PassQueen
a.k.a dumpsqueen.com

Certified ISO/IEC 27001:2022 Foundation

CertiProf I27001F

Version Demo

Total Demo Questions: 6

Total Premium Questions: 60

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Introduction to ISO/IEC 27001:2022	4
Topic 2, Information Security Management System (ISMS)	5
Topic 3, ISO/IEC 27001 Requirements	41
Topic 4, Risk Management	9
Topic 5, Annex A Controls	1
Total	60

QUESTION NO: 1

In the context of clause 6.1 actions to address risks and opportunities, the weakness of an asset or control that can be exploited by a threat is known as:

A. Threat

B. Risk

C. Vulnerability

D. Impact

ANSWER: C

Explanation:

Vulnerability is the correct term for a weakness in an asset, control, process, system, or other element that a threat can exploit. This definition is central to information-security risk assessment: a threat is a potential cause of an unwanted incident, whereas a vulnerability is the condition that may enable that threat to cause harm. For example, an unpatched server, weak password configuration, or inadequate physical access restriction can each represent a vulnerability. When an applicable threat can exploit such a weakness, the organization assesses the potential consequences and likelihood in order to determine and treat information-security risk.

ISO/IEC 27001:2022 clause 6.1 requires organizations to determine risks and opportunities that need to be addressed and, under clause 6.1.2, establish and maintain information-security risk-assessment processes. Identifying relevant vulnerabilities alongside threats and affected information assets supports a consistent, risk-based ISMS and helps select appropriate risk-treatment measures. The ISO overview of ISO/IEC 27001 describes the standard's risk-management basis: ISO/IEC 27001 — Information security management systems. Further terminology and risk-management context are available from the ISO/IEC 27000 family overview: ISO information security management.

QUESTION NO: 2

Within the ISMS, ensuring the integration of information security management system requirements into the organization's processes is a responsibility of:

A. The quality management representative

B. The IT Security Manager

C. The Operations Manager

D. Top management

ANSWER: D

Explanation:

Top management is responsible for ensuring that information security management system requirements are integrated into the organization's processes. ISO/IEC 27001:2022 places this obligation within its leadership requirements, recognizing that an ISMS can operate effectively only when information security is embedded in the organization's normal governance, planning, operational, and decision-making activities. This means top management must ensure that security considerations are incorporated into relevant business processes rather than being managed as a separate, isolated technical function.

This responsibility reflects the accountability of top management for the effectiveness of the ISMS. Senior leaders provide direction, align information-security objectives with organizational priorities, make resources available, and promote the use of the ISMS across the organization. Integration can include considering information-security risks in operational planning, change management, supplier relationships, project delivery, performance evaluation, and business processes. Although specific security activities may be assigned to managers or specialists, top management retains accountability for establishing the conditions in which ISMS requirements are incorporated and supported throughout the organization.

The relevant requirement is stated in ISO/IEC 27001 clause 5.1 on leadership and commitment. See the ISO/IEC 27001 standard overview from ISO and the ISO/IEC JTC 1/SC 27 ISO/IEC 27001 project page.

QUESTION NO: 3

Which of the following must be included in the ISMS policy?

A. The deadline for ISMS implementation

B. The certificate from previous audits

C. The result of a gap analysis

D. A commitment to continual improvement of the ISMS

ANSWER: D

Explanation:

A commitment to continual improvement of the ISMS must be included because ISO/IEC 27001:2022 clause 5.2 defines required content for the information security policy. The policy must be appropriate to the organization's purpose, provide a framework for information security objectives, include a commitment to satisfy applicable information-security requirements, and include a commitment to continual improvement of the information security management system. This commitment establishes that the ISMS is not a one-time implementation; it is to be maintained, monitored, reviewed, and improved as the organization's context, risks, obligations, and information-security needs evolve. The policy is a leadership-level direction-setting document, approved by top management and communicated within the organization and, where appropriate, to interested parties. A clear continual-improvement commitment therefore connects the policy to the ISMS improvement cycle and supports ongoing suitability, adequacy, and effectiveness. ISO describes ISO/IEC 27001 as specifying requirements for establishing, implementing, maintaining, and continually improving an ISMS: ISO/IEC 27001 information page. Further ISO guidance on the standard and its ISMS focus is available from the ISO ISO/IEC 27001 overview.

QUESTION NO: 4

According to ISO/IEC 27001:2022 clause 4.3, what aspects must be considered when determining the scope of the Information Security Management System?

A. Assets and resources

B. Risks and opportunities

C. Threats and vulnerabilities

D. External and internal issues, interested-party requirements, and interfaces and dependencies

ANSWER: D

Explanation:

External and internal issues, interested-party requirements, and interfaces and dependencies is correct because ISO/IEC 27001:2022 clause 4.3 requires an organization to define the ISMS boundaries and applicability using the organization's context. This determination must take account of the external and internal issues identified under clause 4.1, such as regulatory conditions, market circumstances, organizational structure, culture, and technological environment. It must also consider the requirements identified under clause 4.2, including relevant needs and expectations of interested parties that become legal, regulatory, contractual, or otherwise applicable information-security requirements.

In addition, the scope must address interfaces and dependencies between activities undertaken by the organization and activities undertaken by other organizations. This ensures that outsourced services, shared operational processes, suppliers, cloud providers, and other interconnected parties are appropriately considered when establishing ISMS boundaries. The resulting scope must be available as documented information, providing a clear statement of where the ISMS applies and supporting consistent risk management and control implementation. ISO describes ISO/IEC 27001 as the requirements standard for establishing, implementing, maintaining, and continually improving an ISMS: ISO/IEC 27001 overview. The official standard record is also available through the ISO Online Browsing Platform.

QUESTION NO: 5

A member of the system-administration team is scheduled to audit the privileged-access process that the same team operates. The auditor is competent and has not personally approved any access requests. What is the most appropriate audit arrangement?

A. Use a competent auditor independent of the system-administration team to audit the process

B. Allow the administrator to audit the process because the administrator did not approve requests personally

C. Cancel the audit because privileged access is too technical for an internal audit

D. Ask the certification body to perform the internal audit instead

ANSWER: A

Explanation:

Internal audits must be conducted in a way that ensures objectivity and impartiality. Although competence is necessary, assigning an auditor to audit a process operated by the auditor's own team can create a conflict of interest or reduce the credibility of the audit. The organization should arrange for an auditor who is sufficiently independent of the activity being audited while still competent to assess it. ISO/IEC 27001 does not require an external auditor for every internal audit.

QUESTION NO: 6

An organization's monitoring results show that phishing-reporting rates have declined for three consecutive quarters. Which activity is most appropriate for evaluating whether the ISMS remains effective?

A. Analyse and evaluate the trend against defined monitoring and measurement criteria

B. Discontinue monitoring because the reporting rate is a personnel issue

C. Replace the risk assessment process with an annual external audit

D. Accept the decline unless an information security incident has occurred

ANSWER: A

Explanation:

The decline should be analysed and evaluated using the methods and criteria the organization has determined for monitoring and measurement. ISO/IEC 27001:2022 clause 9.1 requires the organization to determine what to monitor and measure, the methods for valid results, when activities are performed, and when results are analysed and evaluated. The result can then inform corrective action, risk treatment, awareness activities, and management review. Collecting data without analysis would not demonstrate effective performance evaluation.