

40 ISO 27001 Interview Questions & Answers

**A practical preparation guide for information-security professionals
and aspiring ISO 27001 lead auditors.**

Fundamentals • Requirements and controls • Risk assessment • Auditing •
Nonconformities • Scenario-based questions • ISO 27001:2022 • Lead auditor careers

How to use this guide

Use the sample answers to structure your own responses rather than memorize them word for word. Where possible, connect concepts to real examples from your work, training, or practice audits. For scenario questions, explain the evidence you would seek, the requirement you would assess, and how you would document your conclusion.

1. ISO 27001 Fundamentals

Q1. What is ISO 27001, and why is it important?

Sample answer: ISO/IEC 27001 is an international standard that specifies requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). It helps an organization manage information-security risks systematically and protect the confidentiality, integrity, and availability of information. It also provides a structured basis for demonstrating that information security is managed and continually reviewed.

Q2. What is an Information Security Management System (ISMS)?

Sample answer: An ISMS is a coordinated set of policies, processes, responsibilities, and controls used to manage information-security risks. It connects risk assessment and treatment with leadership, staff awareness, operational processes, monitoring, audits, and continual improvement. An ISMS is not just a collection of IT tools; it is a management system that covers people, processes, and technology.

Q3. What are the main objectives of ISO 27001?

Sample answer: The main objective is to help an organization manage information-security risks in a consistent, risk-based way. Common goals include protecting confidentiality, integrity, and availability; meeting applicable legal, regulatory, and contractual obligations; clarifying responsibilities; improving resilience; and continually

improving security practices. The specific objectives should reflect the organization's context and business needs.

Q4. What are the key requirements of ISO 27001:2022?

Sample answer: Clauses 4–10 address organizational context, leadership, planning, support, operation, performance evaluation, and improvement. Together, they require an organization to define its ISMS scope, assess and treat risks, establish policies and objectives, provide resources and competence, operate planned processes, evaluate performance, conduct internal audits and management reviews, and address nonconformities. Annex A provides a reference set of security controls to consider through risk treatment.

Q5. What are the benefits of ISO 27001 certification for an organization?

Sample answer: Certification can provide independent evidence that an organization's ISMS has been assessed against ISO/IEC 27001 requirements. It may strengthen customer and partner confidence, support supplier assurance, improve risk visibility, clarify accountability, and encourage continual improvement. Certification does not guarantee that breaches will never occur; its value depends on the effectiveness and ongoing operation of the ISMS.

2. Requirements and Security Controls

Q6. What are Clauses 4 to 10 of ISO 27001?

Sample answer: Clause 4 covers context of the organization; Clause 5, leadership; Clause 6, planning; Clause 7, support; Clause 8, operation; Clause 9, performance evaluation; and Clause 10, improvement. In an interview, explain how these clauses work together: understand the organization and its risks, establish direction and plans, provide support, operate the ISMS, check whether it works, and improve it.

Q7. What is Annex A in ISO 27001:2022?

Sample answer: Annex A is a reference set of information-security controls used when determining risk treatment. The organization selects controls based on its risk assessment, risk-treatment decisions, and applicable requirements. Controls that are included or excluded, along with the rationale and implementation status, are documented in the Statement of Applicability. Annex A should not be treated as a checklist where every control automatically applies to every organization.

Q8. What are the four themes of ISO 27001:2022 Annex A controls?

Sample answer: The 2022 edition groups its 93 Annex A controls into four themes: Organizational, People, Physical, and Technological. These themes organize controls ranging from policies and supplier relationships to awareness, physical protection, access management, and technical safeguards. The organization determines which controls are appropriate for its risks and obligations.

Q9. What is the difference between ISO 27001 requirements and security controls?

Sample answer: Requirements in the main clauses define what the organization must establish and operate in its ISMS. Security controls are measures used to modify or manage risks. Annex A provides a reference set of controls, but control selection should be justified through risk treatment and other applicable requirements. A control may be technical, physical, organizational, or people-focused.

Q10. What is a Statement of Applicability (SoA), and why is it important?

Sample answer: The Statement of Applicability records the necessary controls, why they are included, whether they are implemented, and the justification for excluding Annex A controls where applicable. It connects risk treatment decisions to control selection and gives auditors a structured way to review the organization's control rationale and status. It should remain consistent with the risk assessment and risk-treatment plan.

3. Risk Assessment and Risk Treatment

Q11. What is an information-security risk assessment?

Sample answer: It is a structured process for identifying information-security risks and analyzing and evaluating them against defined criteria. The organization identifies relevant assets, threats, vulnerabilities, potential consequences, and likelihood, then prioritizes risks. The method and acceptance criteria should be defined and applied consistently so results can guide risk treatment and later reviews.

Q12. What is the difference between risk assessment and risk treatment?

Sample answer: Risk assessment identifies, analyzes, and evaluates risks. Risk treatment decides what to do about risks that need action and selects appropriate measures. Treatment options commonly include modifying a risk through controls, avoiding the activity that creates it, sharing or transferring some consequences, or accepting it under authorized criteria. The decisions and residual risks should be documented.

Q13. How do you identify and evaluate information-security risks?

Sample answer: First define the assessment scope, method, and risk criteria. Identify information assets and processes, relevant threats and vulnerabilities, and possible impacts. Estimate likelihood and consequence using the organization's approved method, compare results with acceptance criteria, and prioritize the risks. Involve asset owners and relevant stakeholders, document assumptions, and review the assessment when material changes occur.

Q14. What is a risk register, and what information does it contain?

Sample answer: A risk register is a record used to track identified risks and their management. Depending on the organization's method, it may include a risk ID and description, affected assets or processes, threat and vulnerability information, likelihood, impact, risk rating, owner, treatment decision, planned actions, due dates, and residual risk. It should be kept current and linked to risk-treatment decisions.

Q15. What are the different options for treating information-security risks?

Sample answer: Common options are to modify the risk by applying controls, avoid the risk by discontinuing the relevant activity, share or transfer some risk through arrangements such as insurance or outsourcing, or retain the risk with appropriate authorization. The choice should reflect risk evaluation, business context, obligations, and the organization's risk-acceptance criteria. Outsourcing does not remove all accountability for managing risk.

4. ISO 27001 Auditing Fundamentals

Q16. What is an ISO 27001 audit?

Sample answer: An ISO 27001 audit is a systematic, evidence-based evaluation of whether the ISMS conforms to specified requirements and is effectively implemented within the audit scope. Auditors use methods such as interviews, document and record review, observation, and sampling. Findings should be traceable to objective evidence and relevant audit criteria.

Q17. What is the difference between an internal audit and an external audit?

Sample answer: An internal audit is arranged by or for the organization to evaluate its ISMS and identify opportunities for correction and improvement. An external audit is performed by an independent external party. Certification audits are conducted by a certification body to determine whether the organization meets certification requirements. The exact purpose, independence arrangements, and reporting expectations depend on the audit type.

Q18. What are the main stages of an ISO 27001 certification audit?

Sample answer: Certification commonly involves a Stage 1 review of readiness, documented information, scope, and understanding of the ISMS, followed by a Stage 2 assessment of implementation and effectiveness. The certification body evaluates findings before making a certification decision. After certification, surveillance audits and

recertification activities take place according to the certification cycle and applicable rules.

Q19. What evidence does an ISO 27001 auditor collect during an audit?

Sample answer: Evidence may include policies, risk assessments, risk-treatment plans, the Statement of Applicability, access reviews, training records, incident records, internal-audit results, management-review minutes, corrective-action records, and observations of processes or systems. Evidence should be relevant, sufficient for the audit objective, and verifiable. Auditors should record how evidence supports each finding and respect confidentiality requirements.

Q20. What are the roles and responsibilities of an ISO 27001 lead auditor?

Sample answer: A lead auditor plans and coordinates the audit, confirms scope and criteria, assigns work, leads the audit team, communicates with the auditee, evaluates evidence, and ensures findings are clear and supported. The lead auditor also manages meetings, reports results, and follows the applicable process for closing the audit. Auditors should remain objective, protect confidential information, and avoid auditing beyond their competence.

5. Nonconformities and Corrective Actions

Q21. What is a nonconformity in ISO 27001?

Sample answer: A nonconformity is the failure to meet a requirement. It may involve a requirement of ISO/IEC 27001, the organization's own ISMS arrangements, or another applicable audit criterion. A sound finding states the requirement, the objective evidence, and the gap between them. The auditor should avoid unsupported assumptions and explain the issue clearly.

Q22. What is the difference between a major and a minor nonconformity?

Sample answer: Certification bodies use defined rules to classify findings. Broadly, a major nonconformity indicates a failure that significantly affects the ISMS's ability to achieve intended outcomes, while a minor nonconformity is a more limited failure that does not amount to a major breakdown. Exact classification must follow the certification body's applicable procedures; auditors should not rely only on the apparent size of a single issue.

Q23. How should an auditor document and report a nonconformity?

Sample answer: The auditor should identify the applicable requirement, record clear and verifiable evidence, describe the gap, and explain the finding in precise, neutral language. The finding should be discussed with the auditee to confirm factual accuracy, without negotiating away evidence-based conclusions. The report should follow the audit process and make the issue understandable to those responsible for corrective action.

Q24. What is root cause analysis, and how is it used in corrective action?

Sample answer: Root cause analysis looks beyond the immediate symptom to identify why a nonconformity occurred. Techniques may include asking “why” repeatedly, process mapping, or cause-and-effect analysis. Corrective action should address the underlying cause, not just fix the individual instance. The organization should determine whether similar issues exist elsewhere and retain evidence of actions taken.

Q25. How does an auditor verify that corrective actions are effective?

Sample answer: The auditor reviews evidence that planned actions were implemented and checks whether they address the cause and prevent recurrence. Depending on the issue, evidence may include updated procedures, system records, interviews, samples, or follow-up observations. Closing a finding should follow the applicable audit or certification process and be based on evidence, not merely a promise to act.

6. Scenario-Based Questions

Q26. What would you do if an organization has no documented risk assessment?

Sample answer: First confirm the applicable requirement and the ISMS scope, then gather evidence to determine whether the assessment is missing or exists in another form. If the requirement is not met, document the finding with objective evidence and the relevant criterion. The organization is responsible for performing and documenting the risk assessment; the auditor should not design the organization's solution while auditing it.

Q27. How would you handle a department that refuses to provide audit evidence?

Sample answer: I would explain the audit objective, the evidence requested, and why it is relevant, while maintaining a professional and respectful approach. I would discuss appropriate access or confidentiality arrangements with the audit contact. If evidence remains unavailable, I would document the limitation, assess its effect on the audit, and escalate or report it according to the audit procedure rather than assume what the evidence would show.

Q28. What would you do if an organization failed to implement a selected security control?

Sample answer: I would check the Statement of Applicability, risk-treatment plan, relevant requirements, and evidence of the control's status. I would establish whether the control was selected, whether an approved alternative or change exists, and whether risk

decisions were authorized. If the evidence demonstrates a requirement is not met, I would record the finding against the relevant criterion and leave the organization to determine corrective action.

Q29. How would you respond if an audit revealed repeated security incidents?

Sample answer: I would examine incident records, root-cause analyses, response actions, trends, and evidence of management review. Repeated incidents do not automatically prove nonconformity, but they may indicate that controls or corrective actions are ineffective. I would compare the evidence with relevant ISMS requirements and the organization's own processes, then document any substantiated gaps.

Q30. What would you do if the Statement of Applicability did not match implemented controls?

Sample answer: I would compare the Statement of Applicability with the risk-treatment plan and sampled implementation evidence. I would clarify whether the mismatch is a documentation error, a change that has not been reflected, or an implementation gap. I would document the relevant facts and assess them against the applicable requirements. The organization should maintain alignment between risk decisions, control selection, and actual implementation.

7. Advanced ISO 27001:2022 Questions

Q31. What are the major differences between ISO 27001:2013 and ISO 27001:2022?

Sample answer: The 2022 edition revised the structure of Annex A controls and aligned them with the updated control set in ISO/IEC 27002:2022. Annex A contains 93 controls grouped into four themes, compared with 114 controls in 14 groups in the 2013 edition. Organizations transitioning editions needed to review their controls and risk treatment. The transition deadline for accredited certification was October 31, 2025.

Q32. What changed in Annex A with the 2022 edition?

Sample answer: Annex A was reorganized into Organizational, People, Physical, and Technological themes, with 93 controls in total. The revised set includes new controls and updates to existing ones, reflecting areas such as threat intelligence, cloud services, data leakage prevention, and secure coding. Organizations should assess relevance through their risk process rather than assume that every new control applies automatically.

Q33. What is the role of management review in an ISMS?

Sample answer: Management review enables top management to evaluate whether the ISMS remains suitable, adequate, and effective. Inputs typically include audit results, changes in context, feedback, risk status, performance trends, and opportunities for

improvement. Outputs include decisions about improvement opportunities and changes needed to the ISMS. The review should be evidenced and its actions tracked.

Q34. How does an organization monitor and measure ISMS performance?

Sample answer: The organization defines what needs to be monitored and measured, the methods used, when monitoring occurs, who is responsible, and when results are analyzed. Measures may include incident trends, access-review completion, vulnerability remediation, audit findings, training completion, or corrective-action status. Metrics should help evaluate whether processes and controls achieve their intended outcomes, not simply generate numbers.

Q35. What is the difference between ISO 27001 and ISO 27002?

Sample answer: ISO/IEC 27001 specifies requirements for an information-security management system and is the standard used for ISMS certification. ISO/IEC 27002 provides guidance and implementation detail for information-security controls. The two standards are complementary: ISO 27001 establishes the management-system requirements, while ISO 27002 helps organizations understand and implement controls.

8. Lead Auditor Career and Practical Experience

Q36. What qualifications and skills are important for an ISO 27001 lead auditor?

Sample answer: Useful foundations include knowledge of ISO/IEC 27001:2022, audit principles, risk management, information-security concepts, evidence evaluation, interviewing, report writing, and communication. Formal training can help build audit-method knowledge, while practical experience develops judgment. Employers may have specific requirements for training, experience, or credentials, so candidates should check the expectations for the role and certification scheme.

Q37. What is the difference between an ISO 27001 internal auditor and a lead auditor?

Sample answer: An internal auditor evaluates the organization's ISMS as part of its internal-audit program. A lead auditor has additional responsibility for directing and coordinating an audit team and managing the audit process. The titles alone do not determine authority to conduct certification audits; certification audits are performed under the rules and oversight of an appropriately accredited or recognized certification body.

Q38. How do you plan an ISO 27001 audit program?

Sample answer: Start by considering the organization's importance of processes, changes, previous audit results, and risks. Define the audit program's objectives, scope, criteria, methods, schedule, responsibilities, resources, and competence needs. For each

audit, prepare a plan, identify relevant processes and evidence, and coordinate with auditees. Review results and follow-up actions so the program remains risk-informed and effective.

Q39. What challenges might an ISO 27001 lead auditor face, and how would you address them?

Sample answer: Challenges can include limited evidence, tight schedules, disagreement over findings, complex processes, and stakeholders who are unfamiliar with audit requirements. I would set clear expectations, prioritize based on audit objectives and risk, ask evidence-focused questions, communicate findings calmly, and document limitations. If an issue exceeds my competence or authority, I would seek appropriate support and follow the audit procedure.

Q40. How would you demonstrate your ISO 27001 auditing experience during an interview?

Sample answer: I would describe a specific audit or relevant project using a clear structure: the context and scope, my responsibilities, the evidence I reviewed, the issue or risk identified, the action taken by the responsible team, and the outcome. I would protect confidential information and distinguish my own contribution from the team's work. If I lack direct audit experience, I would be transparent and use training exercises or related experience as examples.

Ready to take the next step?

Keep building your knowledge of ISO 27001:2022, risk-based auditing, and ISMS implementation. If you are considering formal training, review relevant ISO 27001 auditor or lead auditor programs and compare their syllabus, assessment, and experience requirements with your career goals.

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.



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.



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.gsdccouncil.org