PassQueen
a.k.a dumpsqueen.com

ISO 27001:2013 ISMS - Certified Lead Auditor

GAQM ISO-ISMS-LA

Version Demo

Total Demo Questions: 13

Total Premium Questions: 134

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which measure is a preventive measure?

A. Installing a logging system that enables changes in a system to be recognized

B. Shutting down all internet traffic after a hacker has gained access to the company systems

C. Putting sensitive information in a safe

ANSWER: C

Explanation:

“Putting sensitive information in a safe” is a preventive measure because it establishes a physical barrier before an unauthorized access event can occur. A safe limits access to authorized people who hold the key, combination, or other approved means of entry, thereby reducing the likelihood of theft, disclosure, loss, or tampering involving sensitive paper records, storage media, or other physical information assets. In an ISMS, preventive controls are selected and implemented to reduce risk proactively by stopping, deterring, or constraining an undesirable event at its source. Physical protection of information is therefore an important part of information-security risk treatment, alongside administrative and technical safeguards. The precise safeguards should be proportionate to the information classification, asset value, threat environment, and risk assessment results; for highly sensitive material, access to the safe may also be controlled, recorded, and periodically reviewed. This approach aligns with ISO/IEC 27001’s requirement to determine and apply appropriate information-security risk treatment controls and with established physical-protection control practices. See the ISO/IEC 27001 standard overview and NIST’s SP 800-53 security and privacy controls.

QUESTION NO: 2

Which of the following statements are correct for Clean Desk Policy?

A. Don't leave confidential documents on your desk.

B. Don't leave valuable items on your desk if you are not in your work area.

C. Don't leave highly confidential items.

D. Don't leave laptops without cable lock.

ANSWER: A B C D

Explanation:

A clean desk policy requires personnel to protect information and assets whenever a workspace is unattended or accessible to unauthorized people. “Don't leave confidential documents on your desk.” is correct because documents containing sensitive information must be removed from view and secured, such as in a locked drawer or cabinet. “Don't leave valuable items on your desk if you are not in your work area.” is also correct because portable assets and items of value require physical protection when their owner is absent. “Don't leave highly confidential items.” correctly reinforces the need for especially careful handling of highly sensitive records, media, and materials. “Don't leave laptops without cable lock.” is correct when a laptop is left at a desk: the device should be secured with an appropriate physical locking mechanism or otherwise removed and stored securely. These practices support the clear-desk and clear-screen objective in ISO/IEC 27001:2013 Annex A, which seeks to reduce opportunities for unauthorized access, disclosure, loss, or theft of information and equipment. ISO guidance describes clear-desk and clear-screen controls as part of physical and environmental security; see ISO/IEC 27001:2013 and ISO/IEC 27002:2013.

QUESTION NO: 3

Which of the following statements are correct for an ISMS internal audit programme? (Choose three)

A. The importance of the processes concerned

B. Changes affecting the organization

C. Results of previous audits

D. Auditors should audit their own work to confirm technical accuracy

ANSWER: A B C

Explanation:

An internal audit programme should take account of **the importance of the processes concerned**, **changes affecting the organization**, and **the results of previous audits**. These factors support a risk-based audit programme in which important, changed, or previously weak areas receive suitable audit attention.

Auditors must also be selected and audits conducted to ensure objectivity and impartiality. An auditor should not audit his or her own work because this would compromise independence. ISO/IEC 27001:2013 clause 9.2 requires the organization to plan, establish, implement, and maintain audit programmes and retain documented information as evidence of audit programme implementation and audit results. See ISO/IEC 27001:2013.

QUESTION NO: 4

Which of the following are appropriate sources of objective evidence during an ISMS audit? (Choose three)

A. Documented information and records

B. Observations of activities and conditions

C. Interviews corroborated by other evidence

D. The auditor's personal opinion of the auditee

ANSWER: A B C

Explanation:

Documented information and records, **observations of activities and conditions**, and **interviews corroborated by other evidence** are appropriate sources of objective evidence. An auditor gathers verifiable information relevant to the audit criteria and evaluates it to determine conformity. Records may demonstrate that activities were performed, observation can confirm how a process operates in practice, and interviews can provide useful evidence when their content is validated through records, observation, or other reliable sources.

An auditor's personal assumptions are not objective evidence. Audit conclusions must be based on evidence that can be evaluated against requirements, rather than on unsupported impressions. Guidance on collecting and evaluating audit evidence is available in ISO 19011:2018.

QUESTION NO: 5

Stages of Information

A. creation, evolution, maintenance, use, disposition

B. creation, use, disposition, maintenance, evolution

C. creation, distribution, use, maintenance, disposition

D. creation, distribution, maintenance, disposition, use

ANSWER: C

Explanation:

The correct lifecycle is **creation, distribution, use, maintenance, disposition**. Information first comes into existence through creation or collection. It is then distributed to authorized people, systems, or processes that need it. During use, the information supports business activities and decisions; the ISMS must ensure that access, handling, and protection remain appropriate to its classification and associated risks. Maintenance follows as information is stored, updated, retained, backed up, and kept available and accurate for as long as business, legal, regulatory, or contractual requirements demand. Finally, disposition addresses the controlled end of the lifecycle, including archival, transfer, destruction, or secure disposal so that confidentiality is protected after active use ends. This sequence is useful in ISO 27001 auditing because controls should be considered across the full information lifecycle rather than only while information is actively being used. ISO/IEC 27001 requires organizations to determine and manage information-security risks within their ISMS, while secure disposition is reinforced by NIST guidance on media sanitization. See the ISO/IEC 27001 standard overview and NIST SP 800-88 Rev. 1.

QUESTION NO: 6

You are the lead auditor of the courier company SpeeDelivery. You have carried out a risk analysis and now want to determine your risk strategy. You decide to take measures for the large risks but not for the small risks.

What is this risk strategy called?

A. Risk bearing

B. Risk avoidance

C. Risk neutral

D. Risk skipping

ANSWER: A

Explanation:

Risk bearing is correct because it describes retaining, or accepting, risks that the organization has assessed as sufficiently small to remain within its defined risk appetite or acceptance criteria. Risk treatment is not necessarily a single uniform action applied to every identified risk. After analysis and evaluation, management can prioritize material risks for treatment measures while consciously bearing residual or low-level risks where further controls would be disproportionate to the expected benefit. This decision should be explicit, authorized at the appropriate management level, and recorded as part of the risk-treatment process.

In an ISO 27001 ISMS, risk treatment requires organizations to select suitable treatment options and obtain risk-owner approval of both the treatment plan and residual information-security risks. Thus, taking measures for the significant risks while retaining the minor, acceptable risks is a practical application of risk bearing. The decision remains subject to review, because a change in likelihood, impact, legal obligations, or business context may mean that a previously acceptable risk needs treatment later. See ISO's overview of ISO 31000 risk-management principles and the ISO/IEC 27001 standard page covering information security management systems.

QUESTION NO: 7

Which of the following are valid information security risk treatment options? (Choose three)

A. Avoiding the activity that gives rise to the risk

B. Modifying likelihood or consequence through controls

C. Sharing the risk through an appropriate contractual or insurance arrangement

D. Ignoring the risk until an incident occurs

ANSWER: A B C

Explanation:

Avoiding the risk, **modifying the risk through controls**, and **sharing the risk with another party** are valid risk-treatment options. Risk avoidance can involve deciding not to start or continue an activity that creates the risk. Risk modification can reduce likelihood or consequence through safeguards such as access controls, monitoring, segregation, or resilience measures. Risk sharing may involve contractual arrangements or insurance, although such arrangements do not remove the organization's accountability for managing its risks.

ISO/IEC 27001 also permits retaining risk by informed decision when it meets the organization's risk acceptance criteria. Ignoring an identified risk without evaluation, authorization, or monitoring is not a risk-treatment option. See ISO/IEC 27001:2013 and ISO 31000 risk management.

QUESTION NO: 8

Which of the following are required inputs to an ISMS management review? (Choose three)

A. Results of internal audits

B. Status of actions from previous management reviews

C. Changes in external and internal issues relevant to the ISMS

D. Individual employees' private preferences

ANSWER: A B C

Explanation:

Results of internal audits, **the status of actions from previous management reviews**, and **changes in external and internal issues relevant to the ISMS** are management-review inputs under ISO/IEC 27001:2013 clause 9.3.2. Top management needs this information to determine whether the ISMS remains suitable, adequate, and effective.

Other required inputs include feedback from interested parties, results of monitoring and measurement, fulfilment of information security objectives, performance of risk treatment, nonconformities and corrective actions, and opportunities for continual improvement. Individual employees' private preferences are not a required management-review input unless they form part of relevant interested-party feedback or another defined performance measure. See ISO/IEC 27001:2013.

QUESTION NO: 9

What type of compliancy standard, regulation or legislation provides a code of practice for information security?

A. ISO/IEC 27002

B. Personal data protection act

C. Computer criminality act

D. IT Service Management

ANSWER: A

Explanation:

ISO/IEC 27002 is correct because it is the international standard specifically titled *Information security, cybersecurity and privacy protection — Information security controls*, and it serves as the recognized code of practice for selecting, implementing, and managing information-security controls. It provides guidance on a broad set of controls, including organizational, people, physical, and technological controls, which organizations can use to address information-security risks. In an ISO 27001 ISMS context, ISO/IEC 27002 is an important supporting guidance document: ISO/IEC 27001 establishes requirements for an information security management system, while ISO/IEC 27002 offers practical control guidance that helps organizations determine how suitable controls can be applied. Its role as a code of practice is reflected in its history and continuing use as the principal control-guidance standard in the ISO/IEC 27000 family. The International Organization for Standardization describes ISO/IEC 27002 as providing guidance on information-security controls, and ISO's

ISO/IEC 27001 overview identifies it as a related standard supporting ISMS implementation. See ISO/IEC 27002:2022 overview and ISO's ISO/IEC 27001 information-security overview.

QUESTION NO: 10

What is an example of a human threat?

A. a lightning strike

B. fire

C. phishing

D. thunderstrom

ANSWER: C

Explanation:

Phishing is an example of a human threat because it is a deliberate social-engineering attack performed by people. An attacker typically impersonates a trusted organization, colleague, or service and uses email, messages, or fraudulent websites to persuade a recipient to disclose credentials, financial information, or other sensitive data, or to open a malicious attachment or link. In an information security management system, phishing is therefore assessed as a threat source involving human action and intent. Its potential consequences include unauthorized access to information assets, compromise of user accounts, malware infection, and loss of confidentiality, integrity, or availability. ISO/IEC 27001 requires organizations to identify and address information-security risks in a way appropriate to their context; phishing is a common risk scenario that can be treated through measures such as security awareness training, email filtering, multi-factor authentication, incident reporting, and access controls. The UK National Cyber Security Centre provides practical guidance on recognizing and reporting phishing at https://www.ncsc.gov.uk/guidance/spotting-and-reporting-phishing-scams. ISO's overview of ISO/IEC 27001 and its risk-based ISMS approach is available at https://www.iso.org/standard/27001.html.

QUESTION NO: 11

What is the purpose of an Information Security policy?

A. An information security policy makes the security plan concrete by providing the necessary details

B. An information security policy provides insight into threats and the possible consequences

C. An information security policy provides direction and support to the management regarding information security

D. An information security policy documents the analysis of risks and the search for countermeasures

ANSWER: C

Explanation:

An information security policy provides direction and support to the management regarding information security. At the ISMS leadership level, the policy is the formal statement through which top management establishes the organization's information-security intent, sets an appropriate overall direction, and demonstrates commitment to the ISMS. It gives management and personnel a common framework for making security decisions, defining objectives, assigning responsibilities, and ensuring that information-security activities support the organization's business needs and risk environment.

ISO/IEC 27001 requires top management to establish an information security policy that is appropriate to the organization's purpose, includes information-security objectives or a framework for setting them, commits to meeting applicable requirements, and commits to continual improvement. The policy must also be communicated within the organization and made available to relevant interested parties as appropriate. In an audit, this makes the policy an essential piece of leadership evidence: it should show clear management sponsorship and provide the high-level basis from which ISMS

processes, controls, objectives, and operational practices are governed. See the ISO overview of ISO/IEC 27001 and ISO's guidance on information security management.

QUESTION NO: 12

Phishing is what type of Information Security Incident?

A. Private Incidents

B. Cracker/Hacker Attacks

C. Technical Vulnerabilities

D. Legal Incidents

ANSWER: B

Explanation:

"Cracker/Hacker Attacks" is the appropriate classification because phishing is a deliberate, adversarial social-engineering attack used to obtain unauthorized access to information, accounts, systems, or financial assets. A threat actor typically impersonates a trusted organization or person through email, messaging, websites, or other communications, then persuades a target to disclose credentials, open malicious content, approve a fraudulent request, or provide sensitive information. The immediate mechanism is deception, but the security objective is commonly credential theft and subsequent unauthorized system access, which places the activity within an attacker-driven incident category.

For ISMS incident handling, identifying phishing as an external attack helps ensure that the organization activates suitable response activities: preserve the suspicious message and related logs, determine whether credentials or data were exposed, contain affected accounts or endpoints, reset credentials where needed, and assess potential unauthorized access. The UK National Cyber Security Centre describes phishing as fraudulent communications intended to trick people into taking harmful actions, while CISA identifies phishing as a common method used by malicious actors to steal information or gain access. See NCSC phishing guidance and CISA phishing guidance.

QUESTION NO: 13

Four types of Data Classification (Choose two)

A. Restricted Data, Confidential Data

B. Project Data, Highly Confidential Data

C. Financial Data, Highly Confidential Data

D. Unrestricted Data, Highly Confidential Data

ANSWER: A D

Explanation:

"Restricted Data, Confidential Data" and "Unrestricted Data, Highly Confidential Data" correctly identify the four classification levels used in this question: Unrestricted, Confidential, Highly Confidential, and Restricted. A classification scheme enables an organization to apply security controls that are proportionate to the sensitivity of information and the consequences of unauthorized disclosure, modification, loss, or unavailability. Unrestricted information can generally be shared broadly, whereas confidential and highly confidential information require progressively stronger handling protections. Restricted information represents information requiring the greatest degree of protection and the most limited access. Grouping the labels into these two pairs therefore accounts for all four levels without treating a business subject, such as finance or projects, as a classification level. ISO/IEC 27001 requires organizations to determine and apply information-security controls based on risk within their information security management system; classification and handling arrangements are common means of doing this. ISO/IEC 27002 provides guidance on information classification and associated handling procedures. See the ISO/IEC 27001 standard overview and the ISO/IEC 27002 guidance overview.