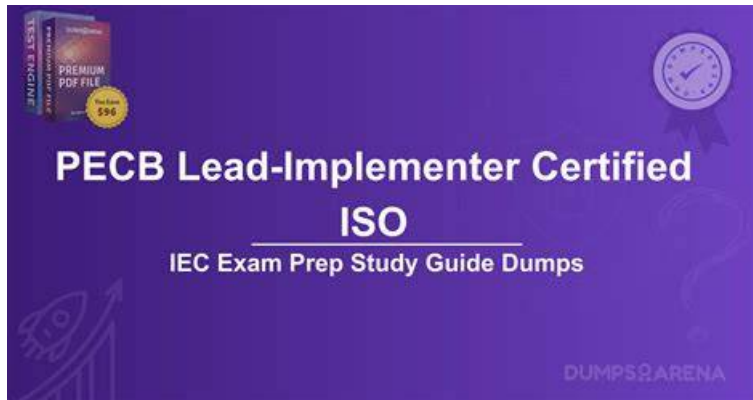


# Actual PECB ISO-IEC-27002-Foundation Dumps - Quick Test Preparation Tips



Our company concentrates on relieving your pressure of preparing the ISO-IEC-27002-Foundation exam. Getting the certificate equals to embrace a promising future and good career development. Perhaps you have heard about our ISO-IEC-27002-Foundation exam question from your friends or news. Why not has a brave attempt? You will certainly benefit from your wise choice. Now our ISO-IEC-27002-Foundation practice materials have won customers' strong support. Our sales volume is increasing every year. The great achievements benefit from our enormous input. First of all, we have done good job on researching the new version of the ISO-IEC-27002-Foundation exam question.

## PECB ISO-IEC-27002-Foundation Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"> <li>• Explain the fundamental concepts of information security, cybersecurity, and privacy based on ISO</li> <li>• IEC 27002: This domain covers the core principles and definitions that underpin information security, including the concepts of confidentiality, integrity, and availability. It focuses on how ISO</li> <li>• IEC 27002 frames cybersecurity and privacy as foundational elements of an organization's overall security posture.</li> </ul>
Topic 2	<ul style="list-style-type: none"> <li>• Discuss the relationship between ISO</li> <li>• IEC 27001, ISO</li> <li>• IEC 27002, and other standards and regulatory frameworks: This domain examines how ISO</li> <li>• IEC 27002 functions as a code of practice that supports the requirements set out in ISO</li> <li>• IEC 27001, and how both standards interact with other relevant frameworks. It also addresses how organizations align these standards with applicable laws, regulations, and industry-specific requirements.</li> </ul>
Topic 3	<ul style="list-style-type: none"> <li>• Interpret the ISO</li> <li>• IEC 27002 organizational, people, physical, and technological controls in the specific context of an organization: This domain covers the four control categories defined in ISO</li> <li>• IEC 27002 organizational, people, physical, and technological and how each applies to real-world organizational environments. It requires understanding how to read, interpret, and contextualize these controls based on an organization's specific needs, risks, and operating conditions.</li> </ul>

>> New ISO-IEC-27002-Foundation Test Cost <<

## Practical PECB ISO-IEC-27002-Foundation: New ISO/IEC 27002 Foundation Exam Test Cost - Top Lead1Pass Exam ISO-IEC-27002-Foundation Preparation

We believe that every customer pays most attention to quality when he is shopping. Only high-quality goods can meet the needs of every customer better. And our ISO-IEC-27002-Foundation training quiz has such high quality, because its hit rate of test questions

is extremely high. Perhaps you will find in the examination that a lot of questions you have seen many times in our ISO-IEC-27002-Foundation Real Exam. And you will find our ISO-IEC-27002-Foundation practice questions are so popular that a lot of our candidates have bought them.

## PECB ISO/IEC 27002 Foundation Exam Sample Questions (Q35-Q40):

### NEW QUESTION # 35

Which control should an organization implement to ensure that the software is written securely and the number of potential vulnerabilities in the software is reduced?

- A. Control 8.28 Secure coding
- B. Control 8.26 Application security requirements
- C. Control 8.29 Security testing in development and acceptance

**Answer: A**

Explanation:

Control 8.28, Secure coding, is the correct control because the question focuses on software being written securely and reducing potential vulnerabilities in the code. Secure coding addresses the practices, rules, and techniques developers should use to avoid common software weaknesses. This can include input validation, output encoding, error handling, authentication handling, secure session management, memory safety, protection against injection, secure API use, cryptographic correctness, dependency management, and code review. Control 8.29, Security testing in development and acceptance, verifies whether security requirements and controls are effective, but testing occurs after or during development and does not itself define how code should be written. Control 8.26, Application security requirements, defines security requirements for applications, but secure coding is the specific implementation practice that reduces vulnerabilities during software construction. ISO/IEC 27002 treats secure development as a lifecycle discipline: requirements define what is needed, secure coding implements it safely, and testing validates it. The direct match to the exam wording is Control 8.28. References/Chapters: ISO/IEC 27002:2022, Control 8.28 Secure coding; Control 8.26 Application security requirements; Control 8.29 Security testing in development and acceptance.

### NEW QUESTION # 36

What should the management of the organization do to ensure that all personnel are aware of and fulfill their information security responsibilities?

- A. Require all personnel to establish and approve information security policies, topic-specific policies and procedures of the organization
- B. Require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization
- C. Require all personnel to read the guidelines of ISO/IEC 27002

**Answer: B**

Explanation:

Management should require all personnel to apply information security according to the organization's established information security policy, topic-specific policies, and procedures. ISO/IEC 27002 makes management responsibilities clear: leadership must ensure personnel understand and fulfill their security duties. Personnel are expected to follow approved policies and procedures, protect information assets, report security events, and comply with assigned responsibilities. Option B is incorrect because establishing and approving policies is a management responsibility, not a duty assigned to all personnel. Option C is incorrect because reading ISO/IEC 27002 guidelines is not a substitute for following the organization's own approved policies and procedures. ISO/IEC 27002 provides guidance to organizations, but employees need practical internal rules that apply to their roles, systems, data, and processes. Management commitment is demonstrated by assigning responsibilities, communicating expectations, providing awareness and training, and enforcing compliance. The core principle is that information security must be operationalized through everyday behavior, not left as abstract documentation. Therefore, option A is the verified answer. References/Chapters: ISO/IEC 27002:2022, Control 5.4 Management responsibilities; Control 5.1 Policies for information security; Control 6.3 Information security awareness, education and training.

### NEW QUESTION # 37

An organization does NOT authenticate the identity of persons that enter the server room, so unauthorized persons can easily gain access to the server. Which control of ISO/IEC 27002 should the organization implement to solve this problem?

- A. Control 8.4 Access to source code
- B. Control 8.6 Capacity management
- **C. Control 7.2 Physical entry**

**Answer: C**

Explanation:

Control 7.2, Physical entry, is the correct control because the problem is unauthorized physical access to a server room. ISO/IEC 27002 expects secure areas to be protected by appropriate entry controls so that only authorized persons can enter. Authentication of identity at entry points may include badges, access cards, biometric verification, PINs, visitor registration, security guards, turnstiles, logs, escorts, or electronic access systems. The server room contains information processing facilities, and unauthorized physical access could lead to theft, tampering, cable disconnection, hardware compromise, installation of rogue devices, or direct access to consoles and storage media. Control 8.6, Capacity management, concerns resource capacity for information processing facilities, not physical access. Control 8.4, Access to source code, concerns protecting program source code from unauthorized access, not entry into a secure physical room. Because the scenario specifically says people can enter the server room without identity authentication, the matching ISO/IEC

27002 physical control is Control 7.2. References/Chapters: ISO/IEC 27002:2022, Control 7.2 Physical entry; Control 7.1 Physical security perimeter; Control 7.4 Physical security monitoring.

### NEW QUESTION # 38

In which group of controls does Control 5.7 Threat intelligence belong?

- A. Technological
- B. People
- **C. Organizational**

**Answer: C**

Explanation:

Control 5.7, Threat intelligence, belongs to the organizational control group. ISO/IEC 27002:2022 organizes controls by clauses: Clause 5 contains organizational controls, Clause 6 contains people controls, Clause 7 contains physical controls, and Clause 8 contains technological controls. Threat intelligence is classified as organizational because it supports governance, decision-making, risk awareness, planning, prioritization, and security strategy across the organization. It involves collecting, analyzing, and using information about existing or emerging threats so the organization can reduce risk and improve controls. Threat intelligence can influence vulnerability management, incident response, monitoring, supplier risk management, awareness training, security architecture, and risk treatment plans. Although threat intelligence may use technological tools, its ISO/IEC 27002 placement is organizational because its primary purpose is to guide security decisions and readiness. Option A is incorrect because technological controls are Clause 8. Option B is incorrect because people controls are Clause 6. The verified answer is option C.

References/Chapters: ISO

/IEC 27002:2022, Clause 5 Organizational controls; Control 5.7 Threat intelligence; Clause 4 Structure of the standard.

### NEW QUESTION # 39

Which of the following controls aims to ensure the integrity of operational systems and prevent exploitation of technical vulnerabilities?

- A. Control 8.17 Clock synchronization
- B. Control 8.15 Logging
- **C. Control 8.19 Installation of software on operational systems**

**Answer: C**

### NEW QUESTION # 40

.....

After you pay for our ISO-IEC-27002-Foundation exam material online, you will get the link to download it in only 5 to 10 minutes. You don't have to wait a long time to start your preparation for the ISO-IEC-27002-Foundation exam. The only thing you must make sure is that you have left your right E-mail address when you purchase our ISO-IEC-27002-Foundation Study Guide. Moreover, you don't need to worry about safety in buying our ISO-IEC-27002-Foundation exam materials. We have considered all

