ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: APMG-International

Code: ISO-IEC-27001-FOUNDATION

Exam: ISO/IEC 27001 (2022) Foundation Exam

https://www.examsnest.com/exam/iso-iec-27001-foundation/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 4.0

Question: 1

Which statement is a factor that will influence the implementation of the information security management system?

A. The ISMS will be separate from the organization's overall management structure

B. The ISMS will encompass all controls specified within ISO/IEC 27001

C. The ISMS will be scaled to the controls according to the needs of the organization

D. The ISMS will be operated as an independent process within the organization

Answer: C

Explanation:

ISO/IEC 27001 makes clear that the ISMS is intended to be tailored to the organization. The standard states: “This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this document are generic and are intended to be applicable to all organizations regardless of type, size or nature.” This means implementation is scaled based on each organization’s risk, context, and needs, not a fixed one-size-fits-all set of activities or controls. Clause 6.1.3 further reinforces that control selection is flexible and risk-driven: “Organizations can design controls as required or identify them from any source,” and “Annex A contains a list of possible information security controls… The information security controls listed in Annex A are not exhaustive and additional information security controls can be included if needed.” Together, these extracts verify that the ISMS implementation is influenced by and scaled to the organization’s needs and selected controls, not separated from management processes (A, D) nor

mandated to include “all controls” (B).

Question: 2

Which factor is required to be determined when understanding the organization and its context?

A. Internal issues affecting the purpose of the ISMS

B. The information security objectives relevant to the ISMS

C. The processes that will be required to operate the ISMS

D. The ISO/IEC 27001 clauses which apply to the management system

Answer: A

Explanation:

Clause 4.1 specifies exactly what must be determined when establishing context: “The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.” This requirement is about understanding internal and external issues (e.g., culture, capabilities, regulatory environment) that influence the ISMS’s effectiveness. Objectives (option B) are addressed later in Clause 6.2; processes (option C) are addressed in Clause 4.4 and operational planning; and “which clauses apply” (option D) is not a determination step—ISO/IEC 27001’s requirements in Clauses 4–10 are not optional. Therefore, the direct, required factor per 4.1 is determining internal (and external) issues relevant to the organization’s purpose and ISMS outcomes.

Question: 3

Which audit activity related to ISO/IEC 27001 may be carried out by a practitioner?

A. Conduct a surveillance audit of their own area of the organization

B. Conduct an internal audit of the organization

C. Conduct an audit of an Accredited Training Organization

D. Conduct an audit of a Certification Body

Answer: B

Explanation:

ISO/IEC 27001 requires internal audits and sets out how they must be conducted: "The organization shall conduct internal audits at planned intervals…" (9.2.1) and "plan, establish, implement and maintain an audit programme(s)… [and] select auditors and conduct audits that ensure objectivity and the impartiality of the audit process" (9.2.2). These extracts confirm that practitioners (internal to the organization) can conduct internal audits provided objectivity and impartiality are ensured (e.g., they do not audit their own work). Surveillance audits (option A) and audits of Accredited Training Organizations or Certification Bodies (options C, D) are third-party activities outside the remit of an internal practitioner under ISO/IEC 27001; the standard's audit requirement is focused on the organization's own internal audit programme. Therefore, conducting an internal audit (B) is the correct practitioner activity per Clause 9.2.

Question: 4

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:

Clause 6.1.2 defines the mandatory elements of risk assessment. Under risk identification, the standard requires: “identifies the information security risks: 1) apply the information security risk assessment process to identify risks…; and 2) identify the risk owners.” By contrast, considering likelihood and determining levels of risk (options B and D) are part of risk analysis (6.1.2 d) “assess the realistic likelihood…”; “determine the levels of risk”), and prioritization for treatment (option C) is part of risk evaluation (6.1.2 e) “prioritize the analysed risks for risk treatment”). Therefore, the specific activity that belongs to risk identification is to identify the risk owners. This sequencing is prescribed to ensure each risk has a designated owner responsible for decisions on treatment and acceptance downstream.

Question: 5

In an audit, what is the definition of an observation?

A. A non-fulfilment of a requirement of ISO/IEC 27001

B. A conformity to the standard where there is an opportunity for improvement

C. An issue excluded from the scope of the standard

D. An issue raised by an interested party

Answer: B

Explanation:

ISO/IEC 27001 mandates internal audits (Clause 9.2) and continual improvement (Clause 10.1) but does not define the specific audit term “observation.” However, the audit framework in 9.2 requires an audit

programme and impartial auditors, and management review inputs include “feedback on the information security performance including trends in… audit results” and “opportunities for continual improvement.” The companion implementation guidance (ISO/IEC 27002) reinforces the concept of opportunities for improvement in the review of policies: “The reviews should include assessing opportunities for improvement and the need for changes to the approach to information security…” In practical ISO audit usage (aligned with ISO 19011 guidance referenced in the Study Guide), an observation is a recorded conformity where improvement is advisable—commonly termed an Opportunity for Improvement (OFI). The Study Guide’s internal audit section emphasizes running an audit programme to identify “potential areas of weakness or non-compliance,” supporting the notion of recording improvement opportunities alongside nonconformities. Therefore, within ISO/IEC 27001 audit practice, the best-fit definition is B: a conformity where there is an opportunity for improvement.

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: APMG-International

Code: ISO-IEC-27001-FOUNDATION

Exam: ISO/IEC 27001 (2022) Foundation Exam

https://www.examsnest.com/exam/iso-iec-27001-foundation/

Use Coupon "**SAVE15**" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation