PECB

When Recognition Matters

EXAM PREPARATION GUIDE

PECB Certified ISO/IEC 27002 Manager

The objective of the "PECB Certified ISO/IEC 27002 Manager" examination is to ensure that the candidate has acquired the necessary knowledge and skills to support an organization in managing the information security controls based on ISO/IEC 27002 standard.

The ISO/IEC 27002 Manager exam is intended for:

- Managers or consultants seeking to be experts in the implementation of an Information Security Management System (ISMS)
- Individuals responsible for an organization's information security
- Members of an information security team
- Expert advisors in information technology
- Technical experts seeking to prepare for an information security audit function

The exam covers the following competency domains:

Domain 1: Fundamental principles and concepts of Information Security
Domain 2: Information Security Controls based on ISO/IEC 27002

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts of Information Security

Main objective: Ensure that the ISO/IEC 27002 Manager candidate understands, and is able to interpret and illustrate the main information security principles and concepts based on ISO/IEC 27001, ISO/IEC 27002 and other best practices.

Competencies	Knowledge statements
1. Ability to understand and explain the organization's operations and the development of information security standards. 2. Ability to understand the differences between various information security standards. 3. Ability to explain and illustrate the main concepts in information security and information security risk management. 4. Ability to distinguish and explain the difference between information asset, data and record. 5. Ability to understand, interpret and illustrate the relationship between the concepts of asset, vulnerability, threat, impact and controls.	1. Knowledge of the main standards and other best practices related to information security. 2. Knowledge of the main information security concepts and terminology as described in ISO/IEC 27000. 3. Knowledge of the concept of risk and its application in information security. 4. Knowledge of the relationship between the concepts of asset, vulnerability, threat, impact and controls. 5. Knowledge of the difference and characteristics of security objectives and controls. 6. Knowledge of the difference between preventive, detective and corrective controls and their characteristics.

Domain 2: Information Security Controls based on ISO/IEC 27002

Main objective: Ensure that the ISO/IEC 27002 Manager candidate understands, and is able to interpret and provide guidance on how to implement and manage the information security controls best practices based on ISO/IEC 27002.

Competencies	Knowledge statements
1. Ability to identify, understand, classify and explain the clauses, security categories and controls of ISO/IEC 27002. 2. Ability to illustrate the information security controls best practices by concrete examples. 3. Ability to compare possible solutions to a real information security issue of an organization and identify/analyze the strength and weakness of each solution. 4. Ability to select and demonstrate the best information security controls in order to address information security control objectives stated by the organization. 5. Ability to create and justify a detailed action plan to manage the implementation of an information security control by listing the related activities. 6. Ability to analyze, evaluate and validate action plans to implement a specific control.	1. Knowledge of the best practices of information security policy controls. 2. Knowledge of human resources security controls best practices. 3. Knowledge of asset management controls best practices. 4. Knowledge of access control controls best practices. 5. Knowledge of cryptography controls best practices. 6. Knowledge of physical and environmental security physical controls best practices. 7. Knowledge of operations security controls best practices. 8. Knowledge of communications security controls best practices. 9. Knowledge of information systems acquisition, development and maintenance controls best practices. 10. Knowledge of supplier management controls best practices. 11. Knowledge of information security incident management controls best practices. 12. Knowledge of business continuity management controls best practices. 13. Knowledge of compliance controls best practices.

Based on these 2 domains and their relevance, 7 questions are included in the exam, as summarized in the following table:

			Level of Understanding (Cognitive/Taxonomy) Required					
		Points per question	Questions that measure comprehension, application and analysis	Questions that measure synthesis and evaluation	Number of questions per competency domain	% of test devoted to each competency domain	Number of points per competency domain	% of points per competency domain
Competency/Domains	Fundamental principles and concepts of Information Security	7	X		1	14.28	7	14
	Information Security Controls based on ISO/IEC 27002	10		X	6	85.71	43	86
		7		X				
		7		X				
		5	X					
		7		X				
		7	X					
	Total points	50	3	4				
	Number of questions per level of understanding							
	% of Test devoted to each level of understanding (cognitive/taxonomy)		42.86	57.14				

The passing score is **70%.**

After successfully passing the exam, candidates will be able to apply for the "PECB Certified ISO/IEC 27002 Manager" credential, depending on their level of experience.

TAKE A CERTIFICATION EXAM

Candidates will be required to arrive at least thirty (30) minutes before the start of the certification exam. Candidates arriving late will not be given additional time to compensate for the late arrival and may be denied entry to the exam.

All candidates are required to present a valid identity card such as a national ID card, driver's license, or passport to the invigilator.

The exam duration is two (2) hours. Non-native speakers recive an additional twenty (20) minutes.

The exam contains essay type questions: This type of format was selected as a means of determining whether an examinee can clearly answer training-related questions, by assessing problem solving techniques, and formulating arguments supported with reasoning and evidence. The exam is set to be "open book", and does not measure the recall of data or information. The examination evaluates the candidate's comprehension, application and analyzing skills. Therefore, candidates will have to justify their answers by providing concrete explanations as to demonstrate that they have been capable of understanding the training concepts. At the end of this document, you will find samples of exam questions and potential answers.

As the exam is "open book", candidates are allowed to use the following reference materials:

- A copy of the ISO/IEC 27002:2013 standard,
- Course notes from the Participant Handout,
- Any personal notes made by the candidate during the course and
- A hard copy dictionary.

The use of electronic devices, such as laptops, cell phones, etc., is not allowed.

Any attempts to copy, collude or otherwise cheat during the exam will automatically lead to the failure of the exam.

PECB exams are available in English. For availability of the exam in a language other than English, please contact examination@pecb.com.

RECEIVE YOUR EXAM RESULTS

Results will be communicated by email within a period of 6 to 8 weeks from the examination date. The candidate will be provided with only two possible examination results: pass or fail, rather than an exact grade.

Candidates who successfully complete the examination will be able to apply for a certified scheme.

In case of exam failure, the results will be accompanied with the list of domains in which the candidate failed to fully answer the question(s). This can help the candidate better prepare for a retake exam.

Candidates who disagree with the exam results may file a complaint by writing to examination@pecb.com. For more information, please refer to www.pecb.com.

EXAM RETAKE POLICY

There is no limit on the number of times a candidate may retake an exam. However, there are some limitations in terms of the allowed time frame in between exam retakes, such as:

- If a candidate does not pass the exam on the first attempt, he/she must wait 15 days for the next attempt (1st retake). Retake fee applies.

Note: *Candidates, who have completed the full training but failed the written exam, are eligible to retake the exam once for free within a 12 month period from the initial date of the exam*.

- If a candidate does not pass the exam on the second attempt, he/she must wait 3 months (from the initial date of the exam) for the next attempt (2nd retake). Retake fee applies.

- If a candidate does not pass the exam on the third attempt, he/she must wait 6 months (from the initial date of the exam) for the next attempt (3rd retake). Retake fee applies.

After the fourth attempt, a waiting period of 12 months from the last session date is required, in order for the candidate to retake the same exam. Regular fee applies.

For the candidates that fail the exam in the 2nd retake, PECB recommends to attend an official training in order to be better prepared for the exam.

To arrange exam retakes (date, time, place, costs), the candidate needs to contact the PECB partner who has initially organized the session.

CLOSING A CASE

If an applicant does not apply for his/her certificate within three years, their case will be closed. Even though an applicant's certification period expires, they have the right to reopen their case. However, PECB will no longer be responsible for any changes regarding the conditions, standards, policies, candidate handbook or exam preparation guide that were applicable before the applicant's case was closed. Applicants requesting their case to reopen must do so in writing, and pay the required fees.

EXAMINATION SECURITY

A significant component of a successful and respected professional certification credential is maintaining the security and confidentiality of the examination. PECB relies upon the ethical behavior of certificate holders and applicants to maintain the security and confidentiality of PECB examinations. When someone who holds PECB credentials reveals information about PECB examination content, he/she violates the PECB Code of Ethics. PECB will take action against individuals who violate PECB Policies and the Code of Ethics. Actions taken may include permanently barring individuals from pursuing PECB credentials and revoking certifications from those who have been awarded the credential. PECB will also pursue legal

action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

SAMPLE EXAM QUESTIONS AND POSSIBLE ANSWERS

Question 1 – Classification of controls:
For each of the following 5 controls, indicate if it used as a preventive, corrective, and/or detective control; and indicate if the control is an administrative, technical, managerial or legal measure. Explain your answer. A control can have more than one characteristic.

- Recruiting a security guard
- Installation of a firewall on a network

Possible answer:
Recruiting a security guard
- Preventive control: it will prevent unauthorized access to the building
- Managerial measure: recruiting an employee is a managerial measure

Installation of a firewall on a network
- Preventive/detective control: protects the network from unauthorized access; detects suspicious network activity
- Technical measure: it is a technical installation and/or configuration

Question 2 – Security controls:
For each of the following clauses of the ISO/IEC 27002 standard, please provide an action plan with at least two concrete actions that would be acceptable to ensure conformity to the clause and satisfy the control objectives.

Clause 11.1.3 Securing offices, rooms and facilities
Clause 13.2.3 Electronic messaging

Possible answer:
Clause 11.1.3 Securing offices, rooms and facilities
- *Installation of an access control system*
- *Installation of an alarm system*

Clause 13.2.3 Electronic messaging
- *Use of encryption*
- *Use of authentication*
- *Use of electronic signature*