PassQueen
a.k.a dumpsqueen.com

ISO 27001 : 2013 - Certified Lead Auditor

GAQM ISO27-13-001

Version Demo

Total Demo Questions: 12

Total Premium Questions: 129

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which of the following does an Asset Register contain? (Choose two)

A. Asset Type

B. Asset Owner

C. Asset Modifier

D. Process ID

ANSWER: A B

Explanation:

An asset register is the maintained inventory used to identify and manage information assets and supporting assets within the information security management system. “Asset Type” is an appropriate register entry because categorising an item—for example, information, software, hardware, service, person, or facility—helps the organisation apply suitable handling, protection, lifecycle, and risk-management activities. Classification by type also supports consistent reporting and the determination of relevant controls.

“Asset Owner” is also a fundamental entry. Ownership assigns accountability for ensuring that the asset is identified, protected appropriately, reviewed, and handled according to organisational requirements. The owner need not be the person who physically possesses or technically administers the asset; rather, the owner is the accountable role with authority to make decisions regarding its protection and use. ISO/IEC 27001 requires organisations to identify assets associated with information and information-processing facilities and establish an inventory, while its asset-management control framework includes assigning ownership. These entries therefore provide both essential identification context and clear accountability for each registered asset. See the ISO/IEC 27001 standard overview and the NIST security-control catalog, which describes maintaining an inventory of system components as an asset-management practice.

QUESTION NO: 2

Availability means

A. Service should be accessible at the required time and usable by all

B. Service should be accessible at the required time and usable only by the authorized entity

C. Service should not be accessible when required

ANSWER: B

Explanation:

“Service should be accessible at the required time and usable only by the authorized entity” is correct because availability in information security is the property that information, systems, and services are accessible and usable when needed by an authorized entity. In an ISO/IEC 27001 information security management system, availability is one of the core information-security properties, alongside confidentiality and integrity. It is not limited to a system merely being online; the service must remain operational enough for approved users or entities to obtain and use it at the time it is required. This objective is supported through risk-based controls such as capacity management, redundancy, backup and restoration arrangements, monitoring, incident response, and business-continuity planning. The wording concerning an authorized entity also reflects that availability must be managed together with access control: a service should be available to legitimate users without permitting inappropriate access. ISO describes availability as a property of information security in its overview of ISO/IEC 27001 and related standards. See the ISO/IEC 27001 standard page and NIST’s definition of availability.

QUESTION NO: 3

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: C

Explanation:

Risk neutral is correct because the company differentiates its response according to the assessed magnitude of each risk. Under this approach, significant risks receive treatment measures, such as reducing their likelihood or limiting their consequences, while minor risks are consciously retained because further controls would not be proportionate to their expected impact. This reflects a balanced decision based on the organization's risk criteria, available resources, and the cost-versus-benefit of treatment.

In an ISO 27001 information-security management system, risk treatment is not expected to eliminate every possible risk. The organization must define criteria for evaluating risks and select appropriate treatment actions for risks that require action. Risks that fall within the organization's acceptance criteria may be retained with an informed management decision. This is consistent with a risk-neutral posture: action is targeted at material exposures rather than automatically being applied to every identified risk. ISO describes risk management as supporting decisions that create and protect value, including decisions on whether and how risks should be treated. See ISO 31000 risk management overview and NIST SP 800-30 Rev. 1.

QUESTION NO: 4

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

A. Approved records of access reviews

B. Configuration records from an information system

C. An auditor's personal belief that a control works

D. An employee's unsupported opinion

ANSWER: A B

Explanation:

Approved records of access reviews and configuration records from an information system are suitable sources of objective evidence. Access-review records can demonstrate that user privileges have been reviewed, authorized, and removed or amended where required. System configuration records can support verification that technical settings have been implemented and maintained in accordance with approved requirements.

An auditor should obtain verifiable evidence through interviews, observation, and examination of documented information and records. Personal assumptions or informal opinions are not objective evidence because they cannot reliably demonstrate that a control has been implemented or is effective. ISO/IEC 27001 requires documented information to be available as evidence of the operation of processes, while ISO 19011 provides guidance on obtaining and evaluating audit evidence. See ISO/IEC 27001:2013 and ISO 19011 auditing guidance.

QUESTION NO: 5

Which of the following are suitable controls for reducing the risk of unauthorized wireless-network access? (Choose two)

A. Use strong authentication and encryption for wireless connections

B. Change default administrative credentials on wireless equipment

C. Publish the wireless administrator password on a notice board

D. Disable all authentication to simplify guest access

ANSWER: A B

Explanation:

Use strong authentication and encryption for wireless connections and *Change default administrative credentials on wireless equipment* are correct. Strong, properly configured wireless authentication and encryption protect network traffic and make it more difficult for unauthorized persons to join or monitor the network. Changing default administrative credentials prevents attackers from using publicly known factory passwords to take control of access points or routers.

Wireless equipment should also be securely configured, patched, monitored, and managed according to documented procedures. Broadcasting credentials or disabling authentication would increase exposure rather than reduce it. The selection of controls should be based on the organization's risk assessment and the sensitivity of the systems reachable through the wireless network. Guidance on wireless security is available in NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks. See also the ISO/IEC 27001:2013 standard page.

QUESTION NO: 6

Which of the following are inputs to information-security risk assessment? (Choose two)

A. Potential consequences of loss of confidentiality, integrity or availability

B. Likelihood that an identified risk will occur

C. Date of the next external certification audit

D. Preferred writing style for policies

ANSWER: A B

Explanation:

Potential consequences of a loss of confidentiality, integrity, or availability and the likelihood that an identified risk will occur are correct inputs. The organization needs defined risk criteria and a consistent method to evaluate the potential impact and likelihood of relevant risk scenarios. This enables risks to be compared and prioritized against the organization's risk acceptance criteria.

Risk assessment also considers assets, threats, vulnerabilities, existing controls, legal and contractual requirements, and business context. The date of the next external certification audit or the preferred writing style for policies does not determine the level of information-security risk. ISO/IEC 27001:2013 requires the organization to define and apply an information-security risk assessment process that produces consistent, valid, and comparable results. See the ISO/IEC 27001:2013 standard page and ISO/IEC 27005 risk management guidance.

QUESTION NO: 7

Which of the following should be considered when information-security requirements are included in supplier agreements? (Choose two)

A. Security responsibilities of the supplier

B. Notification requirements for information security incidents

C. Permission for unrestricted reuse of customer information

D. A commitment to provide services without security terms

ANSWER: A B

Explanation:

Security responsibilities of the supplier and notification requirements for information-security incidents are correct selections. Agreements with suppliers should clearly establish the security obligations expected from each party, including how information is protected, who is responsible for relevant controls, and how compliance may be monitored. Incident-notification requirements are also important because the organization needs timely information to assess, contain, and manage an event affecting its information or services.

Supplier arrangements should address the risks associated with access to, processing of, storage of, communication of, or provision of components for the organization's information. A general commitment to provide services without security terms does not provide sufficient assurance, and unrestricted reuse of customer information would conflict with confidentiality obligations. ISO/IEC 27001:2013 Annex A control A.15.1 addresses information security in supplier relationships. See the ISO/IEC 27001:2013 standard page.

QUESTION NO: 8

You receive the following mail from the IT support team: Dear User,Starting next week, we will be deleting all inactive email accounts in order to create spaceshare the below details in order to continue using your account. In case of no response,

Name:

Email ID:

Password:

DOB:

Kindly contact the webmail team for any further support. Thanks for your attention.

Which of the following is the best response?

A. Ignore the email

B. Respond it by saying that one should not share the password with anyone

C. One should not respond to these mails and report such email to your supervisor

ANSWER: C

Explanation:

One should not respond to these mails and report such email to your supervisor is the best response because the message displays common phishing characteristics: urgency, a threat of account deletion, generic wording, and a request for highly sensitive information, especially a password. Legitimate IT support personnel should not request a user's password by email, since passwords are authentication secrets that must remain known only to the account holder. Reporting the suspected phishing message through the organization's established process—such as to a supervisor, service desk, security team, or phishing-reporting mailbox—allows the organization to investigate it, warn other users, block malicious senders or links, and preserve evidence. This supports ISO/IEC 27001 information-security awareness and incident-reporting practices, which depend on personnel recognizing and promptly reporting suspected security events. The user should avoid replying, clicking links, opening attachments, or providing any requested details. Guidance from the U.S. Cybersecurity and Infrastructure Security Agency similarly advises users to recognize and report phishing. The UK National Cyber Security Centre also emphasizes that credential requests and pressure tactics are important phishing warning signs.

QUESTION NO: 9

Which management activity evaluates the continuing suitability, adequacy and effectiveness of the ISMS?

A. Management review

B. Vulnerability scanning

C. User access provisioning

D. Configuration backup

ANSWER: A

Explanation:

Management review is correct because top management is required to review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy, and effectiveness. The review considers relevant changes, performance information, audit results, nonconformities and corrective actions, monitoring and measurement results, fulfillment of objectives, and opportunities for continual improvement.

Management review is not merely a review of individual security incidents or a technical system-health check. Its purpose is to enable leadership to make informed decisions about the ISMS, including changes to the system, resources, and improvement actions. Documented information should be retained as evidence of the results of management reviews. ISO/IEC 27001:2013 clause 9.3 establishes these requirements. See the ISO/IEC 27001:2013 standard page.

QUESTION NO: 10

How are data and information related?

A. Data is a collection of structured and unstructured information

B. Information consists of facts and statistics collected together for reference or analysis

C. When meaning and value are assigned to data, it becomes information

ANSWER: C

Explanation:

When meaning and value are assigned to data, it becomes information. Data comprises raw facts, observations, measurements, symbols, or values that have not necessarily been interpreted in context. Information results when those data elements are processed, organized, analyzed, or contextualized so that they convey meaning and can support understanding or action. For example, individual access-log entries are data; correlating them to identify repeated failed sign-in attempts from a particular source produces information that may support an information-security decision. This distinction matters in an ISO/IEC 27001 context because an organization needs to identify and protect information in all relevant forms, including the data from which meaningful information can be derived. ISO/IEC 27000 defines information as data that has meaning, reinforcing the relationship expressed in the answer. Effective information security management therefore considers both the raw data handled by systems and the contextual information created through processing, reporting, aggregation, and analysis. See the ISO/IEC 27000 overview at ISO/IEC 27000: Information security management systems — Overview and vocabulary and ISO's overview of the ISO/IEC 27001 standard at ISO/IEC 27001 information security management.

QUESTION NO: 11

Which of the following are characteristics of an effective information security policy? (Choose two)

A. It is approved by management

B. It is communicated to persons who need to understand it

C. It is kept confidential from all employees

D. It is never changed after first publication

ANSWER: A B

Explanation:

It is approved by management and *It is communicated to persons who need to understand it* are correct. Management approval demonstrates leadership direction and establishes the policy as an authorized organizational requirement. Communication ensures that employees, contractors, and other relevant interested parties understand the security principles, obligations, and expectations that apply to them.

An effective policy should also be appropriate to the organization's purpose, provide a framework for information-security objectives, and be reviewed when necessary to remain suitable. A policy is not effective merely because it has been written or stored in a document repository. ISO/IEC 27001:2013 requires top management to establish an information-security policy and ensure it is available and communicated as appropriate. See the ISO/IEC 27001:2013 standard page and ISO's information security management overview.

QUESTION NO: 12

You receive an E-mail from some unknown person claiming to be representative of your bank and asking for your account number and password so that they can fix your account.

Such an attempt of social engineering is called

A. Shoulder Surfing

B. Mountaineering

C. Phishing

D. Spoofing

ANSWER: C

Explanation:

Phishing is correct because it is a social-engineering technique in which an attacker impersonates a trusted organization, such as a bank, through an email or other electronic message to persuade a recipient to disclose sensitive information. The request for an account number and password, paired with a claim that the bank needs the details to "fix" the account, is intended to exploit trust and urgency rather than use a legitimate account-support process. Credentials collected this way can enable unauthorized access to financial accounts and other services where users reuse passwords.

Effective information-security awareness under an ISO/IEC 27001 information security management system includes helping personnel recognize and report suspicious messages, independently verify requests through official contact channels, and avoid providing passwords or account details in response to unsolicited communications. The UK National Cyber Security Centre describes phishing as fraudulent messages that attempt to trick people into providing sensitive information or taking unsafe actions. The U.S. Cybersecurity and Infrastructure Security Agency likewise identifies phishing as a common method used to steal credentials and other valuable data. See the NCSC phishing guidance and CISA phishing guidance.