk ownership)
- [ ] Evidence of leadership commitment to objectives, resources, and oversight

Typical evidence auditors expect:

- Approved policy plus communication record
- Role definitions (ISMS owner, risk owners, control owners)
- Records of leadership decisions (priorities, resourcing, risk acceptance

ISO 27001 Clause 6: Planning

This section checks that your risk-based approach is documented and traceable.

Checklist items:

- [ ] Risk assessment method defined and applied
- [ ] Risk treatment plan produced and maintained
- [ ] Statement of Applicability (SoA) completed and aligned to scope

Typical evidence auditors expect:

- Risk assessment methodology and scoring criteria
- Current risk register covering the ISMS scope
- Risk treatment plan with owners and target dates
- SoA listing Annex A controls, applicability, and justified exclusions

ISO 27001 Clause 7: Support

This section checks that competence, awareness, and document control support the ISMS.

Checklist items:

- [ ] Competence needs identified for in-scope roles
- [ ] Training and awareness delivered and tracked
- [ ] Document control in place (approval, versioning, access, retention)

Typical evidence auditors expect:

- Training completion reports and role-based training records
- Awareness materials or communications
- Document index plus examples showing approvals and version control
- Evidence staff can access current documents when needed

ISO 27001 Clause 8: Operation

This section checks that controls run as working processes and generate records.

Checklist items:

- [ ] Controls implemented per SoA and risk treatment plan
- [ ] Operating procedures exist for key activities (access, change, backup, supplier checks)
- [ ] Evidence produced through normal work, not audit-only effort

Typical evidence auditors expect:

- Tickets, approvals, and review outputs
- Logs or monitoring records, where relevant to scope
- Supplier checks and contract clauses, where applicable
- Incident records and follow-up actions

SO 27001 Clause 9: Performance Evaluation

This section checks that you monitor, audit, and review ISMS performance.

Checklist items:

- [ ] Internal audit programme defined and delivered
- [ ] Management review carried out with tracked outputs

Typical evidence auditors expect:

- Internal audit plan, reports, and follow-up actions
- Sampling approach and independence, where feasible
- Management review minutes covering risks, incidents, audit results, metrics
- Decisions and actions with owners and due dates

ISO 27001 Clause 10: Improvement

This checklist section confirms issues are recorded, corrected, and followed through so the ISMS improves over time.

Checklist items:

- [ ] Nonconformities recorded, assessed, and corrected
- [ ] Corrective actions tracked and verified as effective

Typical evidence auditors expect:

- Nonconformity and corrective action procedure (documented and used)
- Corrective action log with root cause, actions, owners, and deadlines
- Evidence actions were completed and checked for effectiveness
- Corrective actions raised from incidents (where applicable) and tracked to closure

Annex A Controls: Evidence Types at a Glance

This section helps organise Annex A evidence so auditors can sample efficiently.

Policy evidence:

- Approved policies, standards, or procedures mapped to SoA items

Technical evidence:

- Configuration outputs or reports (for example: MFA status or backup jobs)
- Screenshots are used sparingly and supported by records over time

Operational evidence:

- Tickets, approvals, registers, review notes, minutes, or trackers showing routine operation
- Recurring proof, such as access reviews, supplier reviews, or incident reviews

Key Takeaways: ISO 27001 Audit Checklist Summary

- An ISO 27001 checklist works best when it maps clauses to specific evidence
- Auditors sample both documents and operating records over time
- Clause 6 links scope, risks, controls, and the SoA, and auditors often treat it as central to audit readiness
- Clause 8 depends on repeatable processes that generate records through normal work
- Clauses 9 and 10 show the ISMS is monitored, reviewed, and improved

FAQs

Is an ISO 27001 checklist mandatory?

No. ISO/IEC 27001 requires an effective Information Security Management System (ISMS) and evidence that it operates, but it does not require a specific checklist format. A checklist is useful because it provides a structured way to confirm clause coverage and gather evidence. It should support risk-based decisions rather than replace them.

Do auditors use checklists?

Yes. Auditors often use structured audit plans or checklists to ensure they consistently cover ISO 27001 clauses and sample the right areas of the ISMS. Certification bodies, typically accredited by UKAS, will still rely on sampling and judgement. Evidence must be recent, traceable to scope and risks, and consistent over time.

Can a checklist guarantee audit success?

No. A checklist can improve audit readiness, but it cannot guarantee a pass. Certification audits focus on effectiveness: whether the ISMS works in practice for the defined scope, and whether controls produce consistent, usable evidence over time. A checklist may highlight obvious gaps, but it cannot compensate for controls that are not operating or records that are missing or inconsistent.

How often should an ISO 27001 checklist be reviewed?

Review it regularly, based on where you are in the ISMS cycle. During implementation, review it monthly or at key milestones to make sure evidence is building and ownership is clear. Before Stage 1 and Stage 2 audits, review it again to confirm recent records exist and match the scope, risks, and SoA. After certification, review it at least annually and after material changes (new services, major system changes, supplier changes, or significant incidents) so evidence stays current.

For more information on how SureCloud can assist your organization, visit us online at **www.surecloud.com**, or email **sales@surecloud.com**

SureCloud Summary

SureCloud Ltd. has two decades of experience as a leading provider of Governance, Risk, and Compliance (GRC) solutions since its founding in 2006. Headquartered in the UK, with offices in the US, SureCloud supports a global portfolio of organisations with its holistic and intelligent GRC platform. Whether addressing cyber risk, data privacy, third parties, or compliance demands, SureCloud has a proven record of empowering organisations to continuously identify, manage and automate their risk and regulatory alignment.

Corporate Headquarters 1 Sherwood Street, London, W1D 7HR