ISO 27001 Foundation practice questions and answers

> **Original practice questions written from ISO/IEC 27001:2022 and ISO/IEC 27002:2022. 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-foundation/.

QUESTION 1

Hollis & Brandt Accountants tells its office staff to put client papers away and lock their computer screens whenever they leave their desks. Which Annex A theme holds the control requiring both rules?

A. People

B. Physical

C. Technological

QUESTION 2

An ISMS team sets an objective to build a culture in which staff report security mistakes without fear, and finds no practicable way to measure it. Which of these does Clause 6.2 still require for this objective?

A. Approval as an exception by top management

B. A justification recorded in the SoA

C. Monitoring of its progress over time

QUESTION 3

An organization briefs all staff on its new security policy and puts its firewall team through vendor certification training, keeping their certificates. Which ISO/IEC 27001:2022 clause covers the team's training?

A. Clause 7.2 Competence

B. Clause 7.4 Communication

C. Clause 7.3 Awareness

QUESTION 4

A company's document system adds a hidden 'Restricted' tag to each file's properties so its email gateway can stop such files leaving automatically. Which control does adding the tag implement?

A. Control 5.12 Classification of information

B. Control 5.13 Labelling of information

C. Control 5.14 Information transfer

QUESTION 5

An organization plans to move its customer database to a new hosting provider next quarter. Which clause of ISO/IEC 27001:2022 requires a risk assessment to be performed because of this change?

A. Clause 6.3 Planning of changes

B. Clause 6.1.2 Information security risk assessment

C. Clause 8.2 Information security risk assessment

QUESTION 6

During a power cut, the servers keep running on a backup generator, but the server room's air-conditioning is not wired to it and stops, so the servers overheat. Which Annex A control MOST directly covers this gap?

A. Supporting utilities

B. Equipment siting and protection

C. Equipment maintenance

QUESTION 7

A document states that backups of information, software and systems should be kept and regularly tested in line with the topic-specific backup policy. Which document is it?

A. ISO/IEC 27003

B. ISO/IEC 27001 Annex A

C. ISO/IEC 27002

QUESTION 8

A company's information security policy says nothing about how requests for exceptions to the policy are handled. How should this gap be classed?

A. A departure from ISO/IEC 27002 guidance

B. A nonconformity with Clause 5.2

C. A nonconformity with Annex A Control 5.1

QUESTION 9

Which ISO/IEC 27001 requirement most directly reflects the process approach?

A. Including processes and their interactions in the ISMS

B. Defining and applying a risk assessment process

C. Considering interfaces and dependencies for the scope

QUESTION 10

Ransomware that reached one office PC encrypted every server in the company within an hour. Every device could connect directly to every other device. Which control would MOST directly have limited how far it spread?

A. Control 8.7 (protection against malware)

B. Control 8.22 (segregation of networks)

C. Control 8.20 (networks security)

Answers

Q1 Correct answer: **B.** Physical

ISO/IEC 27001:2022 Annex A places clear desk and clear screen rules (Control 7.7) in the physical theme. That staff carry the rules out, or that software can lock screens, does not move the control into the people or technological theme.

`Cited: ISO/IEC 27001:2022 Annex A`

`Trap pattern: T-01 Look-alike controls`

Q2 Correct answer: **C.** Monitoring of its progress over time

Clause 6.2 says information security objectives shall be measurable if practicable, so a sound objective that cannot sensibly be measured is allowed. The clause's other requirements still apply to it, and monitoring is one of them. Monitoring means keeping track of status, which does not depend on having a number to report.

`Cited: ISO/IEC 27001:2022 Clause 6.2`

`Trap pattern: T-02 Requirement vs good practice`

Q3 Correct answer: **A.** Clause 7.2 Competence

One activity can look like another, so ask what it achieves. Building the skills a role needs, through education, training or experience, and keeping evidence such as certificates is competence in Clause 7.2. Making sure people know the policy and their part in the ISMS is awareness in Clause 7.3, and planning what is communicated, when, with whom and how is Clause 7.4.

`Cited: ISO/IEC 27001:2022 Clause 7.2`

`Trap pattern: T-03 Neighbouring clauses`

Q4 Correct answer: **B.** Control 5.13 Labelling of information

Classification (Control 5.12) decides the level; labelling (Control 5.13) puts that level on the information so it can be recognized. ISO/IEC 27002 gives supporting automation as part of the purpose of labelling and recommends metadata for digital information, so that systems can make decisions based on the label.

`Cited: ISO/IEC 27002:2022 Control 5.13`

`Trap pattern: T-01 Look-alike controls`

Q5 Correct answer: **C.** Clause 8.2 Information security risk assessment

Risk assessment appears twice in ISO/IEC 27001:2022. Clause 6.1.2, part of planning, defines the process and its criteria. Clause 8.2, part of operation, requires assessments to be performed at planned intervals and whenever significant changes are proposed or occur, with the results retained as documented information. A proposed hosting move is exactly that kind of trigger.

`Cited: ISO/IEC 27001:2022 Clause 8.2`

`Trap pattern: T-03 Neighbouring clauses`

Q6 Correct answer: **A.** Supporting utilities

Supporting utilities are more than the power feed to the servers. ISO/IEC 27002 lists ventilation and air conditioning alongside electricity, water and telecommunications. Annex A Control 7.11 requires information processing facilities to be protected from disruptions caused by utility failures, so the servers' cooling needs protecting against a power cut as well.

Cited: ISO/IEC 27002:2022 Control 7.11

Trap pattern: T-01 Look-alike controls

Q7 Correct answer: **C.** ISO/IEC 27002

Control 8.13 Information backup reads almost the same in both documents, so the verb decides. ISO/IEC 27001 Annex A states it with 'shall', the wording of a requirement. ISO/IEC 27002 states it with 'should', the wording of guidance. ISO/IEC 27003 is guidance too, but it covers the ISMS clauses, not individual controls.

Cited: ISO/IEC 27002:2022 Control 8.13

Trap pattern: T-02 Requirement vs good practice

Q8 Correct answer: **A.** A departure from ISO/IEC 27002 guidance

ISO/IEC 27001 Clause 5.2 sets the content requirements for the information security policy, and exception handling is not one of them. ISO/IEC 27002 recommends extra statements, such as how exemptions and exceptions are handled, but its guidance is not mandatory. The gap is worth closing, yet it is not a nonconformity.

Cited: ISO/IEC 27002:2022 Control 5.1

Trap pattern: T-02 Requirement vs good practice

Q9 Correct answer: **A.** Including processes and their interactions in the ISMS

The process approach treats a management system as a set of processes whose interactions are identified and managed. ISO/IEC 27001 Clause 4.4 reflects it by requiring the ISMS to include the processes needed and their interactions. Scope interfaces (Clause 4.3) and the risk assessment process (Clause 6.1.2) also involve processes or activities, but neither is about how the ISMS processes fit together.

Cited: ISO/IEC 27001:2022 Clause 4.4

Trap pattern: T-03 Neighbouring clauses

Q10 Correct answer: **B.** Control 8.22 (segregation of networks)

The ransomware spread so far because nothing stood between the office PCs and the servers. Annex A Control 8.22 requires groups of services, users and systems to be kept separate within the organization's networks. ISO/IEC 27002 describes splitting a network into domains, such as a desktop domain and a server domain, with traffic between them controlled at the perimeter.

Cited: ISO/IEC 27002:2022 Control 8.22

Trap pattern: T-01 Look-alike controls

Want the full bank?

Mindset Prep has 250+ clause-cited ISO 27001 Foundation 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-f