GRC Interview & Study Guide

ISO/IEC 27001 & 27002

Prepared by **Naresh Thalla Mudhiraj** · thallanaresh.com

Personal learning project. Views are my own and do not represent any employer.

Basic to Advanced · scenario-based questions · practical examples · why each topic matters

Version 2.0 · generated 21 October 2026

The international standard for an Information Security Management System (ISMS) and its supporting control guidance.

Study material written in plain language. Framework and regulatory details change; always confirm against the official, current publication before relying on them.

ISO/IEC 27001 & 27002

The international standard for an Information Security Management System (ISMS) and its supporting control guidance.

Q: What is ISO/IEC 27001?

Basic

ISO/IEC 27001 is the international standard that specifies requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS). The current version is ISO/IEC 27001:2022.

- **It is risk-based:** the organisation identifies its information security risks and selects controls to treat them.
- Organisations can be certified by an accredited certification body.
- Clauses 4–10 contain the mandatory management system requirements; Annex A lists reference controls.

Practical example: A healthcare SaaS vendor gets ISO 27001 certified so that hospital customers accept its security posture without each one sending a 300-question questionnaire.

Why this matters: ISO 27001 is the most widely recognised security certification globally, and its structure appears in many regional regulations.

Q: What is the Statement of Applicability (SoA)?

Basic

The SoA is a mandatory ISO 27001 document that lists all Annex A controls and, for each one:

- Whether it is applicable (included) or excluded.
- The justification for inclusion (e.g. linked to risks, legal or contractual requirements).
- The justification for exclusion.
- Its implementation status.

It also includes any additional controls the organisation uses beyond Annex A. The SoA links the risk treatment plan to the controls actually in place.

Practical example: An SoA line: 'A.7.4 Physical security monitoring: Excluded. Justification: fully remote company with no offices; data centres covered by cloud provider's ISO 27001 certificate.' Each control has a status and justification like this.

Why this matters: Auditors use the SoA as a roadmap for the audit. A weak SoA (e.g. exclusions without justification) is an early red flag.

Q: What is an ISMS?

Basic

An Information Security Management System (ISMS) is the set of policies, processes, roles, risk assessments and controls an organisation uses to manage information security systematically and keep improving it.

- It is a management system, not a technical product.
- **It follows the Plan-Do-Check-Act idea:** plan based on risk, implement controls, monitor and audit, then improve.
- ISO/IEC 27001 defines the requirements for an ISMS. Organisations can be certified against it.

Practical example: A hospital's ISMS includes its security policy, risk methodology, risk register, Statement of Applicability, internal audit programme, management reviews and corrective-action log, all of it reviewed and improved each year.

Why this matters: Interviewers want to hear that security is managed as an ongoing business process with leadership involvement, not as a one-off project.

Q: What are the four themes of Annex A in ISO/IEC 27001:2022, and how many controls are there?

Basic

ISO/IEC 27001:2022 Annex A has 93 controls in four themes:

- **Organizational controls (clause 5):** 37 controls, such as policies, roles, threat intelligence, supplier security and cloud services.
- **People controls (clause 6):** 8 controls, such as screening, awareness and remote working.
- **Physical controls (clause 7):** 14 controls, such as secure areas, physical security monitoring and equipment.
- **Technological controls (clause 8):** 34 controls, such as access, logging, secure coding and data masking.

The 2013 version had 114 controls in 14 domains. Many were merged, and 11 new controls were added.

Practical example: When converting an old SoA, the former 'A.12.4.1 Event logging' maps to the 2022 control 8.15 Logging, and 'A.9.2.6 Removal of access rights' maps into 5.18 Access rights.

Why this matters: This is one of the most commonly asked ISO questions and shows you are current with the 2022 revision.

Q: What are the 11 new controls added in ISO/IEC 27001:2022?

Basic

- 5.7 Threat intelligence.
- 5.23 Information security for use of cloud services.
- 5.30 ICT readiness for business continuity.
- 7.4 Physical security monitoring.
- 8.9 Configuration management.
- 8.10 Information deletion.
- 8.11 Data masking.
- 8.12 Data leakage prevention.
- 8.16 Monitoring activities.
- 8.23 Web filtering.
- 8.28 Secure coding.

Practical example: For 8.28 Secure coding, a SaaS company shows its secure-coding standard, peer review rules, static code analysis in the CI pipeline and developer training records as evidence.

Why this matters: These controls reflect the modern threat landscape (cloud, data leakage, threat intelligence) and are where auditors look closely during transition and surveillance audits.

Q: A small startup asks you whether it 'needs' ISO 27001. How do you advise them?

Basic · **Scenario**

- ISO 27001 is voluntary unless a customer, contract or regulator requires it. Ask what is driving the question.
- **Look at the market:** enterprise and healthcare customers, and many buyers in Europe, Asia and India, often ask for it. US customers often prefer SOC 2.
- **Consider the effort:** scope, policies, risk assessment, controls, internal audit and certification fees, plus ongoing surveillance audits.
- **Suggest a phased path:** start with a gap assessment and basic controls, keep the scope focused on the product customers buy, then certify when sales need it.
- **Explain the benefits beyond the certificate:** fewer questionnaires and better-organised security.

Practical example: A 25-person health-tech startup is losing hospital tenders without a certificate. They scope ISO 27001 to their SaaS platform, use a GRC tool to speed up evidence, and certify within about 9 months.

Why this matters: Good GRC advice is proportionate and tied to business goals. Recommending certification without understanding the driver wastes money.

Q: What are the main clauses (4–10) of ISO 27001?

Intermediate

- **Clause 4 – Context of the organisation:** internal/external issues, interested parties, ISMS scope.
- **Clause 5 – Leadership:** top management commitment, information security policy, roles and responsibilities.
- **Clause 6 – Planning:** risk assessment, risk treatment, Statement of Applicability, security objectives, planning of changes.
- **Clause 7 – Support:** resources, competence, awareness, communication, documented information.
- **Clause 8 – Operation:** operational planning and control, performing risk assessments and treatment.
- **Clause 9 – Performance evaluation:** monitoring and measurement, internal audit, management review.
- **Clause 10 – Improvement:** continual improvement, nonconformity and corrective action.

Clauses 1–3 cover scope, normative references and terms and definitions.

Practical example: Clause 6 drives the risk assessment and SoA, clause 8 is where the risk treatment plan is actually executed, and clause 9 is where the internal audit and management review prove the ISMS works.

Why this matters: Certification auditors assess against clauses 4–10 first. Many first-time certifications fail on management system elements, not technical controls.

Q: How is Annex A structured in ISO 27001:2022?

Intermediate

Annex A of the 2022 version contains 93 controls grouped into four themes:

- Organisational controls (37)
- People controls (8)
- Physical controls (14)
- Technological controls (34)

The 2013 version had 114 controls in 14 domains. The 2022 update merged many controls and added 11 new ones, including threat intelligence, information security for use of cloud services, ICT readiness for business continuity, data masking, data leakage prevention, web filtering and secure coding.

ISO/IEC 27002:2022 gives implementation guidance for each control and introduces attributes (e.g. control type, security properties, cybersecurity concepts) for filtering and mapping.

Practical example: Threat intelligence (5.7) sits in the Organizational theme, screening (6.1) in People, physical security monitoring (7.4) in Physical, and data masking (8.11) in Technological.

Why this matters: Knowing the 2022 structure shows you are current — the transition period from the 2013 version has ended.

Q: What is the difference between ISO 27001 and ISO 27002?

Intermediate

- ISO/IEC 27001 contains the requirements for an ISMS. Organisations are certified against it ('shall' statements).
- ISO/IEC 27002 is a code of practice giving guidance on implementing security controls. Organisations are not certified against it.

Annex A of 27001 lists the controls by name and short description; 27002 explains the purpose and implementation guidance for each.

Practical example: 27001 says you must select controls based on risk and justify them in the SoA; 27002 explains how to implement control 8.15 Logging, such as what events to log and how to protect logs.

Why this matters: Mixing these up is a common mistake in interviews. The distinction is simple but important.

Q: Describe the ISO 27001 certification process.

Intermediate

1. Define scope and implement the ISMS (risk assessment, SoA, policies, controls, internal audit, management review).
2. **Stage 1 audit:** the certification body reviews documentation and readiness.
3. **Stage 2 audit:** assesses whether the ISMS is implemented and operating effectively.
4. Address any nonconformities (major nonconformities must be resolved before certification).
5. Certificate issued, typically valid for three years.
6. Surveillance audits during the cycle (usually annually), then a recertification audit before expiry.

Practical example: Stage 1 in January (documentation review finds the SoA lacks justifications), Stage 2 in March (on-site evidence testing), certificate issued in April, surveillance audits in years 2 and 3, recertification in year 3.

Why this matters: Interviewers want to know you have lived through — or can run — a certification cycle end to end.

Q: How do internal audit and management review work in an ISMS?

Intermediate

- **Internal audit (Clause 9.2):** planned audits, at defined intervals, to check the ISMS conforms to the organisation's own requirements and the standard and is effectively implemented. Auditors must be objective and impartial (they should not audit their own work).
- **Management review (Clause 9.3):** top management reviews the ISMS at planned intervals. Inputs include status of previous actions, changes in context, performance and audit results, feedback from interested parties, risk assessment results and improvement opportunities. Outputs are decisions on improvement and changes.

Both must be documented and are always checked during certification audits.

Practical example: The internal audit programme covers all clauses and relevant Annex A controls over the cycle. Findings feed the management review, where top management decides on resources and changes, with minutes kept as evidence.

Why this matters: These two activities prove that leadership oversees the ISMS and that it improves over time — the heart of a management system.

Q: What changed in the ISO 27001 clauses in 2022, and what did Amendment 1:2024 add?

Intermediate

Clause changes in 2022 were modest but important:

- **4.2:** requirements of interested parties that will be addressed through the ISMS must be determined.
- **4.4:** processes needed and their interactions must be determined.
- **6.2:** information security objectives must be monitored.
- **6.3 (new):** planning of changes to the ISMS.
- **8.1:** criteria for processes and control of externally provided processes, products or services.

Amendment 1:2024 added climate action changes: in clause 4.1, the organisation must determine whether climate change is a relevant issue, and in 4.2 that interested parties can have climate-related requirements.

Practical example: During a surveillance audit, the auditor asks to see how the company decided whether climate change is relevant to its ISMS. The context document records that flood risk to the primary data centre was considered and is addressed in business continuity planning.

Why this matters: Auditors check these clause-level changes, not just Annex A. Knowing the climate amendment shows you follow the standard closely.

Q: What are control attributes in ISO/IEC 27002:2022, and how are they useful?

Intermediate

ISO/IEC 27002:2022 tags each control with five attributes so you can filter and view controls in different ways:

- **Control type:** preventive, detective, corrective.
- **Information security properties:** confidentiality, integrity, availability.
- **Cybersecurity concepts:** identify, protect, detect, respond, recover (aligned to the NIST CSF functions).
- **Operational capabilities:** such as governance, asset management, identity and access management.
- **Security domains:** governance and ecosystem, protection, defence, resilience.

Organisations can also create their own attributes.

Practical example: Filtering the SoA by the 'detect' concept shows only a handful of implemented detective controls for cloud services, which justifies a project to add cloud security posture monitoring.

Why this matters: Attributes make it easier to map ISO controls to other frameworks and to report coverage, for example 'do we have enough detective controls?'.

Q: How do you define the scope of an ISMS?

Intermediate

Clause 4.3 requires a documented scope that considers internal and external issues (4.1), interested parties' requirements (4.2) and interfaces and dependencies with other organisations.

- **Define it in business terms:** services, locations, teams, systems and data.

- **Be clear about interfaces:** what is outside scope and how it connects (for example, an outsourced data centre or a group IT function).
- Exclusions must not undermine the ISMS. You cannot exclude a team that has full access to in-scope data.
- Make it match what customers think they are buying. A scope that is too narrow can mislead them and will be challenged.

Practical example: 'The ISMS covers the development, operation and support of the cloud-based revenue-cycle platform, delivered from the Bengaluru and Singapore offices, including supporting HR, IT and supplier management processes.'

Why this matters: Scope decides the cost of the ISMS and the value of the certificate. Customers increasingly read the scope statement closely.

Q: What is the information security risk treatment plan, and how does it link to the SoA?

Intermediate

Clause 6.1.3 requires the organisation to select risk treatment options, determine the necessary controls, compare them with Annex A, produce a Statement of Applicability and formulate a risk treatment plan.

- The risk treatment plan lists the actions to treat each risk, with owners, resources and timelines.
- Risk owners must approve the plan and accept the residual risks.
- The SoA lists all necessary controls, the justification for including them, whether they are implemented, and justification for excluding any Annex A controls.

So the chain is: risk assessment → treatment decision → controls → SoA and treatment plan → implementation (clause 8.3).

Practical example: Risk R-07 'Data loss from lost laptops' is treated with 8.1 User endpoint devices and 8.24 Use of cryptography. The plan sets an encryption rollout by Q2, owned by the IT manager, and the SoA marks both controls 'implemented' once the rollout is verified.

Why this matters: Auditors trace this chain. A control in the SoA with no link to a risk, or a high risk with no treatment, is a common nonconformity.

Q: During the Stage 1 audit, the auditor says your risk assessment does not cover cloud services. What do you do before Stage 2?

Intermediate · **Scenario**

- Accept the observation and understand what the auditor expects (risk identification for cloud services, clause 6.1.2, and control 5.23).
- Update the risk assessment to include each cloud service in scope: data stored, shared responsibility, provider assurance and exit risks.
- Decide treatments and update the SoA and risk treatment plan.
- **Implement or evidence the cloud controls:** provider due diligence, configuration baselines, monitoring.
- Get risk owner approval and keep the records ready for Stage 2.

Stage 1 findings are meant to be fixed before Stage 2, so this is normal and manageable.

Practical example: The team adds risks for its main cloud platform, its SaaS email and its backup provider, reviews each provider's ISO 27001 and SOC 2 reports, and documents customer-side responsibilities. Stage 2 goes ahead with no nonconformity on cloud.

Why this matters: Stage 1 identifies readiness gaps. Showing that you can close them quickly and properly gives the auditor confidence in the ISMS.

Q: An auditor raises a minor nonconformity for a missing document approval. How do you handle the corrective action?

Intermediate · **Scenario**

1. **Correction:** fix the immediate problem (get the document approved and published).
2. **Root cause:** why was it missed? For example, the document management process has no approval step or reminder.
3. **Corrective action:** change the process so it does not recur, such as a mandatory approval workflow.
4. Check other documents for the same problem (extent of condition).
5. Submit the corrective action plan within the certification body's timeframe and keep evidence.
6. Verify effectiveness later. The auditor will check at the next audit.

Practical example: The supplier security policy was never formally approved. The fix approves it, adds an approval step to the document workflow, and a check of all 18 policies finds two more unapproved ones, which are approved within a week.

Why this matters: ISO 27001 clause 10.2 requires correction, root cause and corrective action. A plan that only fixes the one document will be challenged.

Q: Your company is moving to a new office and a new cloud provider during the certification cycle. What ISO 27001 actions are needed?

Intermediate · **Scenario**

- **Clause 6.3 (planning of changes):** plan the changes to the ISMS in a controlled way.
- Update the risk assessment for the new site and the new provider, and update the SoA if controls change.
- Apply physical security controls to the new office (clause 7 controls) and supplier/cloud controls (5.19–5.23) to the new provider.
- Update the scope statement if locations or services change, and inform the certification body, which may need to audit the new site.
- Update business continuity plans and asset inventory.

Practical example: The certification body is told 2 months in advance. A short special audit of the new office is added to the next surveillance visit, and the cloud migration is tracked as a change with its own risk assessment and sign-off.

Why this matters: Changes are where controls break. Certification bodies expect to be told about significant changes and to see that they were managed through the ISMS.

Q: The auditor asks how you decided which Annex A controls are not applicable. What evidence do you show?

Intermediate · **Scenario**

- The SoA with a justification for each exclusion, linked to the scope and the risk assessment.
- The risk assessment results showing no risk that the control would treat, or that the risk is treated in another way.
- Context evidence, such as 'no physical office' or 'no in-house software development', backed by facts (lease documents, organisation chart).
- Records that the risk owners and top management approved the SoA.

Note that a control can still apply partly through a supplier (for example the cloud provider's data centre). Then you manage it through supplier controls rather than excluding it.

Practical example: The company excluded 8.28 Secure coding because 'we buy software'. The auditor finds it customises its CRM with scripts. The control is reinstated in the SoA with a lightweight secure scripting standard and peer review.

Why this matters: Exclusions are a classic audit focus because an unjustified exclusion can hide a real gap.

Q: What is the difference between a major and a minor nonconformity?

Advanced

- **Major nonconformity:** a requirement is not met in a way that raises significant doubt about the ISMS achieving its intended outcomes — e.g. no internal audit performed, no management review, or a systemic failure of a control area.
- **Minor nonconformity:** a single or occasional lapse that does not undermine the system as a whole — e.g. one missed access review.
- **Opportunity for improvement / observation:** not a nonconformity, but a suggestion.

Corrective action should address root cause, and its effectiveness is checked in a later audit.

Practical example: Major: no internal audit has ever been performed (clause 9.2 not implemented). Minor: one of 15 sampled supplier contracts is missing the agreed information security clause, while the other 14 have it.

Why this matters: How you respond to nonconformities (root cause and corrective action) is itself an ISMS requirement in Clause 10.

Q: How does ISO/IEC 27001 integrate with other management systems such as ISO 9001, ISO 22301, ISO/IEC 27701 and ISO/IEC 42001?

Advanced

All of these use the ISO harmonised structure (clauses 4–10 with common text), so they can share one integrated management system:

- **Common processes:** context, leadership, document control, internal audit, management review and corrective action.
- ISO 22301 (business continuity) links to 27001 controls 5.29 and 5.30.
- ISO/IEC 27701 adds privacy information management (PII controller and processor requirements) on top of information security.
- ISO/IEC 42001 (AI management system) uses the same structure for governing AI.
- Integrated audits by the certification body can reduce audit days and duplicate work.

Practical example: A health-tech company runs one integrated management review covering ISO 27001, ISO 22301 and ISO 42001. It shares one internal audit programme and one corrective-action log, and its certification body audits all three together.

Why this matters: Organisations rarely want separate management systems. Integration saves money and gives leadership one view.

Q: How do you measure the effectiveness of an ISMS (clause 9.1)?

Advanced

Clause 9.1 requires you to decide what to monitor and measure, the methods, when, who analyses it and how results are evaluated.

- **Measure both the ISMS processes and the controls:** objectives achieved, risk treatment progress, audit results, incidents, control KPIs.
- Link metrics to information security objectives (clause 6.2), which must be measurable where practicable.
- Keep documented evidence of results and analysis, and use them in management review.
- Avoid measuring only activity (number of trainings). Include outcomes (phishing report rate, time to revoke access).

Practical example: Objective: 'Reduce critical vulnerabilities older than 30 days to zero by Q4.' The metric is tracked monthly, reviewed at management review, and a missed target in Q3 triggers extra patching resources.

Why this matters: Auditors frequently raise nonconformities under 9.1 when organisations collect data but never analyse it or act on it.

Q: Top management has not attended a management review in a year. Why is this a problem and how do you fix it?

Advanced · **Scenario**

- Clause 5.1 (leadership and commitment) and clause 9.3 (management review) require top management to direct and review the ISMS. Without them, it is likely to be a major nonconformity.
- **Find out why:** meetings too long, too technical or badly timed.
- **Redesign the review:** a short pack covering the 9.3 inputs (status of actions, changes, performance, feedback, risk results, improvement opportunities), with clear decisions needed.
- Combine it with an existing leadership meeting if possible.
- Record minutes with decisions and actions, which is the evidence auditors want.

Practical example: The management review is moved into the quarterly executive meeting as a 30-minute item with a 5-page pack. The CEO approves two resource requests, and the minutes become clean evidence for the next surveillance audit.

Why this matters: Leadership involvement is the heart of an ISMS. A certification body will treat its absence as a failure of the management system, not a paperwork issue.

Q: An auditor samples 5 leavers and finds one still had access 3 weeks after leaving. Is this a major or minor nonconformity, and what would you argue?

Advanced · **Scenario**

- A single isolated failure where the process exists and generally works is usually a minor nonconformity. It becomes major if the control is missing entirely, failing systematically, or has led to a serious incident.
- **Provide context with evidence:** the leaver process, the other samples that passed, and whether the account was actually used after the leave date (check logs).
- Do not argue the facts if they are correct. Explain the root cause and corrective action.
- **Look for the extent of the problem:** run a full reconciliation of all leavers against active accounts.

Practical example: Logs show the account was never used after the leave date, and the other 4 samples were removed within a day. The full reconciliation finds one more case, both are fixed, and the auditor records a minor nonconformity with the corrective action accepted.

Why this matters: Understanding how auditors grade nonconformities helps you respond professionally and protect the certificate without being defensive.