ISO 27001 Audit Readiness Checklist

A practical guide to prepare documentation, evidence, and governance records for an ISO/IEC 27001 audit.

1. Introduction

1.1 Why ISO 27001 audit preparation matters

ISO/IEC 27001 audit preparation matters because certification is not only about having information security documents in place. Auditors look for evidence that the Information Security Management System, or ISMS, is defined, implemented, monitored, reviewed, and improved in practice. A policy that exists but is not communicated, followed, or reviewed may still result in a nonconformity.

Strong preparation helps the organization reduce audit stress, avoid last-minute evidence collection, and demonstrate that information security is managed as a business process. It also helps leadership understand whether risks are being treated effectively and whether controls are operating as intended.

- **For leadership:** audit readiness provides confidence that information security risks are visible, owned, and controlled.
- **For security teams:** it confirms that procedures, logs, reviews, and tickets are available as audit evidence.
- **For customers and partners:** certification can demonstrate a mature approach to protecting information.
- **For auditors:** clear records make it easier to verify conformance without unnecessary delays.

Example: If an organization states that privileged access is reviewed quarterly, the auditor may ask for the latest access review record, reviewer name, review date, exceptions found, and evidence that exceptions were resolved. The readiness task is not just to write the access review procedure, but to show that the review actually happened.

1.2 How to use this checklist

Use this checklist as a working audit preparation tool. For each item, confirm whether the document exists, whether it is approved, whether it reflects current practice, and whether supporting evidence is available. Mark each item as complete, partial, or not started, then assign an owner and target date for open gaps.

- **Step 1:** Confirm the ISMS scope and applicable business units, locations, systems, services, and third parties.
- **Step 2:** Collect mandatory documents and key evidence records.
- **Step 3:** Check whether each document is approved, version-controlled, and communicated where relevant.
- **Step 4:** Match evidence to audit questions before the external auditor arrives.
- **Step 5:** Track gaps through corrective actions and management review.

Practical tip: Create an evidence folder or audit tracker with columns for requirement, document name, evidence location, owner, status, and comments. This makes Stage 1 documentation review and Stage 2 evidence testing easier to manage.

2. ISMS Documentation Checklist

The following documentation checklist focuses on the core ISMS records that auditors commonly review. The goal is to ensure that documents are not only created, but also approved, current, aligned with the ISMS scope, and supported by evidence of operation.

2.1 Information security policy and objectives

The information security policy sets the direction for the ISMS. It should be approved by top management, communicated to employees and relevant external parties, and reviewed at planned intervals. The policy should connect information security to business priorities such as customer trust, regulatory compliance, service continuity, and protection of confidential information.

- Confirm that the policy has an owner, approval date, version number, and review cycle.
- Check whether the policy is available to employees, such as through an intranet, employee handbook, or onboarding pack.
- Ensure information security objectives are measurable and linked to risk or business priorities.
- Verify that objectives are monitored, reviewed, and updated when business or risk conditions change.

Example objectives: Complete quarterly access reviews for all critical applications; reduce overdue security awareness training to less than 5%; resolve critical vulnerabilities within the agreed service level; complete supplier security reviews for all high-risk vendors before contract renewal.

Example objectives: Complete quarterly access reviews for all critical applications; reduce overdue security awareness training to less than 5%; resolve critical vulnerabilities within the agreed service level; complete supplier security reviews for all high-risk vendors before contract renewal.

2.2 Risk assessment methodology and risk register

The risk assessment methodology explains how the organization identifies, analyzes, evaluates, and prioritizes information security risks. It should be repeatable, consistent, and clearly linked to the ISMS scope. The risk register then records the actual risks, risk owners, likelihood, impact, treatment decisions, target dates, and current status.

- Confirm that the methodology defines risk criteria, scoring scales, likelihood, impact, and acceptance thresholds.
- Check whether the risk register includes assets, threats, vulnerabilities, consequences, inherent risk, treatment option, residual risk, and risk owner.
- Verify that risks are reviewed at planned intervals and when significant changes occur.
- Ensure each high or unacceptable risk has a documented treatment plan and accountable owner.

Example: A risk entry may state that customer data stored in a cloud application could be exposed due to weak administrative access controls. The treatment may include enforcing multifactor authentication, quarterly privileged access reviews, and logging of administrator activity. The auditor will expect the register, treatment plan, and evidence of control operation to be consistent.

2.3 Statement of Applicability (SoA)

The Statement of Applicability, or SoA, is a key ISMS document because it connects risk treatment decisions to the selected information security controls. It should explain which Annex A controls are applicable, which are not applicable, the justification for each decision, and the implementation status of applicable controls.

- Confirm that the SoA covers all ISO/IEC 27001:2022 Annex A controls.
- Check that every included control has a clear reason, such as risk treatment, legal requirement, contractual obligation, or business need.
- Check that every excluded control has a documented and defensible justification.
- Verify that the implementation status is accurate and supported by evidence.
- Ensure the SoA aligns with the risk register, risk treatment plan, and implemented policies.

Example: If supplier security is marked as applicable, the SoA should link to supplier risk procedures, due diligence records, contract security clauses, and evidence of supplier reviews. If a physical security control is excluded because the organization is

fully remote and has no managed office premises, the justification should be specific and approved.

2.4 Internal audit reports

Internal audits provide independent assurance that the ISMS conforms to planned arrangements and is operating effectively. The audit programme should cover relevant ISO clauses, Annex A controls, business processes, locations, systems, and previous nonconformities. Internal audit results should be reported to management and used to drive corrective action.

- Confirm that an internal audit programme or schedule exists.
- Check whether auditors are objective and independent of the areas they audit where practical.
- Verify that audit reports include scope, criteria, date, auditor, auditees, findings, evidence reviewed, and conclusions.
- Ensure nonconformities and observations are tracked through corrective action records.
- Confirm that repeat findings are escalated to management review.

Example: An internal audit of access control may sample new joiners, movers, leavers, privileged users, and terminated employees. Evidence may include approval tickets, access review reports, HR termination dates, system screenshots, and exception remediation records.

2.5 Management review records

Management review records show that top management reviews the continuing suitability, adequacy, and effectiveness of the ISMS. These records should demonstrate that leadership considers audit results, risk status, security objectives, incidents, supplier issues, resource needs, opportunities for improvement, and changes affecting the ISMS.

- Confirm that management reviews are conducted at planned intervals.
- Check whether meeting minutes include agenda items, inputs reviewed, decisions made, action owners, and due dates.
- Verify that information security objectives and performance metrics are reviewed.
- Ensure risk treatment progress, internal audit findings, incidents, and corrective actions are discussed.
- Confirm that outputs include improvement actions, resource decisions, and changes needed to the ISMS.

3. Process Readiness Checklist

Process readiness confirms that ISO 27001 controls are not only documented but also operating in day-to-day business activities. Auditors usually test whether access reviews, asset ownership, supplier reviews, awareness training, business continuity, and incident response processes are performed consistently and supported by records.

3.1 Access control reviews

Access control reviews help confirm that users have only the access they need for their current role. The organization should be able to show how access is requested, approved, changed, reviewed, and removed. Reviews should cover employees, contractors, administrators, service accounts, and third-party users where applicable.

- Confirm that access review frequency is defined for critical systems.
- Check whether access rights are approved by business or system owners.
- Verify joiner, mover, and leaver activity against HR records and access tickets.
- Review privileged access separately because it carries higher risk.
- Ensure access review exceptions are tracked through remediation.

Example: For a finance application, the auditor may sample five users and ask why each user has access, who approved it, when it was last reviewed, and whether any terminated user accounts remain active.

3.2 Asset management

Asset management gives the organization visibility over information, systems, devices, applications, cloud services, and other associated assets that need protection. Each important asset should have an owner, classification, acceptable use rules, and a basic handling or protection approach.

- Confirm that the asset inventory is current and aligned with the ISMS scope.
- Check whether each critical asset has an assigned owner.
- Verify that assets are classified based on confidentiality, integrity, availability, or business criticality.
- Review whether asset changes, disposals, and returns are recorded.
- Ensure cloud services and externally hosted systems are included where relevant.

Example: A customer database should appear in the asset register with its business owner, hosting location, data classification, backup requirement, linked risk entries, and access control owner.

3.3 Supplier and third-party risk management

Supplier and third-party risk management ensures that external providers are assessed before and during their engagement. This includes cloud providers, outsourced IT support, payroll processors, data hosting platforms, consultants, and any supplier that stores, processes, or accesses sensitive information.

- Confirm that high-risk suppliers are identified and assessed before onboarding.
- Check whether supplier contracts include information security, confidentiality, incident notification, and right-to-audit clauses where applicable.
- Verify that supplier reviews are performed at defined intervals.
- Ensure supplier incidents, service changes, and performance issues are tracked.
- Maintain evidence of due diligence, such as questionnaires, certifications, security reports, or risk approvals.

Example: Before using a new cloud-based HR platform, the organization should review how employee data is protected, where it is hosted, whether encryption is used, how incidents are reported, and whether the supplier has relevant assurance reports or certifications.

3.4 Security awareness training

Security awareness training helps ensure that employees and contractors understand their responsibilities for protecting information. Training should be relevant to the role, refreshed at planned intervals, and supported by completion records. It should cover common risks such as phishing, password hygiene, data handling, incident reporting, remote working, and acceptable use.

Audit checks: Confirm onboarding training, annual refresher completion, role-specific awareness, overdue training follow-up, and evidence that training content is reviewed and updated.

- Confirm that new employees complete security awareness during onboarding.
- Check whether annual refresher training is tracked and overdue completions are followed up.
- Verify that role-specific training is provided for privileged users, developers, service desk teams, and data handlers.
- Review phishing simulation or awareness campaign results if used.
- Ensure training content reflects current threats and company policies.

3.5 Business continuity and incident response

Business continuity and incident response readiness shows that the organization can continue critical activities, recover important systems, and respond to security incidents in a controlled way. Auditors will look for documented plans, assigned roles, tested procedures, incident records, lessons learned, and corrective actions from exercises or real events.

Business continuity and incident response readiness shows that the organization can continue critical activities, recover important systems, and respond to security incidents in a controlled way. Auditors will look for documented plans, assigned roles, tested procedures, incident records, lessons learned, and corrective actions from exercises or real events.

4. Evidence Readiness Checklist

Evidence readiness means being able to prove that the ISMS is working in practice. Auditors will usually sample records, ask control owners to explain their processes, and compare evidence against policies, risk treatment plans, and the Statement of Applicability.

4.1 Evidence for implemented controls

For each applicable control, collect evidence that shows the control is designed, implemented, and operating. Evidence should be mapped to the relevant ISO clause, Annex A control, risk, policy, and control owner.

- Maintain a control evidence tracker with control name, evidence type, owner, frequency, and storage location.
- Use current evidence rather than outdated screenshots or old reports.
- Check that evidence supports actual operation, not just design intent.
- Link evidence to the SoA and risk treatment plan where relevant.

Example: If multifactor authentication is listed as an implemented control, evidence may include configuration screenshots, identity provider settings, access policy rules, exception approvals, and logs showing successful MFA enforcement.

4.2 Records and logs

Records and logs provide time-based proof that activities happened. They can include access logs, backup logs, vulnerability scan results, incident tickets, training completion records, supplier review files, change approvals, and monitoring alerts.

- Confirm that logs are retained for the required period.
- Check that records are complete, readable, and attributable to a person, system, or process.
- Protect audit evidence from unauthorized modification or deletion.
- Ensure logs are reviewed when the policy says they should be reviewed.

4.3 Review and testing records

Review and testing records show that controls are checked for effectiveness. These records may include internal audit results, access review sign-offs, disaster recovery tests, incident response exercises, tabletop exercise notes, supplier reassessments, and vulnerability remediation reviews.

Audit checks: Keep records of control reviews, test dates, participants, results, exceptions, and follow-up actions. Confirm that testing follows the frequency defined in policies, and track failed tests through corrective action records.

Example: A disaster recovery test record should show the tested system, test scenario, recovery target, actual recovery result, issues found, owner of each issue, and target date for remediation.

4.4 Assigned owners and responsibilities

Control ownership is essential for audit readiness. Each policy, risk, control, system, supplier, and corrective action should have a named owner who understands their responsibility and can explain how the related process works.

- Confirm that owners are named individuals or roles with clear accountability.
- Check whether owners understand required evidence and review frequency.
- Ensure responsibilities are updated when people change roles.
- Map each high-risk area to a responsible business or technical owner.

5. Common Audit Gaps to Check

Common audit gaps usually appear when documentation, evidence, and actual practice are not aligned. Before the audit, review these areas carefully and treat any weakness as a remediation item with an owner and due date.

5.1 Outdated risk assessments

Risk assessments become weak when they are not reviewed after major business, technology, supplier, or threat changes. An outdated risk register may not reflect new cloud services, new customer requirements, new systems, or recent incidents.

Check before audit: Confirm that risks have recent review dates, current owners, updated treatment status, and clear links to business changes.

5.2 Missing links between risks and controls

A common gap is treating the risk register, Statement of Applicability, and control evidence as separate documents. Auditors expect a clear chain from risk to treatment decision, selected control, implementation evidence, and residual risk acceptance.

Example: If the risk is unauthorized access to financial records, the linked controls may include access approval, periodic access reviews, MFA, logging, and privileged access monitoring.

- Keep records of control reviews, test dates, participants, results, exceptions, and follow-up actions.

- Confirm that tests are performed at the frequency defined in policies or procedures.
- Track failed tests or weaknesses through corrective action records.
- Use test results to update risk assessments, procedures, and training where needed.

5.3 Incomplete internal audits

Incomplete internal audits occur when the audit is too narrow, evidence is not sampled properly, or findings are not documented clearly. An internal audit should cover both management system requirements and selected operational controls, not just confirm that documents exist.

- Confirm that the audit programme covers ISO clauses, Annex A controls, locations, processes, and previous findings.
- Check that the audit report records evidence reviewed, samples tested, findings, conclusions, and responsible owners.
- Ensure internal audit findings are transferred into corrective action tracking.
- Verify that management reviews discuss significant or repeated audit findings.

Example: If access control is audited, the internal audit should test a sample of access requests, leaver records, privileged users, and review sign-offs. A statement such as "access control reviewed" is not enough unless it is supported by sampled evidence.

5.4 Weak corrective actions

Weak corrective actions happen when teams correct the immediate issue but do not remove the root cause. Auditors often expect to see the full corrective action trail: problem identified, containment action, root-cause analysis, corrective action, owner, due date, implementation evidence, and effectiveness review.

- Avoid closing findings with only “training completed” unless training clearly addresses the root cause.
- Use root-cause techniques such as 5 Whys for significant nonconformities.
- Assign clear owners and realistic due dates for each action.
- Verify effectiveness after implementation, such as by retesting the control or reviewing later records.

Example: If several users missed mandatory security training, the root cause may not be employee negligence. It may be that HR onboarding does not trigger training automatically, managers do not receive overdue reports, or the learning system does not escalate reminders.

5.5 Policies that do not match actual practices

Policies create audit risk when they describe controls that are not actually performed. A policy may say that logs are reviewed weekly, access is reviewed quarterly, suppliers are reassessed annually, or backups are tested monthly. If the organization cannot show evidence for those activities, the policy becomes a source of nonconformity.

- Compare each policy requirement with available operating evidence.
- Update policies where wording is unrealistic, outdated, or inconsistent with current processes.
- Do not overpromise control frequency unless the team can consistently meet it.
- Make sure process owners understand the policy obligations they are expected to perform.

6. Internal Audit Preparation

Internal audit preparation is the organization's opportunity to test the ISMS before an external auditor does. It should not be treated as a paperwork exercise. A useful internal audit reviews documents, samples real evidence, interviews process owners, records clear findings, and confirms that corrective actions are tracked to closure.

6.1 Review documentation

Start by reviewing the core ISMS documents against the audit scope and ISO 27001 requirements. The review should confirm that documents are current, approved, version-controlled, consistent with one another, and aligned with the way teams actually work.

- Check the ISMS scope, information security policy, risk assessment, risk treatment plan, and Statement of Applicability.
- Review internal audit reports, management review minutes, corrective action logs, and evidence trackers.
- Look for inconsistencies between policies, procedures, risk records, and actual evidence.
- Confirm that obsolete documents are removed or clearly marked as superseded.

6.2 Sample real evidence

Sampling real evidence helps confirm that controls operate consistently over time. Instead of accepting a process owner's statement that a control is performed, the

internal auditor should test records from the audit period and check whether they support the documented process.

Example: For access management, sample a few joiner requests, leaver records, privileged access approvals, and quarterly access review sign-offs. The sample should show who requested access, who approved it, when it was reviewed, and whether exceptions were resolved.

- Select samples from different dates, teams, systems, and risk levels.
- Test whether evidence matches the policy frequency and approval requirements.
- Record any missing, incomplete, or inconsistent evidence as a potential finding.
- Use sampling results to identify systemic weaknesses, not only isolated mistakes.

6.3 Interview relevant employees

Interviews help confirm whether employees understand their responsibilities and whether practice matches documentation. Interviewees may include risk owners, system owners, HR, IT operations, security, procurement, service desk, incident response leads, and business process owners.

- Ask employees to explain the process in their own words.
- Confirm whether they know where policies, procedures, and reporting channels are located.

- Check whether control owners understand what evidence they must retain.
- Do not coach employees to give scripted answers; prepare them to explain real work clearly.

6.4 Record findings

Findings should be written clearly and linked to evidence. A good finding states the requirement, the condition observed, the evidence reviewed, the risk or impact, and whether the issue is a nonconformity, observation, or improvement opportunity.

Example finding: The access control procedure requires quarterly privileged access reviews, but no review evidence was available for the finance application for the last quarter. This creates a risk that inappropriate privileged access may remain undetected.

6.5 Track corrective actions

Corrective actions should be tracked from identification to closure. Each action should include the finding, root cause, planned action, owner, due date, implementation evidence, and effectiveness check.

- Assign one accountable owner for each corrective action.
- Set realistic due dates and review overdue actions regularly.
- Verify that the action fixes the root cause, not only the immediate symptom.
- Retest the control or review later records before closing significant findings.

7. Final Pre-Audit Review

The final pre-audit review is the last readiness checkpoint before the external audit. It confirms that documentation, evidence, control testing, gap closure, and team preparation are complete enough for a confident audit discussion.

7.1 Documentation complete

Confirm that all required ISMS documents are available, approved, version-controlled, and aligned with the audit scope. The documentation set should include the ISMS scope, policies, risk methodology, risk register, SoA, internal audit records, management review records, and corrective action records.

7.2 Controls tested

Review whether key controls have been tested or reviewed during the audit period. Priority should be given to high-risk controls such as access management, backup restoration, incident response, vulnerability management, supplier reviews, and security awareness completion.

7.3 Evidence available

Make sure evidence is organized and easy to retrieve. The audit team should be able to locate sample records quickly, explain what each record proves, and show how it links to the relevant risk, control, or policy requirement.

7.4 Gaps addressed

Before the audit, review all open gaps and confirm whether they are closed, accepted with justification, or actively being remediated. For unresolved items, maintain a clear action plan with owner, due date, current status, and risk-based priority.

7.5 Team prepared for auditor interviews

Prepare relevant employees by explaining the audit purpose, likely topics, documents they own, and evidence they may need to show. The goal is not to script answers, but to help employees answer accurately, calmly, and consistently with actual practice.

- Brief process owners on their roles, responsibilities, and evidence locations.
- Remind employees to answer only what is asked and avoid guessing.
- Confirm who will coordinate evidence requests during the audit.
- Prepare a list of key contacts for security, IT, HR, procurement, legal, and business operations.

Conclusion

ISO 27001 audit readiness is strongest when documentation, evidence, ownership, and daily practice tell the same story. A well-prepared organization can show not only that policies exist, but that risks are known, controls are operating, reviews are performed, incidents are managed, and improvements are tracked. Use this checklist as a living tool before internal audits, certification audits, surveillance audits, and management reviews. The real measure of readiness is whether the ISMS can be explained and evidenced without last-minute reconstruction.

GSDC
Global Skill Development Council

CERTIFIED ISO 27001:2022 LEAD AUDITOR

ISO 27001 LEAD AUDITOR CERTIFICATION IS BASED ON INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) AND GLOBAL COMPLIANCE STANDARDS

ABOUT GSDC CERTIFICATION

EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.

CREATED BY EXPERTS

GSDC certifications are created and authored by world's leading experts in the field.

EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.

LEARNING MATERIALS

Get access to learning materials such as videos, ebooks, templates, and practice exams, which will help you clear the certification exam.

LEARNING OBJECTIVE

- Verify adherence to legal and regulatory requirements
- Provide recommendations for enhancing ISMS
- Ensure continuous improvement of security practices
- Foster a culture of risk management awareness

Enroll now with the code **LEARN20** To avail **20%** discount

Enroll Now

www.gsdcouncil.org