ISO 27001 Lead Implementer practice questions and answers

> **Original practice questions written from ISO/IEC 27001:2022, ISO/IEC 27005:2022 and ISO/IEC 27003:2017. 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-implementer/.

QUESTION 1

During an ISMS implementation, the team has completed the risk treatment decisions and is preparing the next two artefacts. Per ISO/IEC 27001:2022, which statement correctly distinguishes the Statement of Applicability (SoA) from the Risk Treatment Plan (RTP)?

A. The SoA justifies inclusion or exclusion of each Annex A control; the RTP specifies who does what, by when, and with what resources to implement the treatment

B. The SoA is signed by top management; the RTP is signed by the risk owner only

C. The SoA lists residual risks above the risk acceptance criteria; the RTP lists controls selected from Annex A

D. The SoA replaces the RTP for organisations that adopt the full Annex A control set

QUESTION 2

An organisation purchases cyber-insurance to cover the financial impact of a successful ransomware attack. Per ISO/IEC 27005:2022, this treatment is best categorised as:

A. Risk retention (acceptance)

B. Risk modification (mitigation)

C. Risk sharing (transfer)

D. Risk avoidance

QUESTION 3

Six months after ISMS certification, the organisation conducts its second internal audit and identifies that one Annex A control is not being applied consistently. The Lead Implementer asks whether this should be treated as an implementation gap or an operation-phase nonconformity. The correct framing is:

A. Implementation gap, raised under Clause 6.1.3: the control was inadequately implemented and needs redesign

B. Both: the gap proves the implementation was incomplete and the operation is failing

C. Operation-phase nonconformity, raised under Clause 10.2: the ISMS is operational, so any control gap is now an operational issue

D. Neither: inconsistent application is normal in the first year of operation

QUESTION 4

In the ISMS implementation sequence, which order correctly reflects ISO/IEC 27001:2022 Clause 6?

A. Risk Treatment Plan -> risk assessment -> SoA -> risk treatment decisions -> implementation

B. SoA -> risk assessment -> risk treatment decisions -> Risk Treatment Plan -> implementation

C. Risk assessment -> SoA -> risk treatment decisions -> Risk Treatment Plan -> implementation

D. Risk assessment -> risk treatment decisions -> SoA -> Risk Treatment Plan -> implementation

QUESTION 5

An organisation identifies a high risk from operating a legacy mainframe with no vendor patch support. Management decides to migrate off the mainframe within six months. Per ISO/IEC 27005:2022, this treatment is:

A. Risk acceptance: management has acknowledged the risk and chosen to proceed for six months

B. Risk avoidance: the activity creating the risk will be ceased

C. Risk modification: migration is a control that reduces the impact

D. Risk sharing: the migration shifts the risk to the new platform vendor

QUESTION 6

Per ISO/IEC 27003:2017 guidance on ISO/IEC 27001 Clause 6, which activity is part of the implementation phase rather than the operation phase?

A. Producing the Statement of Applicability and Risk Treatment Plan

B. Investigating a security incident and applying corrective action

C. Conducting the management review of ISMS performance

D. Reviewing the Information Security Policy on the published cycle

QUESTION 7

Per ISO/IEC 27001:2022 Clause 6.1.3 d), the Statement of Applicability shall contain:

A. The full list of Annex A controls, ranked by residual risk after treatment

B. The necessary controls, the justification for their inclusion, whether each is implemented, and the justification for excluding any Annex A control

C. The audit programme, the audit findings from the most recent internal audit, and the corrective actions

D. The risk treatment plan, the residual risks, and the management approvals for acceptance

QUESTION 8

An organisation has documented its risk acceptance criteria as 'risks with a residual rating of medium or below are acceptable to top management'. After treatment, a particular risk has a residual rating of 'high'. Per ISO/IEC 27001:2022, the appropriate next step is:

A. Apply risk avoidance and cease the underlying activity

B. Update the Risk Treatment Plan with additional controls, OR seek formal risk owner approval to retain the residual risk above criteria

C. Document the residual risk in the SoA so it appears in the audit trail

D. Update the risk acceptance criteria to permit high residual risks for this case

QUESTION 9

Per ISO/IEC 27001:2022 Clause 10.2, when a nonconformity is identified during ISMS operation, the organisation shall:

A. Treat it as an implementation gap and return to Clause 6 to redesign the affected control

B. Defer corrective action until the next surveillance audit so the certification body can verify it

C. Document the nonconformity in the SoA and re-issue at the next management review

D. React, evaluate the need to eliminate the cause, implement actions, review effectiveness, and update the ISMS if necessary

QUESTION 10

Per ISO/IEC 27001:2022 Clause 6.1.3 f), who must formally approve the residual information security risks at the end of the risk treatment process?

A. The internal auditor, under Clause 9.2

B. The risk owner, under Clause 6.1.3 f)

C. Top management, under Clause 5.1

D. The certification body, before initial certification

Answers

Q1 Correct answer: **A.** The SoA justifies inclusion or exclusion of each Annex A control; the RTP specifies who does what, by when, and with what resources to implement the treatment

ISO/IEC 27001:2022 Clause 6.1.3 d) defines the SoA as the document justifying inclusions and exclusions of Annex A controls. Clause 6.1.3 e) defines the RTP as the plan to implement the treatment: who, what, when, with what resources. Option C swaps the content of the two artefacts (a textbook SoA-vs-RTP trap). Option B invents a signing rule the standard does not prescribe. Option D contradicts 6.1.3 d): the SoA is required regardless of how many Annex A controls are selected.

`Cited: ISO/IEC 27001:2022, Clauses 6.1.3 d) and 6.1.3 e)`

`Trap pattern: T-01 SoA vs Risk Treatment Plan`

Q2 Correct answer: **C.** Risk sharing (transfer)

ISO/IEC 27005:2022 Clause 8.5 lists four risk treatment options. Cyber-insurance shifts the financial consequence of an event to a third party, which is risk sharing (formerly 'transfer'). Mitigation (Option B) means applying controls that reduce likelihood or impact. Insurance does not change the underlying control posture. Acceptance (Option A) means doing nothing further. Insurance is a positive action. Avoidance (Option D) means ceasing the activity. The transfer-vs-mitigate confusion is exam-grade because both colloquially 'reduce the impact on us'.

`Cited: ISO/IEC 27005:2022, Clause 8.5`

`Trap pattern: T-03 Risk treatment verb swap`

Q3 Correct answer: **C.** Operation-phase nonconformity, raised under Clause 10.2: the ISMS is operational, so any control gap is now an operational issue

Once the ISMS is certified and operational, control gaps fall under Clause 10.2 (Nonconformity and corrective action). The ISMS has transitioned from implementation (Clause 6) to operation (Clause 8) and is now governed by performance evaluation (Clause 9) and improvement (Clause 10). Option A is the implementation-vs-operation phase trap: it sends the team back to the wrong clause. Option B makes both apply, which is incorrect after the phase transition. Option D dismisses the nonconformity entirely.

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

`Trap pattern: T-02 Implementation vs operation phase`

Q4 Correct answer: **D.** Risk assessment -> risk treatment decisions -> SoA -> Risk Treatment Plan -> implementation

Clauses 6.1.2 (risk assessment) and 6.1.3 a) to c) (selecting treatment options, determining controls, comparing to Annex A) come first. Then 6.1.3 d) (SoA) and 6.1.3 e) (RTP) are produced. Implementation follows under Clause 8. Option C places the SoA before treatment decisions, which is impossible because the SoA documents those decisions. Option B makes the SoA the starting point, contradicting the risk-driven approach. Option A inverts the entire logic.

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

`Trap pattern: T-01 SoA vs Risk Treatment Plan`

Q5 Correct answer: **B.** Risk avoidance: the activity creating the risk will be ceased

ISO/IEC 27005:2022 Clause 8.5 defines risk avoidance as ceasing the activity that gives rise to the risk. Migrating off the mainframe is exactly that. Option A confuses 'temporary continued operation while migrating' with formal risk acceptance: acceptance means the risk stays. Option C labels migration as 'control modification', but migration removes the risk source rather than reducing it. Option D mis-frames the new platform: the original mainframe risk is eliminated, not transferred (the new platform has different risks that need their own assessment).

Cited: ISO/IEC 27005:2022, Clause 8.5

Trap pattern: T-03 Risk treatment verb swap

Q6 Correct answer: **A.** Producing the Statement of Applicability and Risk Treatment Plan

Producing the SoA and RTP sits in Clause 6 (Planning), which is the implementation phase. Options B, C, and D all belong to operation, performance evaluation, or improvement (Clauses 9 and 10): the running ISMS, not the initial build. Implementation-vs-operation confusion is the T-02 trap: candidates put operational artefacts in the build phase or vice versa.

Cited: ISO/IEC 27001:2022, Clause 6.1.3 (with ISO/IEC 27003:2017 guidance)

Trap pattern: T-02 Implementation vs operation phase

Q7 Correct answer: **B.** The necessary controls, the justification for their inclusion, whether each is implemented, and the justification for excluding any Annex A control

Clause 6.1.3 d) lists exactly the four items in Option B: necessary controls, justifications for inclusion, implementation status, and justifications for any Annex A exclusions. Option A mis-frames the SoA as a risk-ranked list. Option D describes RTP content (Clause 6.1.3 e) and acceptance approvals): the classic SoA-vs-RTP swap. Option C describes audit artefacts, which belong to Clause 9.2.

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

Trap pattern: T-01 SoA vs Risk Treatment Plan

Q8 Correct answer: **B.** Update the Risk Treatment Plan with additional controls, OR seek formal risk owner approval to retain the residual risk above criteria

Clause 6.1.3 f) requires formal risk owner approval where residual risk falls outside the documented acceptance criteria, OR further treatment to bring it within criteria. Option B captures both legitimate paths. Option D changes the criteria to suit one risk, which corrupts the acceptance framework. Option C uses the SoA as a residual-risk register, which is the classic SoA-vs-RTP confusion: residuals belong in the risk register, not the SoA. Option A forces avoidance when acceptance with explicit approval is also valid.

Cited: ISO/IEC 27001:2022, Clause 6.1.3 f)

Trap pattern: T-01 SoA vs Risk Treatment Plan

Q9 Correct answer: **D.** React, evaluate the need to eliminate the cause, implement actions, review effectiveness, and update the ISMS if necessary

Clause 10.2 prescribes a five-step sequence: react, evaluate the cause, implement actions, review effectiveness, update the ISMS if needed. Option D matches that. Option C uses the SoA as a corrective-action register (wrong artefact). Option A is the implementation-vs-operation phase trap: a nonconformity during operation is handled in Clause 10.2, not by returning to Clause 6. Option B delays corrective action beyond what the standard permits and mis-frames the certification body's role.

Cited: ISO/IEC 27001:2022, Clause 10.2

Trap pattern: T-02 Implementation vs operation phase

Q10 Correct answer: **B.** The risk owner, under Clause 6.1.3 f)

Clause 6.1.3 f) explicitly assigns residual-risk approval to the risk owner. Option C confuses risk-owner approval with top-management leadership commitment, which is a separate Clause 5.1 obligation. Option A invokes the internal auditor, who reviews but does not approve. Option D mis-frames the certification body: they review for conformance, not approve risk decisions. The 'who approves what' confusion is a SoA-vs-RTP-adjacent trap because candidates also conflate it with the management approvals around the RTP.

Cited: ISO/IEC 27001:2022, Clause 6.1.3 f)

Trap pattern: T-01 SoA vs Risk Treatment Plan

Want the full bank?

Mindset Prep has 450+ clause-cited ISO 27001 Lead Implementer 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-li