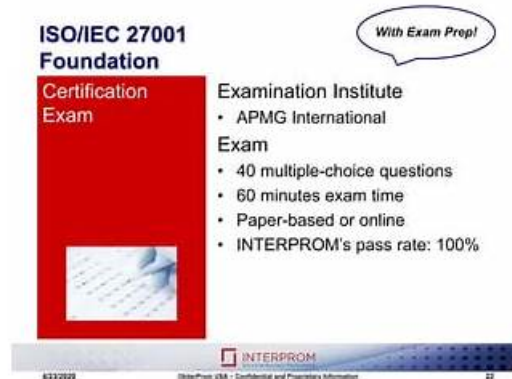


APMG-International - ISO-IEC-27001-Foundation–High-quality Valid Exam Sims



P.S. Free 2026 APMG-International ISO-IEC-27001-Foundation dumps are available on Google Drive shared by Prep4away: <https://drive.google.com/open?id=1-jh9EkCjRC8iGn2VKaGhbPg8RSCHAWV7>

The meaning of qualifying examinations is, in some ways, to prove the candidate's ability to obtain qualifications that show your ability in various fields of expertise. If you choose our ISO-IEC-27001-Foundation learning guide materials, you can create more unlimited value in the limited study time, through qualifying examinations, this is our ISO-IEC-27001-Foundation Real Questions and the common goal of every user, we are trustworthy helpers, so please don't miss such a good opportunity. The acquisition of ISO-IEC-27001-Foundation qualification certificates can better meet the needs of users' career development.

APMG-International ISO-IEC-27001-Foundation Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"> • Cybersecurity: Cybersecurity, also known as IT security or computer security, involves safeguarding computer systems, networks, and data from unauthorized access, theft, damage, or disruption to ensure the integrity and availability of digital information.
Topic 2	<ul style="list-style-type: none"> • Self Confidence: Self-confidence is the belief in one's abilities, competence, and value, reflecting a sense of assurance and inner strength.
Topic 3	<ul style="list-style-type: none"> • Continuous Improvement Process (CI, CIP): A continuous or continual improvement process (CIP or CI) involves ongoing, systematic efforts to enhance products, services, or operational processes to achieve higher efficiency and effectiveness over time.
Topic 4	<ul style="list-style-type: none"> • Information Management (IM): Information management (IM) encompasses the entire lifecycle of information within an organization—from its collection and storage to its distribution, use, and eventual archiving or disposal.
Topic 5	<ul style="list-style-type: none"> • Security Breaches: Security breaches occur when unauthorized access or violations of security protocols are detected or imminent, potentially compromising data or system integrity.
Topic 6	<ul style="list-style-type: none"> • Compliance: Regulatory compliance refers to an organization's commitment to understanding and adhering to applicable laws, policies, and regulations to operate within established legal and ethical standards.
Topic 7	<ul style="list-style-type: none"> • Framework Design: Framework design is the process of developing a reusable structural foundation that supports and guides the creation and organization of software systems.

ISO-IEC-27001-Foundation Latest Test Braindumps - Latest ISO-IEC-27001-Foundation Exam Preparation

Through all these years' experience, our ISO-IEC-27001-Foundation training materials are becoming more and more perfect. Moreover, we hold considerate after-sales services and sense-and-respond tenet all these years. So if you get any questions of our ISO-IEC-27001-Foundation learning guide, please get us informed. It means we will deal with your doubts with our ISO-IEC-27001-Foundation practice materials 24/7 with efficiency and patience.

APMG-International ISO/IEC 27001 (2022) Foundation Exam Sample Questions (Q20-Q25):

NEW QUESTION # 20

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

- A. Management responsible for each area of operation
- **B. Top management of the organization**
- C. Auditors who audit each area of operation
- D. ISO/IEC 27001 practitioners within the organization

Answer: B

Explanation:

Clause 5.1 (Leadership and Commitment) requires that:

"Top management shall demonstrate leadership and commitment with respect to the information security management system by... ensuring that the resources needed for the ISMS are available... and supporting persons to contribute to the effectiveness of the ISMS." This makes it explicit that top management has the responsibility to ensure personnel are supported so they can contribute to the ISMS. Option B (line management) may provide local support, but ultimate accountability rests with top management. Auditors (C) only evaluate compliance, not provide support.

Practitioners (D) help implement, but they don't bear formal responsibility under the standard.

Thus, the verified answer is A: Top management of the organization.

NEW QUESTION # 21

Which statement about the conduct of audits is true?

- A. During Stage 1 of a certification audit, evidence is collected by observing activities
- B. The certificate issued after a successful re-certification audit in typical schemes lasts for one year
- C. Third party audits are conducted by a customer of the organization
- **D. One of the focus areas for a surveillance audit is the output from internal audits and management reviews**

Answer: D

Explanation:

Clause 9.2 (Internal Audit) and Clause 9.3 (Management Review) highlight that audit outputs and management reviews are key inputs for evaluating ISMS performance. Surveillance audits, conducted by Certification Bodies, check ongoing compliance and effectiveness. ISO certification schemes (per ISO/IEC

17021) require surveillance audits to verify whether corrective actions and continuous improvements are being made. A critical focus area is the results of internal audits and management reviews, ensuring that the organization maintains its ISMS between certification cycles.

Option A is incorrect - third-party audits are performed by independent Certification Bodies, not customers.

Option B is incorrect - certificates are typically valid for three years with annual surveillance. Option D is incorrect - Stage 1 is primarily a documentation and readiness review, not evidence observation.

Therefore, the verified correct answer is C.

NEW QUESTION # 22

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

- **A. Determine the risk owners**
- B. Determine the level of risk
- C. Consider the likelihood of the occurrence
- D. Prioritize the risk for treatment

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...; and2) 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.

NEW QUESTION # 23

Identify the missing word(s) in the following sentence.

"Information security, cybersecurity and privacy protection - [?]" is the title of ISO/IEC 27005.

- A. Information security controls
- B. Guidelines for information security management systems auditing
- C. Information security management systems - Requirements
- **D. Guidance on managing information security risks**

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract ISO/IEC 27005 standards:

ISO/IEC 27005:2022 is titled:

"Information security, cybersecurity and privacy protection - Guidance on managing information security risks." This standard provides structured methodologies for identifying, analyzing, evaluating, and treating risks, in alignment with ISO/IEC 27001's risk management requirements (Clause 6.1.2 and 6.1.3). It supports organizations in implementing the risk management process that underpins an ISMS. Options A and B are titles of other ISO standards (ISO/IEC 27007 for auditing, ISO/IEC 27001 for requirements). Option D refers to ISO/IEC 27002 (controls).

Thus, the correct answer is C: Guidance on managing information security risks.

NEW QUESTION # 24

What is the definition of the term 'integrity' according to ISO/IEC 27000?

- A. The property of availability and confidentiality
- B. The property that information is NOT made available inappropriately
- C. The property of being accessible and usable
- **D. The property of accuracy and completeness**

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract ISO/IEC 27000 standards:

According to ISO/IEC 27000:2018, Clause 3.35:

"Integrity is the property of accuracy and completeness."

This is one of the three core principles of information security (CIA triad):

- * Confidentiality: ensuring information is not made available to unauthorized persons (related to option B).
- * Integrity: ensuring data is accurate, complete, and unaltered except by authorized means.
- * Availability: ensuring information is accessible and usable when required (related to option A).

