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 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 an 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 an information security risk management

Main objective: Ensure that the candidate understands, and is able to interpret 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 contro 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 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

Domain 3: Information security risk management framework and process based on ISO/IEC 27005

Main objective: Ensure that the candidate can contribute in the development of an 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

Domain 4: Other information security risk assessment methods

Main objective: Ensure that the 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:

				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 the exam 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 an 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 the exam devoted to each level of understanding (cognitive/taxonomy)		57.14	42.85				

The exam passing score is **70%**.

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

General Information on the Exam

Candidates are required to arrive/be present at least 30 minutes before the exam starts. Candidates who arrive late will not be given additional time to compensate for the late arrival and may not be allowed to sit for the exam.

Candidates are required to bring a valid identity card (a national ID card, driver's license, or passport) and show it to the invigilator.

If requested on the day of the exam (paper-based exams), additional time can be provided to candidates taking the exam in a non-native language, as follows:

- 10 additional minutes for Foundation exams
- 20 additional minutes for Manager exams
- 30 additional minutes for Lead exams

PECB Exam Format and Type

1. Paper-based: Exams are provided on paper, where candidates are not allowed to use anything but the exam paper and a pen. The use of electronic devices, such as laptops, tablets, or phones, is not allowed. The exam session is supervised by a PECB approved Invigilator at the location where the Reseller has organized the training course.

2. Online: Exams are provided electronically via the PECB Exams application. The use of electronic devices, such as tablets and cell phones, is not allowed. The exam session is supervised remotely by a PECB Invigilator via the PECB Exams application and an external/integrated camera.

For more detailed information about the online format, please refer to the PECB Online Exam Guide.

PECB exams are available in two types:
1. Essay-type question exam
2. Multiple-choice question exam

This exam comprises essay-type questions. They are used to determine and evaluate whether a candidate can clearly answer questions related to the defined competency domains. Additionally, problem-solving techniques and arguments that are supported with reasoning and evidence will also be evaluated.

The exam is open book and is not intended to measure memorizing or recalling information. It aims to evaluate candidates' comprehension, analytical skills, and applied knowledge. Therefore, candidates are required to provide logical and convincing answers and explanations in order to demonstrate that they have understood the content and the main concepts of the competency domains.

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

- A copy of the ISO/IEC 27005 standard
- Training course materials(accessed through PECB Exams app and/or printed)
- Any personal notes made by the candidate during the training course(accessed through PECB Exams app and/or printed)
- A hard copy dictionary

Any attempt to copy, collude, or otherwise cheat during the exam session will lead to automatic failure.

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

Note: PECB will progressively transition to multiple-choice exams. They will also be open book and comprise scenario-based questions that will allow PECB to evaluate candidates' knowledge, abilities, and skills to use information in new situations (apply), draw connections among ideas (analyze), and justify a stand or decision (evaluate). All PECB multiple-choice exams have one question and three alternatives, of which only one is correct.

For specific information about exam types, languages available, and other details, visit the List of PECB Exams.

Receiving the Exam Results

Exam results will be communicated via email. The only possible results are *pass* and *fail;* no specific grade will be included.

- The time span for the communication starts from the exam date and lasts three to eight weeks for essay type exams and two to four weeks for multiple-choice paper-based exams

- For online multiple-choice exams, candidates receive their results instantly

Candidates who successfully complete the exam will be able to apply for one of the credentials of the respective certification scheme.

For candidates who fail the exam, a list of the domains where they have performed poorly will be added to the email to help them prepare better for a retake.

Candidates that disagree with the results may request for a re-evaluation by writing to results@pecb.com within 30 working days of receiving the results. Re-evaluation requests received after 30 days will not be processed. If candidates do not agree with the results of the reevaluation, they have 30 working days from the date when they received the reevaluated exam results to file a complaint through the PECB Ticketing System. Complaints received after 30 days will not be processed.

Exam Retake Policy

There is no limit on the number of times that a candidate may retake an exam. However, there are certain limitations in terms of the allowed time frames between exam retakes.

- If a candidate does not pass the exam on the 1st attempt, they must wait 15 days from the initial date of the exam for the next attempt (1st retake). Retake fees apply.
  Note: *Candidates who have completed the training course but failed the 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 2nd attempt, they must wait three months after the initial date of the exam for the next attempt (2nd retake). Retake fees apply.
  Note: *For candidates that fail the exam in the 2nd retake, PECB recommends them to attend a training course in order to be better prepared for the exam.*
- If a candidate does not pass the exam on the 3rd attempt, they must wait six months after the initial date of the exam for the next attempt (3rd retake). Retake fees apply.
- After the 4th attempt, the waiting period for further retake exams is 12 months from the date of the last attempt. Retake fees apply.

To arrange exam retakes (date, time, place, costs), candidates need to contact the PECB Reseller/Distributor who has initially organized the session.

Reschedule the Exam

For any changes with regard to the exam date, time, location, or other details, please contact examination@pecb.com.

Closing a Case

If a candidate does not apply for the certificate within three years, their case will be closed. Candidates whose case has been closed due to the expiration of the certification period have the right to request to reopen their case. However, PECB will no longer be responsible for any changes in the conditions, standards, policies, candidate handbook, or exam preparation guide that were applicable before the case was closed. A candidate requesting their case to reopen must do so in writing and pay the required fee.

Exam Security

A significant component of a successful and respected professional certification credential is maintaining the security and confidentiality of the exam. PECB relies upon the ethical behavior of certificate holders and applicants to maintain the security and confidentiality of PECB exams. Any disclosure of information about the content of PECB exams indicates violation of PECB's Code of Ethics. PECB will take action against individuals who violate PECB Policies and the Code of Ethics. These actions include permanently barring individuals from pursuing PECB credentials and revoking the awarded credentials. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

PECB

Sample Exam Questions

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 answer:
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 answer:

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. Only one person is available for this function	Treatment errors Malicious act The person leaves the company or is sick and unavailable	 X	X	 X	Website containing erroneous information: loss of credibility Unavailable website: loss in revenues 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