ISO 27001 Lead Auditor practice questions and answers

> **Original practice questions written from ISO/IEC 27001:2022, ISO 19011:2018 and ISO/IEC 17021-1:2015. Not real exam questions.**

Ten questions, then the answer key with the correct option, a plain-English rationale and the clause each answer comes from. Answer all ten before you turn to the answers.

Prefer instant scoring? The same questions are online at mindsetprep.com.au/free-practice-questions/iso-27001-lead-auditor/.

QUESTION 1

During the on-site phase of a Stage 2 certification audit, the team collects access-control logs showing five attempts to disable MFA in the preceding month. According to ISO 19011:2018, this information is best described as:

A. Audit evidence that has not yet been evaluated against criteria

B. An audit finding that should be raised at the closing meeting

C. A nonconformity under ISO/IEC 17021-1

D. An audit conclusion supporting the certification decision

QUESTION 2

ISO/IEC 27001:2022 Clause 6.1.3 d) addresses the Statement of Applicability (SoA). Which option most accurately reflects the standard's wording?

A. The organisation may produce a SoA when an external party requires it

B. The organisation should produce a SoA aligned with Annex A

C. The organisation must produce a SoA only after the risk treatment plan is approved

D. The organisation shall produce a SoA that justifies inclusions and exclusions of Annex A controls

QUESTION 3

An audit team leader is assigned to a client where she worked three years ago in a junior risk role. According to ISO/IEC 17021-1:2015, the most appropriate response is to:

A. Disclose the prior engagement to the certification body and reassign if impartiality cannot be safeguarded

B. Proceed because three years exceeds the cooling-off period for junior staff

C. Proceed but limit the audit to ISMS Clauses 4 to 7 and assign Annex A to a different auditor

D. Decline because demonstrated sector competence creates an independence conflict

QUESTION 4

After interviews and document review, the auditor concludes that the organisation's risk treatment plan does not address two risks rated 'high' in the assessment. Under ISO 19011:2018 and ISO/IEC 27001:2022, this is most precisely described as:

A. An audit finding that may or may not be a nonconformity, pending evaluation

B. A nonconformity against Clause 6.1.3 of ISO/IEC 27001:2022

C. Audit evidence requiring further investigation

D. An opportunity for improvement to be noted in the report

QUESTION 5

ISO/IEC 27001:2022 Clause 9.2 addresses internal audit. Which statement is correct?

A. Internal audits may be replaced by external surveillance audits where a certified ISMS is in scope

B. The organisation shall conduct internal audits at planned intervals against its own ISMS requirements and the standard

C. Internal audits must follow ISO 19011:2018 exactly, including the audit programme structure

D. The organisation should conduct internal audits at least annually as a recommended practice

QUESTION 6

An audit team is being assembled for a Stage 2 audit of a fintech ISMS. The most senior auditor available holds an information-security qualification and has twelve years of financial-services security experience, but she conducted internal ISMS audits for the same fintech's parent company three years ago. According to ISO 19011:2018 and ISO/IEC 17021-1:2015, the most accurate framing of her status is:

A. Both competence and independence are established by the twelve years of financial-services experience

B. Her competence is in question because financial-services audits require additional sector-specific qualifications regardless of experience

C. Her independence is not in question because three years exceeds the impartiality cooling-off window for internal-audit work, so the only remaining concern is competence

D. Her competence is established by qualification and experience; her independence with respect to this specific client is a separate question for the certification body to evaluate

QUESTION 7

After the audit team completes evaluation of all findings, they prepare a single statement summarising whether the management system fulfils the audit criteria. Per ISO 19011:2018, this statement is the:

A. Audit finding

B. Audit conclusion

C. Audit observation

D. Audit report

QUESTION 8

ISO/IEC 27001:2022 Clause 7.5 covers documented information. Which statement is correct?

A. Documented information must follow ISO 30301:2019 records-management requirements

B. The ISMS should include all Annex A control documentation regardless of applicability

C. The ISMS shall include documented information required by the standard and that determined by the organisation as necessary

D. Documented information may be omitted where the organisation can demonstrate equivalent oral practices

QUESTION 9

An auditor evaluator is reviewing a new lead-auditor candidate who has completed Lead Auditor training, holds an ISO/IEC 27001 implementer certification, and has audited three ISMSes as a team member. Under ISO 19011:2018 Clause 7, the candidate's status is best described as:

A. Competence is conditional on completing one further audit as team leader before lead-auditor sign-off

B. Competence is demonstrated for lead auditor; impartiality of any specific assignment is a separate evaluation

C. Both competence and independence are demonstrated together by the training certificate

D. Independence is the deciding factor; training and experience are secondary to absence of conflict

QUESTION 10

During an interview, a system administrator states that backups are tested monthly. The auditor records the statement. To convert this into objective audit evidence under ISO 19011:2018, the auditor most appropriately:

A. Notes the statement and raises a nonconformity if records cannot later be located

B. Records the verbal statement and treats it as evidence sufficient for the finding

C. Requests records of recent backup-test results that the administrator can produce on the spot

D. Asks two other staff the same question and accepts a majority answer

Answers

Q1 Correct answer: **A.** Audit evidence that has not yet been evaluated against criteria

ISO 19011:2018 Clause 3 (Terms and definitions) defines audit evidence as records, statements of fact or other information that are relevant to the audit criteria and verifiable. Evaluation against criteria is what turns evidence into a finding; only consideration of all findings produces a conclusion. The log entries here are raw evidence, not yet evaluated. The other options jump one or more stages ahead: the classic evidence-vs-finding swap exam-writers reuse.

`Cited: ISO 19011:2018, Clause 3 (Terms and definitions)`

`Trap pattern: T-01 Evidence vs finding`

Q2 Correct answer: **D.** The organisation shall produce a SoA that justifies inclusions and exclusions of Annex A controls

Clause 6.1.3 d) uses 'shall'. The SoA is mandatory in any ISMS conforming to ISO/IEC 27001:2022, and it must justify both inclusions and exclusions of Annex A controls. The other options soften the requirement to 'should' or 'may', or add a triggering condition the standard does not contain. Exam-style wrong options routinely swap 'shall' for a softer modal verb because the eye slides past the change under time pressure.

`Cited: ISO/IEC 27001:2022, Clause 6.1.3 d)`

`Trap pattern: T-02 Shall vs should`

Q3 Correct answer: **A.** Disclose the prior engagement to the certification body and reassign if impartiality cannot be safeguarded

ISO/IEC 17021-1:2015 Clause 5.2 requires the certification body to identify and manage impartiality risks. The standard prescribes specific cooling-off periods for prior consultancy or internal-audit relationships, but prior employment in a non-consulting junior role falls under the broader impartiality-risk identification requirement and is evaluated case-by-case. Option B fabricates a junior-staff cooling-off rule. Option D is the classic competence-vs-independence swap: sector competence does not by itself disqualify; the relationship does. Option C is a workaround the standard does not sanction.

`Cited: ISO/IEC 17021-1:2015, Clause 5.2`

`Trap pattern: T-03 Competence vs independence`

Q4 Correct answer: **B.** A nonconformity against Clause 6.1.3 of ISO/IEC 27001:2022

When evaluated evidence shows a 'shall' requirement is not met, the finding is a nonconformity (ISO 19011:2018 Clause 3 Terms and definitions; ISO/IEC 27001:2022 Clause 10.2). Option A drags it back to the pending-evaluation stage that has already passed in the stem. Option C drags it back further to raw evidence: the classic T-01 swap. Option D downgrades a clause breach to an OFI, which understates the issue when a mandatory clause is in scope.

`Cited: ISO/IEC 27001:2022, Clause 10.2 (Nonconformity and corrective action)`

`Trap pattern: T-01 Evidence vs finding`

Q5 Correct answer: **B.** The organisation shall conduct internal audits at planned intervals against its own ISMS requirements and the standard

Clause 9.2 uses 'shall' and requires audits at planned intervals against both the organisation's own ISMS requirements and the standard. Option D softens to 'should' and adds an interval ('annually') that the standard does not specify. Option A is wrong: surveillance does not replace internal audit. Option C overstates ISO 19011, which is a guidance document whose verbs are 'should', not 'shall'.

Cited: ISO/IEC 27001:2022, Clause 9.2

Trap pattern: T-02 Shall vs should

Q6 Correct answer: **D.** Her competence is established by qualification and experience; her independence with respect to this specific client is a separate question for the certification body to evaluate

ISO 19011:2018 Clause 7 treats competence (knowledge, skills, attributes, experience) as one axis, and ISO/IEC 17021-1:2015 Clause 5.2 treats impartiality and independence as a separate, per-engagement axis. Option D keeps the two axes distinct, which is what the standards require. Option C inverts the relationship and invents a fixed cooling-off length for internal-audit work. Option A collapses both axes into one: the classic competence-vs-independence trap. Option B mis-frames the competence question; sector experience is exactly what 19011 Clause 7 counts as competence evidence.

Cited: ISO 19011:2018, Clause 7 + ISO/IEC 17021-1:2015, Clause 5.2

Trap pattern: T-03 Competence vs independence

Q7 Correct answer: **B.** Audit conclusion

ISO 19011:2018 Clause 3 (Terms and definitions) defines the audit conclusion as the outcome of an audit after consideration of the audit objectives and all audit findings. Option A is a single finding, not the summary. Option D is the deliverable that contains the conclusion, not the conclusion itself. Option C is an informal observation that did not meet finding criteria. The evidence-vs-finding trap extends to any step of the vocabulary chain: evidence to finding to conclusion to report.

Cited: ISO 19011:2018, Clause 3 (Terms and definitions)

Trap pattern: T-01 Evidence vs finding

Q8 Correct answer: **C.** The ISMS shall include documented information required by the standard and that determined by the organisation as necessary

Clause 7.5.1 uses 'shall' and requires both the documentation explicitly mandated by the standard AND any further documentation the organisation determines is necessary. Option B both softens the verb from 'shall' to 'should' and overreaches by requiring documentation for all Annex A controls regardless of SoA selection (Annex A applicability is governed by Clause 6.1.3, not by 7.5). Option D contradicts the standard outright. Option A imports ISO 30301:2019, which is unrelated to 27001 conformance.

Cited: ISO/IEC 27001:2022, Clause 7.5.1

Trap pattern: T-02 Shall vs should

Q9 Correct answer: **B.** Competence is demonstrated for lead auditor; impartiality of any specific assignment is a separate evaluation

ISO 19011:2018 Clause 7 treats auditor competence (knowledge, skills, attributes, experience) as a distinct concept from independence and impartiality, which are evaluated per assignment. Option B correctly separates them. Option A invents an experience-count rule the standard does not specify. Option D subordinates competence to independence; the standard treats them as parallel. Option C collapses them into one: the classic competence-vs-independence trap.

Cited: ISO 19011:2018, Clause 7 (Competence and evaluation of auditors)

Trap pattern: T-03 Competence vs independence

Q10 Correct answer: **C.** Requests records of recent backup-test results that the administrator can produce on the spot

ISO 19011:2018 Clause 3 (Terms and definitions) requires audit evidence to be verifiable. An unverified verbal statement is not yet objective evidence; corroborating records turn it into one. Option B accepts unverified hearsay, exactly what the standard excludes. Option D uses social proof rather than verification. Option A jumps to a nonconformity without giving the auditee a reasonable opportunity to produce the evidence on the day.

Cited: ISO 19011:2018, Clause 3 (Terms and definitions)

Trap pattern: T-01 Evidence vs finding

Want the full bank?

Mindset Prep has 600+ clause-cited ISO 27001 Lead Auditor questions, each with the cited clause and a rationale, and an adaptive engine that brings back the clauses you miss. Start with a 3-day free trial.

Start the 3-day free trial

https://app.mindsetprep.com.au/start?source=free-questions-pdf&exam=iso-27001-la