DUMPSBOSS.

ISO/IEC 27001 (2022) Foundation Exam

APMG-International ISO-IEC-27001-Foundation

Version Demo

Total Demo Questions: 7

Total Premium Questions: 71

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Introduction to ISO/IEC 27001	8
Topic 2, The requirements for an ISMS	31
Topic 3, Risk assessment and treatment	10
Topic 4, Annex A controls	22
Total	71

QUESTION NO: 1

Which activity is a required element of information security risk identification?

A. Determine the risk owners

B. Consider the likelihood of the occurrence

C. Prioritize the risk for treatment

D. Determine the level of risk

ANSWER: A

Explanation:

Determine the risk owners is a required activity within information security risk identification under ISO/IEC 27001:2022 clause 6.1.2. The organization must define and apply an information security risk assessment process that identifies risks associated with the loss of confidentiality, integrity, and availability of information within the scope of the ISMS. As part of identifying those risks, it must identify the risk owners. A risk owner is the person or entity accountable for managing a particular information security risk and for making appropriate decisions about its treatment or acceptance in accordance with the organization's established criteria. Assigning ownership at identification ensures that each identified risk has clear accountability throughout subsequent assessment, evaluation, treatment, monitoring, and review activities. This supports effective governance of the ISMS because decisions are made by parties with suitable authority and understanding of the relevant business context. ISO/IEC 27001 requires the process to be repeatable and to produce consistent, valid, and comparable results, making the identification of accountable risk owners an essential input to the wider risk-management lifecycle. See the ISO overview of ISO/IEC 27001 and APMG's ISO/IEC 27001 certification information.

QUESTION NO: 2

Which statement describes a purpose of monitoring, measurement, analysis and evaluation according to ISO/IEC 27001?

A. To evaluate information security performance

B. To ensure that employees and contractors are competent

C. To monitor the use of information assets

D. To track the use of outsourced processes

ANSWER: A

Explanation:

To evaluate information security performance is correct because ISO/IEC 27001:2022 clause 9.1 requires the organization to determine what needs to be monitored and measured, the methods for doing so, when results are analysed and evaluated, and who performs those activities. The purpose is to obtain reliable evidence about how well the information security management system and its information-security processes are performing. This enables the organization to assess whether intended outcomes are being achieved, identify trends or areas needing attention, and provide meaningful input to management review and continual improvement. Monitoring and measurement therefore support informed decisions about the effectiveness and performance of the ISMS rather than merely collecting operational data. The ISO overview of ISO/IEC 27001 identifies performance evaluation as a core requirement within an ISMS and explains that the standard provides requirements for establishing, implementing, maintaining, and continually improving information security management. See ISO/IEC 27001:2022 on the ISO website and the ISO/IEC 27001 information-security overview.

QUESTION NO: 3

A new regulation introduces security requirements for the organization's processing of customer information. The legal team informs the ISMS manager, but there is no documented assessment of the requirement or record of how it will be addressed.

Which control should be applied first to establish the required governance?

A. Compliance with policies, rules and standards for information security

B. Identification of legal, statutory, regulatory and contractual requirements

C. Information security in supplier relationships

D. Protection of privacy and protection of personally identifiable information

ANSWER: B

Explanation:

Identification of legal, statutory, regulatory and contractual requirements is the appropriate control. Annex A control 5.31 requires legal, statutory, regulatory and contractual requirements relevant to information security, and the organization's approach to meeting them, to be identified, documented and kept up to date.

Compliance with policies, rules and standards for information security is concerned with reviewing adherence to the organization's established internal requirements. Information security in supplier relationships and privacy protection may become relevant depending on the circumstances, but they do not replace the requirement to identify, document and maintain the applicable regulatory requirement and the organization's approach to it.

QUESTION NO: 4

Which attribute is NOT a required focus of continual ISMS improvement?

A. Adequacy

B. Effectiveness

C. Suitability

D. Importance

ANSWER: D

Explanation:

Importance is the attribute that is not specified as a required focus for continual improvement of an information security management system. ISO/IEC 27001:2022, clause 10.2, requires an organization to continually improve the ISMS's suitability, adequacy, and effectiveness. These three qualities ensure that the ISMS remains appropriate to the organization's context and needs, is sufficient in its scope and arrangements, and continues to achieve its intended information-security outcomes. Continual improvement is therefore an ongoing management-system activity supported by performance evaluation, internal audits, management review, treatment of nonconformities, and changes to risks, requirements, or organizational circumstances. The standard does not identify importance as a distinct quality against which continual improvement of the ISMS must be directed. Importance may inform business decisions and risk priorities, but it is not one of the explicit clause 10.2 continual-improvement attributes. The ISO catalogue provides the official publication record for ISO/IEC 27001:2022: ISO/IEC 27001:2022 — ISO. APMG's certification page also identifies ISO/IEC 27001 Foundation as covering the requirements and operation of an ISMS: APMG ISO/IEC 27001 certification.

QUESTION NO: 5

Which International Standard can be used to implement an integrated management system with ISO/IEC 27001?

A. ISO/IEC 27003

B. ISO/IEC 27013

C. ISO 9001

D. None of the above

ANSWER: B

Explanation:

ISO/IEC 27013 is the appropriate standard because it provides guidance for the integrated implementation of an information security management system conforming to ISO/IEC 27001 and a service management system conforming to ISO/IEC 20000-1. It is specifically intended to help organizations establish a coordinated management-system approach where information security and IT service management have related objectives, controls, processes, documented information, internal audits, management reviews, and continual-improvement activities. This integrated approach can reduce unnecessary duplication while ensuring that the distinct requirements of both management-system standards continue to be addressed.

For an ISO/IEC 27001 Foundation context, the key point is that ISO/IEC 27013 is not merely a general implementation guide: its defined purpose is integration between the ISO/IEC 27001 ISMS and the ISO/IEC 20000-1 service management system. Accordingly, it is the International Standard directly applicable to implementing this particular integrated management system. The ISO catalogue describes ISO/IEC 27013 as guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1. See the ISO/IEC 27013:2021 catalogue entry and the ISO/IEC 27001:2022 catalogue entry.

QUESTION NO: 6

Who is required to ensure that staff are supported so that they can contribute to the information security management system?

A. Top management of the organization

B. Management responsible for each area of operation

C. Auditors who audit each area of operation

D. ISO/IEC 27001 practitioners within the organization

ANSWER: A

Explanation:

Top management of the organization is required to support people so that they can contribute to the effectiveness of the information security management system (ISMS). ISO/IEC 27001:2022 clause 5.1 places this responsibility directly within top management's leadership and commitment obligations. This means the organization's highest level of accountable leadership must create the conditions in which personnel can make an effective contribution to information security: for example, by providing direction, appropriate resources, authority, organizational support, and a culture in which ISMS responsibilities are understood and taken seriously. The requirement is not limited to making resources available. It also requires active leadership that enables people across relevant functions to participate in operating, maintaining, and improving the ISMS. "Top management" is defined in the standard as the person or group of people who directs and controls an organization at the highest level, so the exact structure will depend on the organization's governance arrangements. This leadership accountability is fundamental to ensuring that information security objectives and ISMS requirements are embedded in organizational operations. The ISO overview of ISO/IEC 27001 describes the standard's framework for establishing, implementing, maintaining, and continually improving an ISMS: ISO/IEC 27001:2022. Further information on the ISO/IEC 27000 family is available from ISO's information security management page.

QUESTION NO: 7

An internal audit finds that privileged accounts have repeatedly been created without the required approval. The immediate issue is corrected by obtaining approvals for the existing accounts.

Which further action is required when responding to this nonconformity?

A. Replace the access-control policy with a new policy

B. Determine whether similar nonconformities exist or could occur elsewhere

C. Close the finding once the existing accounts have been approved

D. Transfer responsibility for the issue to the certification body

ANSWER: B

Explanation:

The organization must evaluate whether similar nonconformities exist, or could potentially occur, elsewhere. ISO/IEC 27001:2022 clause 10.1 requires the organization to determine the cause of a nonconformity and determine whether similar nonconformities exist or could potentially occur. Correcting the currently identified accounts does not establish whether the same approval failure affects other systems, teams or account types.

Changing the information security policy is not always necessary. The organization must review the effectiveness of corrective action, but it cannot reasonably do so without first addressing the cause and the possibility of similar issues elsewhere.