PECB BEYOND RECOGNITION

Exam Preparation Guide

ISO/IEC 27005 RISK MANAGER

GENERAL

The objective of the "PECB Certified ISO/IEC 27005 Risk Manager" exam is to ensure that the candidate has acquired the necessary knowledge and the skills to interpret information security risk management concepts, principles and generic guidelines based on ISO/IEC 27005 standard.

The ISO/IEC 27005 Risk Manager exam is intended for:

- Risk managers
- Managers or consultants responsible for the effective management of risk within an organization
- Individuals seeking to gain comprehensive knowledge of risk management concepts, processes and principles
- Members of the information security team
- IT consultants and information security professionals
- Staff implementing or seeking to comply with ISO/IEC 27001 or involved in a risk management program
- Advisors involved in Risk Management

The exam covers the following competency domains:

- **Domain 1**: Fundamental principles and concepts of information security risk management
- **Domain 2**: implementation of the information security risk management program
- **Domain 3**: Information security risk management framework and process based on ISO/IEC 27005
- **Domain 4**: Other information security risk assessment methods

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts of information security risk management

Main objective: Ensure that the ISO/IEC 27005 Risk Manager candidate understands, and is able to interpret and illustrate the main risk management guidelines and concepts related to a risk management framework based on ISO/IEC 27005

Competencies	Knowledge statements
1. Ability to understand and explain the operations of the ISO organization and the development of risk management standards 2. Ability to explain and illustrate the main concepts in information security and information security risk management 3. Ability to understand, interpret and illustrate the relationship between the concepts of asset, vulnerability, threat, likelihood, consequence and control 4. Ability to distinguish the relationship between ISO/IEC 27005, and other related standards and best practices	1. Knowledge of ISO/IEC 27005 and other standards related to risk management 2. Knowledge of the main information security concepts and terminology as described in ISO/IEC 27000 and ISO/IEC 27005 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, likelihood, impact and control 5. Knowledge of the ISO 31000 risk management principles and their application in organizations 6. Knowledge of the relationship and differences between ISO/IEC 27005, ISO/IEC 27001, ISO/IEC 27002 and ISO 31000

Domain 2: Implementation of the information security risk management program

Main objective: Ensure that the ISO/IEC 27005 Risk Manager candidate can implement an information security risk management program based on ISO/IEC 27005

Competencies	Knowledge statements
1. Ability to understand, analyze needs and provide guidance in the context of the implementation and management of an information security risk management framework 2. Ability to select a risk assessment approach for an organization 3. Ability to define and write policies and procedures 4. Ability to define the key responsibilities of the management and the principle stakeholders 5. Ability to understand the objectives, values and strategies of the organization 6. Ability to establish the external and internal context of the organization 7. Ability to define the scope and boundaries related to the information security risk management process	1. Knowledge of the roles and responsibilities of the key actors during the implementation and the operation of a risk management framework 2. Knowledge of the main organizational structures applicable for an organization to manage its risk 3. Knowledge of the best practices of the external and internal context of the organization 4. Knowledge of the characteristics and the differences between the different documents related to policies and procedures 5. Knowledge of defining the scope and boundaries of information security risk management 6. Knowledge of techniques and best practices to draft policies, procedures and others types of documents

PECB

Domain 3: Information Security Risk Management framework and process based on ISO/IEC 27005

Main objective: Ensure that the ISO/IEC 27005 Risk Manager candidate can contribute in the development of the information security risk management framework, and is able to manage risks based on the risk management process, as recommended by ISO/IEC 27005

Competencies	Knowledge statements
1. Ability to choose a risk analysis methodology 2. Ability to interpret and understand the results of a risk evaluation 3. Ability to choose a risk treatment option for different risk scenarios 4. Ability to prepare and implement the risk treatment plan 5. Ability to ensure communication and consultation between the decision-makers, external and internal stakeholders 6. Ability to monitor and review the risk management process and the implemented controls 7. Ability to ensure continual improvement of the risk management program	1. Knowledge of the qualitative and quantitative risk analysis methodologies 2. Knowledge of planning risk assessment projects and activities by ensuring the participation and support of stakeholders throughout the risk assessment process 3. Knowledge of estimating the risk level according to the evaluation criteria and the risk acceptance criteria 4. Knowledge of the risk treatment options including risk modification, risk retention, risk avoidance and risk sharing 5. Knowledge of monitoring and review of specific elements of risk factors and risk management 6. Knowledge of setting continual improvement objectives

PECB

Domain 4: Other information security risk assessment methods

Main objective: Ensure that the ISO/IEC 27005 Risk Manager candidate can use other risk assessment methodologies such as OCTAVE, MEHARI, EBIOS and Harmonized Threat and Risk Assessment (TRA) Method

Competencies	Knowledge statements
1. Ability to understand the three OCTAVE versions: OCTAVE, OCTAVE-S, and OCTAVE-Allegro 2. Ability to implement the results from OCTAVE-S process performed in three phases 3. Ability to conduct a risk assessment using the OCTAVE Allegro process following its eight steps 4. Ability to conduct a risk assessment using the MEHARI method and its four phases 5. Ability to conduct a risk assessment using the EBIOS methodology and its five modules 6. Ability to interpret the application of ISO/IEC 27005 in EBIOS 7. Ability to conduct a risk assessment using the Harmonized Threat and Risk Assessment (TRA) method and its five phases	1. Knowledge of the three phases of the OCTAVE method 2. Knowledge of identifying infrastructure vulnerabilities and developing security strategy and plans as specified in the OCTAVE-S method 3. Knowledge of the OCTAVE Allegro roadmap. 4. Knowledge of the four phases of the MEHARI approach 5. Knowledge of the five modules of EBIOS risk assessment methodology 6. Knowledge of the relationship between EBIOS & ISO/IEC 27005 7. Knowledge of the five phases of Harmonized Threat and Risk Assessment (TRA) methodology

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

			Leve l 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 Risk Management	5	X		3	42.85	20	40
		5	X					
		10	X					
	Implementation of the Information Security Risk Management program	10		X	1	14.29	10	20
	Information Security risk management framework and process based on ISO/IEC 27005	10		X	2	28.57	15	30
		5		X				
	Other Information Security risk assessment methods	5	X		1	14.29	5	10
Total points		50						
Number of Questions per level of understanding			4	3				
% of Test Devoted to each level of understanding (cognitive/taxonomy)			57.14	42.85				

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

After successfully passing the exam, candidates will be able to apply for "PECB Certified ISO/IEC 27005 Risk Manager" credential, depending on their level of experience.

TAKE THE EXAM

Candidates will be required to arrive at least 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 duration of the exam is two hours. Non-native speakers will receive an additional 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.

Since the exam is "open book", candidates are authorized to use:

- A copy of the **ISO/IEC 27005** standard
- Course notes from the Participant Handout
- Any personal notes made by the student during the training course
- A hard copy dictionary

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

All 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 via email within a period of six to eight weeks from the exam date. The candidate will be provided with only two possible exam results: pass or fail, rather than an exact grade.

In case of exam failure, the results will be accompanied with the list of domains in which the candidate has 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, the candidate must wait 15 days (from the initial date of the exam) for the next attempt (first retake). The retake fee applies.

  Note: *Candidates who have completed the full training course 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, the candidate must wait three months (from the initial date of the exam) for the next attempt (second retake). The retake fee applies.

- If a candidate does not pass the exam on the third attempt, the candidate must wait six months (from the initial date of the exam) for the next attempt (third retake). The 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. The regular fee applies.

For the candidates that fail the exam in the second retake, PECB recommends to attend an official training course 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 training course 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.

Exam 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 - Identification of assets:

Explain why the assets below have the highest value to an organization. Please identify whether the following are primary or supporting assets:

Asset 1: The organization's website
Asset 2: The organization's two owners

Possible answers:

Asset 1: The organization's website

- Justification of the value: The website of the organization is the main marketing tool and supports the selling process
- The organization's website is a primary asset

Asset 2: The organization's two owners

- Justification of the value: They initiate original ideas that lead to innovative products
- The organization's personnel is considered as a supporting asset

Question 2: Information security risk identification

Identify threats, vulnerabilities and impacts associated with the incident scenarios below and indicate if it is possible that the impacts affect the availability, integrity and/or the confidentiality of the information. Complete the risk matrix.

Possible answers:

Statement	Vulnerabilities	Threats	C	I	A	Potential Impacts
1. The person who designed the website of the corporate, is the only one who takes care of the updates and the uploading of the site.	Absence of segregation of duties.	Treatment errors		X		Website containing erroneous information: loss of credibility
	Only one person is available for this function	Malicious act	X			Unavailable website: loss in revenues
		The person leaves the company or is sick and unavailable			X	Loss of reputation and customers trust in cases of malicious acts.

Address:
Head Quarters
6683 Jean Talon E,
Suite 336 Montreal,
H1S 0A5, QC,
CANADA

Tel./Fax.
T: +1-844-426-7322
F: +1-844-329-7322

PECB Help Center
Visit our Help Center to browse Frequently Asked Questions (FAQ), view manuals for using PECB website and applications, read documents related to PECB processes, or to contact us via Support Center's online tracking system. Visit Help Center here: www.pecb.com/help

Emails:
Examination: examination@pecb.com
Certification: certification@pecb.com
Customer Care: customer@pecb.com