PECB

ISO-IEC-27002-Foundation

ISO/IEC 27002 Foundation Exam

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.

Latest Version: 6.0

Question: 1

What does ISO/IEC 27002 provide?

A. Guidance for the implementation of information security controls
B. Requirements for the implementation of information security controls
C. Guidance for the management of information security risks

Answer: A

Explanation:
ISO/IEC 27002:2022 provides guidance for selecting, implementing, and managing information security controls. It is not the certification requirements standard; that role belongs to ISO/IEC 27001. ISO/IEC 27002 supports organizations by explaining the purpose of each control, the implementation guidance, and other related information needed to apply controls appropriately. Its controls are grouped into organizational, people, physical, and technological themes. The standard is intended to be used as a reference when organizations design security measures based on their risks, business needs, legal obligations, contractual requirements, and information security objectives. Therefore, option A is correct because “guidance” is the core function of ISO/IEC 27002. Option B is incorrect because ISO/IEC 27002 does not set mandatory requirements for certification. Option C is related to risk management, but it is not the main purpose of ISO/IEC 27002; risk management guidance is more directly associated with ISO/IEC 27005. ISO/IEC 27002 guides control implementation after risk and control needs are determined. Reference/Chapters: ISO/IEC 27002:2022, Clause 1 Scope; Clause 4 Structure of the standard; Controls 5–8.

Question: 2

Which of the following is an example of an organizational asset in cyberspace?

A. Medical data
B. Digital customer identity
C. Intellectual property

Answer: B

Explanation:
A digital customer identity is the best example of an organizational asset in cyberspace because it exists, functions, and is protected within digital systems, networks, applications, and online

services. ISO/IEC 27002 treats identities, authentication information, access rights, and digital accounts as critical security subjects because compromise of identity can enable unauthorized access, fraud, impersonation, privacy breaches, and loss of accountability. A digital customer identity can include usernames, identifiers, credentials, account attributes, authentication factors, access permissions, profile data, and linked personal information. Medical data and intellectual property are also important information assets, but the phrase “asset in cyberspace” points most directly to a digitally represented identity used for electronic interaction. ISO/IEC 27002 contains several controls that protect this asset type, including identity management, authentication information, access rights, secure authentication, and access restriction. These controls ensure that identities are created, maintained, verified, modified, disabled, and removed in a controlled manner. The exam logic therefore favors option B because cyberspace emphasizes digital identity and online representation. Reference/Chapters: ISO/IEC 27002:2022, Control 5.16 Identity management; Control 5.17 Authentication information; Control 5.18 Access rights; Control 8.5 Secure authentication.

Question: 3

Which statement below describes the principle of confidentiality?

A. Property that information is not made available or disclosed to unauthorized individuals, entities, or processes
B. Property of accuracy and completeness
C. Property of being accessible and usable upon demand by an authorized entity

Answer: A

Explanation:
Confidentiality means that information is protected from unauthorized disclosure or availability. The correct statement is option A because it expresses the essential confidentiality concept: information must not be made available or disclosed to unauthorized individuals, entities, or processes. ISO/IEC 27002 supports confidentiality through controls such as information classification, labelling, access control, identity management, authentication, cryptography, data masking, information transfer rules, and data leakage prevention. The purpose is to ensure that only approved users, systems, or processes can view or receive information according to business need and authorization. Option B describes integrity, because accuracy and completeness relate to whether information remains correct and unaltered. Option C describes availability, because accessibility and usability on demand relate to authorized access when needed. In ISO/IEC 27002, many controls are mapped to confidentiality, integrity, and availability through control attributes. A confidentiality breach can occur through excessive internal access, accidental disclosure, lost media, weak access permissions, exposed credentials, or insecure transfer. Reference/Chapters: ISO/IEC 27002:2022, Clause 4 control attributes; Control 5.12 Classification of information; Control 5.15 Access control; Control 8.24 Use of cryptography.

Question: 4

Some employees of an organization find the data processing procedures complicated and have been struggling to follow them effectively. Which of the following threats is the organization facing in this case?

A. Data input error by employees
B. Hacking
C. Information theft

Answer: A

Explanation:
The situation describes a people-related operational threat: data input error by employees. The root cause is not a malicious external attack or theft; it is that employees cannot reliably follow complicated processing procedures. ISO/IEC 27002 recognizes that people, competence, awareness, and documented procedures are essential to information security. When procedures are unclear, excessive, or difficult to follow, employees may enter incorrect data, omit fields, select wrong categories, mishandle classifications, misroute information, or unintentionally corrupt records. This primarily threatens integrity because the information may no longer be accurate or complete. Hacking would involve unauthorized technical intrusion, and information theft would involve intentional unauthorized taking or disclosure of information. Neither is stated in the scenario. ISO/IEC 27002 addresses this type of risk through information security awareness, education and training, documented operating procedures, clear responsibilities, and appropriate segregation of duties. Effective controls should make correct behavior practical and repeatable, not merely documented. Therefore, the verified answer is option A.
Reference/Chapters: ISO/IEC 27002:2022, Control 6.3 Information security awareness, education and training; Control 5.37 Documented operating procedures; Control 5.3 Segregation of duties.

Question: 5

An organization has set up a fire alarm. What type of control is this?

A. Corrective and managerial
B. Detective and technical
C. Preventive and legal

Answer: B

Explanation:
A fire alarm is a detective and technical control. It is detective because it identifies or signals that a fire-related event may be occurring. The alarm does not normally stop the fire from

starting, and it does not restore damaged assets after the event. Its purpose is to detect indicators such as smoke, heat, or fire and trigger response actions such as evacuation, suppression, emergency communication, or incident handling. It is technical because it operates through engineered or electronic mechanisms rather than through management approval, legal clauses, or purely administrative processes. ISO/IEC 27002:2022 classifies controls using attributes, including control type. Control types include preventive, detective, and corrective. Fire alarms align with the physical security control area because fire is a physical and environmental threat to information processing facilities, equipment, storage media, and supporting infrastructure. The value of the control is timely detection, reducing the chance that a physical event escalates unnoticed into major damage or service disruption.
Reference/Chapters: ISO/IEC 27002:2022, Clause 4 control attributes; Control 7.4 Physical security monitoring; Control 7.5 Protecting against physical and environmental threats.

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/