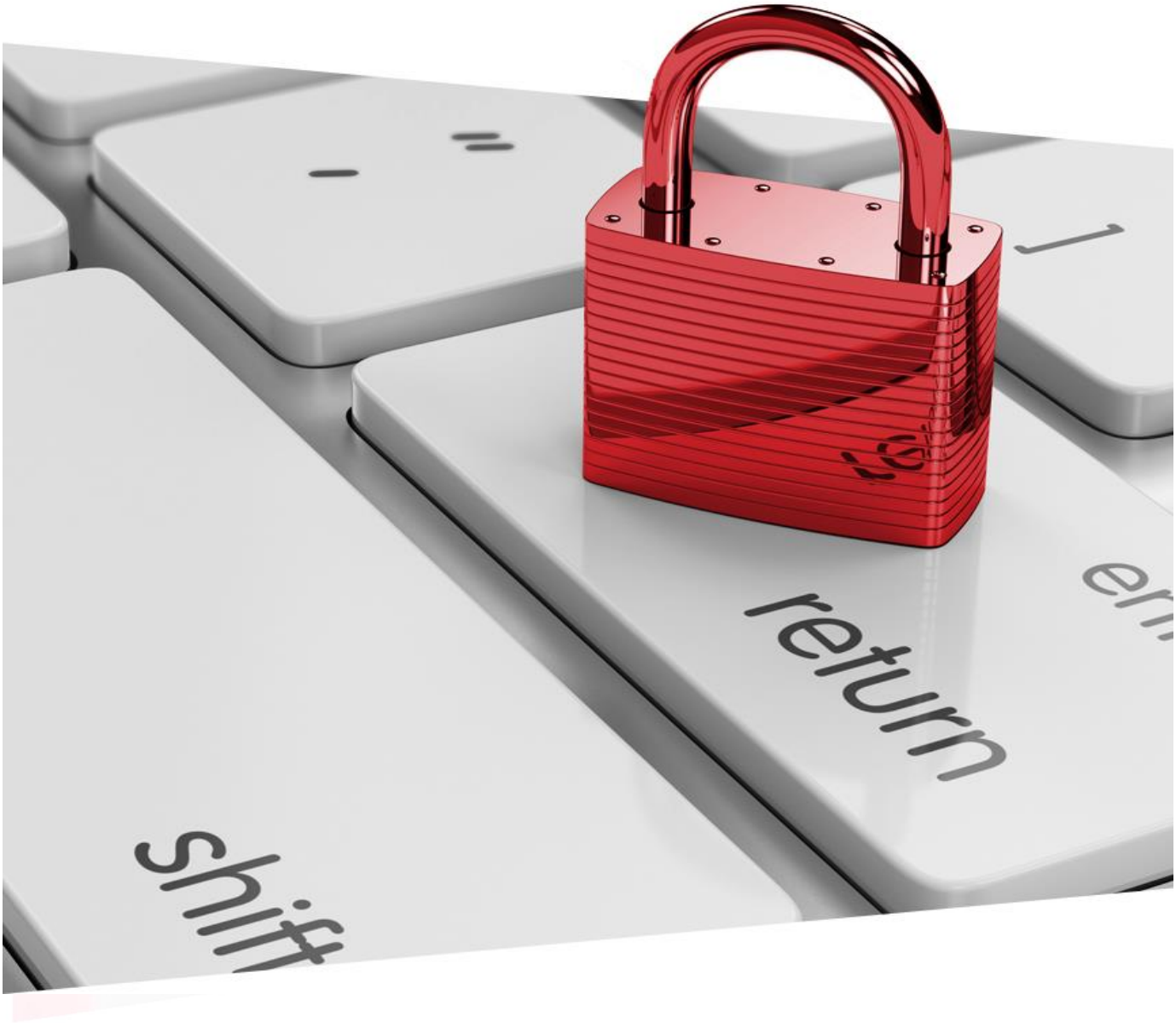
PECB

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 the knowledge for implementing information security controls and the skills to support an organization in managing information security controls according to ISO/IEC 27002:2013.

The target population for this examination is:

- Managers or consultants wanting to implement an Information Security Management System (ISMS)
- Project managers or consultants wanting to master the Information Security Management System implementation process
- Persons responsible for the information security or conformity in an organization
- Members of the information security team
- Expert advisors in information technology
- Technical experts wanting to prepare for an information security audit function

The exam content covers the following domains:

1. Fundamental Principles and Concepts in Information Security
2. Information Security Control Best Practice based on ISO/IEC 27002

The content of the exam is divided as follows:

Domain 1: Fundamental Principles and Concepts in Information Security

Main objective: To ensure that the ISO/IEC 27002 Lead Manager candidate can understand, interpret and illustrate the main information security concepts and standard requirements.

Competencies	Knowledge statements
1. Understand and explain the operations of the ISO organization and the development of information security standards. 2. Ability to identify, analyze and evaluate the information security compliance requirements for an organization. 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. Understand, interpret and illustrate the relationship between the concepts of asset, vulnerability, threat, impact and controls.	1. Knowledge of the main standards in information security 2. Knowledge of the different sources of information security requirement for an organization: laws, regulations, international and industry standards, contracts, market practices, internal policies 3. Knowledge of the main information security concepts and terminology as described in ISO/IEC 27000 4. Knowledge of the concept of risk and its application in information security 5. Knowledge of the relationship between the concepts of asset, vulnerability, threat, impact and controls 6. Knowledge of the difference and characteristics of security objectives and controls 7. Knowledge of the difference between preventive, detective and corrective controls and their characteristics

Domain 2: Information Security Control Best Practices based on ISO/IEC 27002

Main objective: To ensure that the ISO/IEC 27002 Lead Manager candidate can understand, interpret and provide guidance on how to implement and manage 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 detail and illustrate the security controls best practices by concrete examples 3. Ability to compare possible solutions to a real security issue of an organization and identify/analyze the strength and weakness of each solution 4. Ability to select and demonstrate the best 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 implement a security control by listing the activities related 6. Ability to analyze, evaluate and validate action plans to implement a specific control.	1. Knowledge of Information Security Policy Controls Best Practices 2. Knowledge of Organizing Information Security Controls Best Practices 3. Knowledge of Human Resources Security Controls Best Practices 4. Knowledge of Asset Management Controls Best Practices 5. Knowledge of Access Control Controls Best Practices 6. Knowledge of Cryptography Controls Best Practices 7. Knowledge of Physical and Environmental Security Physical Controls Best Practices 8. Knowledge of Operations Security Controls Best Practices 9. Knowledge of Communications Security Controls Best Practices 10. Knowledge of Information Systems Acquisition, Development and Maintenance Controls Best Practices 11. Knowledge of Supplier Management Controls Best Practices 12. Knowledge of Information Security Incident Management Controls Best Practices 13. Knowledge of Business Continuity Management Controls Best Practices 14. Knowledge of Compliance Controls Best Practices

Based on these 2 domains and their relevance, 50 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 competency domain
Competency Domains	Fundamental principles and concepts in information security	1	x		21	42	21	42
		1		x				
		1	x					
		1	x					
		1	x					
		1	x					
		1	x					
		1	x					
		1	x					
		1	x					
		1		x				
		1	x					
		1	x					
		1	x					
		1	x					
		1	x					
		1	x					
		1	x					
		1	x					
		1	x					
		1	x					
	Information Security Control Best Practices based on ISO 27002	1		x	29	58	29	58
		1		x				
		1		x				
		1		x				
		1		x				
		1	x					
		1	x					
		1		x				
		1		x				
		1		x				
		1		x				
		1		x				
		1		x				
		1		x				
		1		x				
		1		x				
		1		x				
		1		x				
		1		x				
		1		x				
		1		x				
		1		x				
		1		x				
		1	x					
		1		x				
		1	x					
		1	x					
		1		x				
		1		x				
Total points		50						
Number of Questions per level of understanding			24	26				
% of Test Devoted to each level of understanding (cognitive/taxonomy)			48.00	52.00				

The passing score is established at **70%.**

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

TAKE A CERTIFICATION EXAM

Candidates will be required to arrive at least thirty (30) minutes before the beginning 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 room (if they arrive more than 5 minutes after the beginning of the exam scheduled time).

All candidates will need to present a valid identity card with a picture such as a driver's license or a government ID to the invigilator.

The exam duration is two (2) hours.

The questions are multiple-choice type questions. This type of format was chosen because it measures different levels of studying, and has resulted to be an effective assessment tool. The multiple-choice exam can be used to evaluate a candidate comprehension on many subjects, including both simple and complicated concepts. First and foremost, multiple-choice exam will not commonly demonstrate if the candidate's response is right or wrong, additionally it will provide continuance of the learning process. Because of this particularity, the exam is not "open book" and does not measure the recall of data or information. The examination helps candidates to comprehend, resolve problems, perform judgment and prove knowledge of facts by way of explaining and analyzing the information. At the end of this document, you will find sample exam questions and their answers.

The exam is "closed book". The use of electronic devices, such as laptops, cell phones, etc., is not allowed. Candidates are only authorised to use a hard copy dictionary.

All attempt to copy, collude or otherwise cheat during the exam will automatically lead to the exam's failure.

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 in a period of 2 to 4 weeks, after taking the exam. The results will not include the exact grade of the candidate, only a mention of pass or fail.

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

In the case of a failure, the results will be accompanied with the list of domains in which the candidate had a low grade, to provide guidance for exams' retake preparation.

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

EXAM RETAKE POLICY

There is no limitation on how many times a candidate can retake the same exam. However, there are some limitations in terms of allowed time-frame in between exams.

When candidates fail the examination, they are only allowed to retake the examination once within 12 months after the first attempt. If second examination is unsuccessful, candidates will be allowed to retake the exam only after 1 year (12 months). Retake fee applies.

Only candidates, who have completed a full PECB training but fail the written exam, are eligible to retake the exam for free, under one condition:

"A candidate can only retake the exam once and this retake must occur within 12 months from the initial exam's date."

When candidates fail the same examination for the second time, their file is automatically closed for 1 year.

CLOSING FILES

Closing a file is equivalent to rejecting a candidate's application. As a result, when candidates request that their file be reopened, PECB will no longer be bound by the conditions, standards, policies, candidate handbook or exam preparation guide that were in effect before their file was closed.

Candidates who want to request that their file be reopened 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 behaviour 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, they violate 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 ANSWERS

1. Please determine which of the following statements is true?

a) Anything that adds value to the organization is considered "Asset"

b) Decision to treat a risk is called "risk acceptance"

c) Process of selection and implementation of measures to modify risk is called "risk treatment"

d) Attack of computer virus is a vulnerability

e) Attack of computer virus is a threat

Correct answer: a)

2. An organization has installed a motion detector in their main building. What type of control is this?

a) Detective

b) Corrective

c) Preventive

d) All of the above

e) None of the above

Correct answer: c)

3. An organization that has selected clause 11.1.2 on Physical entry controls. Which of the following is explicitly required by ISO/IEC 27002:2013 standard?

a) Employees should only be granted access to locations they need to access to perform their work

b) Physical access rights should be regularly reviewed and updated;

c) Employees should wear visible identification at all time;

d) Visitors should sign a visitor's register before being granted access in work areas;

e) All of the above

Correct answer: e)