PECB

When Recognition Matters

EXAM PREPARATION GUIDE

PECB Certified ISO/IEC 27005 Lead Risk Manager

The objective of the “PECB Certified ISO/IEC 27005 Lead Risk Manager” examination is to ensure that the candidate has the knowledge and the skills to support an organization to identify, analyze, prioritize and manage information security risks. Furthermore, the objective of this examination is to ensure that the candidate also has the knowledge and the skills to support an organization in implementing and managing an information security risk management program using the ISO/IEC 27005:2011 standard as a reference framework.

The target population for this examination is (this is a non-exhaustive list):

- Risk managers
- Auditors seeking to understand the implementation of a risk management program based on ISO/IEC 27005
- Persons responsible for information security or conformity within an organization
- Members of an information security team who need to ensure that information security risks are being effectively managed
- IT consultants, information security managers
- Staff implementing or seeking to comply with ISO/IEC 27001 or involved in the implementation of a risk management program
- Risk analysts

The exam content covers the following domains:

Domain 1: Fundamental principles and concepts of Information Security Risk Management
Domain 2: Implementation of an Information Security Risk Management program
Domain 3: Information security risk assessment
Domain 4: Information security risk treatment
Domain 5: Information security risk communication, monitoring and improvement
Domain 6: Information security risk assessment methodologies

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts of Information Security Risk Management

Main objective: To ensure that the ISO/IEC 27005 Lead Risk Manager candidate can understand, interpret and illustrate the main information security risk management guidelines and concepts related to the risk management framework based on ISO/IEC 27005

Competencies	Knowledge statements
1. Understand and explain the structure of ISO/IEC 27005 and its framework 2. Ability to identify, analyze and evaluate the guidance of different information security risk management frameworks 3. Ability to explain and illustrate the main concepts in information security and information security risk management 4. Ability to distinguish the relationship between ISO/IEC 27005, and other related standards 5. Ability to understand, interpret and illustrate the relationship between the concepts of asset, threat, likelihood, consequence and controls	1. Knowledge of basic concepts for the implementation of an information security risk management program 2. Knowledge of the main standards and frameworks of risk management 3. Knowledge of the main information security concepts and terminology as described in ISO/IEC 27000 & ISO/IEC 27005 4. Knowledge of the concept of risk and its application in information security 5. Knowledge of the 11 principles of Risk Management as described in ISO 3100 6. Knowledge of the relationship between the concepts of asset, threat, likelihood, impact and controls 7. Knowledge of the relationship and differences between ISO/IEC 27005, ISO/IEC 27001, ISO/IEC 27002 and ISO 31000

Domain 2: Implementation of an Information Security Risk Management Program

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

Competencies	Knowledge statements
1. Ability to understand, analyze and provide guidance of the attribution of roles and responsibilities in the context of the implementation and management of an information security risk management framework 2. Ability to implement the required processes of an information security risk management framework 3. Ability to define, write and establish risk management policies and procedures 4. Ability to understand several recognized risk assessment methodologies 5. Ability to identify, review and select a risk assessment approach appropriate for a specific organization 6. Ability to integrate the information security risk management framework into organizational processes by appointing key responsibilities of key players 7. Ability to understand the objectives, values and strategies of the organization 8. Ability to identify the external and internal context of the organization 9. Ability to identify the basic criteria for the evaluation of information security risk 10. Ability to define the scope and boundaries related to the information security risk management process 11. Ability to define and analyze the stakeholders of an organization	1. Knowledge of the roles and responsibilities of the key actors during the implementation of a risk management framework and its operation 2. Knowledge of the main organizational structures applicable for the management of the risk within an organization 3. Knowledge of the most frequently used practices during the establishment of external and internal context of the organization 4. Knowledge of techniques and best practices to write policies, procedures and others types of required documentation 5. Knowledge of the objectives of a risk management program and risk assessment process 6. Knowledge of key aspects of external and internal context 7. Knowledge of different information security risk assessment approaches 8. General knowledge of the main risk assessment methodologies, including EBIOS, MEHARI and OCTAVE 9. Knowledge of the process of information security risk management and its relation with the scope and boundaries 10. Knowledge of typical stakeholders and their requirements

Domain 3: Information security risk assessment

Main objective: To ensure that the ISO/IEC 27005 Lead Risk Manager candidate can perform a risk assessment according to best practices and guidelines provided by ISO/IEC 27005

Competencies	Knowledge statements
1. Ability to identify, recognize and record information security risks according to ISO/IEC 27005 2. Ability to understand and interpret the identification of assets, threats, existing controls, vulnerabilities, and consequences 3. Ability to identify primary and supporting assets of an organization 4. Ability to identify the consequences in terms of confidentiality, integrity and availability of assets 5. Ability to generate, interpret and understand risk analysis reports 6. Ability to perform risk assessments in various settings and establishments 7. Ability to assess the likelihood and determine the level of risk for each identified incident scenario 8. Ability to choose a risk analysis methodology that suits the needs of the organization 9. Ability to calculate the level of risk in terms of the combination of consequences and their likelihood 10. Ability to conduct, interpret and understand a risk evaluation 11. The ability to set the evaluation criteria 12. Ability to plan activities for a risk assessment process and integrate risk assessment processes to information security risk management frameworks and an ISMS	1. Knowledge on planning risk assessment projects and activities by ensuring the participation and support of stakeholders throughout the risk assessment process. 2. Knowledge of information gathering techniques 3. Knowledge on identification of assets, risk sources, vulnerabilities, existing measures, impacts, incident likelihood and the relation between these concepts 4. Knowledge of the qualitative and quantitative risk analysis methodologies 5. General knowledge of ROSI quantitative method 6. Knowledge on likelihood assessment and risk level determination for different identified incident scenarios 7. Knowledge of risk level estimation according to the evaluation criteria and the risk acceptance criteria 8. Knowledge on the outcomes of risk analysis and risk prioritization 9. Knowledge of the guidelines and best practices of risk assessment integration based on ISO/IEC 27005

Domain 4: Information security risk treatment

Main objective: To ensure that the ISO/IEC 27005 Lead Risk Manager candidate can apply and conduct a risk treatment process as part of an information security risk management framework based on ISO/IEC 27005

Competencies	Knowledge statements
1. Ability to understand the risk treatment process based on ISO/IEC 27005 2. Ability to understand and manage information security risk by identifying, analyzing, and evaluating whether the risk should be modified by risk treatment controls 3. Ability to select the appropriate controls to reduce, retain, avoid or share the risks 4. The ability to draft, propose and implement different risk treatment plans 5. Ability to evaluate the residual risk	1. General knowledge of the risk treatment process 2. Knowledge of the risk treatment options including risk modification, risk retention, risk avoidance and risk sharing 3. Knowledge of the best practices related with risk treatment options 4. Knowledge of residual risk evaluation based on the risk acceptance criteria 5. Knowledge of documenting the chosen treatment options by a risk treatment plan 6. General knowledge of information needed to compose a risk treatment plan

Domain 5: Information security risk communication, monitoring and improvement

Main objective: To ensure that the ISO/IEC 27005 Lead Risk Manager candidate can apply processes for information security risk communication, consultation, monitoring and review based on ISO/IEC 27005.

Competencies	Knowledge statements
1. Ability to comprehend and evaluate requirements of information security risk communication objectives 2. Ability to understand the importance of a good communication 3. The ability to establish an efficient internal communication within the organization 4. The ability to establish an efficient communication with the external stakeholders 5. Ability to ensure communication and consultation between the decision-makers and external & internal stakeholders 6. Ability to establish a risk communication plan 7. Ability to record the information security risk management decisions and activities 8. Ability to monitor and review the risk management process, risks and controls 9. Ability to ensure continual improvement of the risk management program	1. General knowledge of the information security communication process 2. Knowledge of the principles of an efficient communication strategy 3. Knowledge of establishing internal communication within the organization 4. Knowledge of establishing external communication with stakeholders 5. Knowledge of communication activities 6. Knowledge of monitoring and review of specific elements of risk factors 7. Knowledge of monitoring and review of risk management 8. Knowledge of setting continual improvement objectives 9. Knowledge of ensuring risk management recording

Domain 6: Information security risk assessment methodologies

Main objective: To ensure that the ISO/IEC 27005 Lead 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: the original 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 understand the relationship between OCTAVE Allegro & ISO/IEC 27005 5. Ability to conduct a risk assessment using the MEHARI method and its four phases 6. Ability to conduct a risk assessment using the EBIOS methodology and its five modules 7. Ability to interpret the application of ISO/IEC 27005 in EBIOS 8. Ability to conduct a risk assessment using the Harmonized Threat and Risk Assessment (TRA) method and its five phases	1. General knowledge of the three phases of the original OCTAVE method 2. Knowledge of building asset based threat profiles, 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 similarities and differences between OCTAVE Allegro & ISO/IEC 27005 5. Knowledge of the four phases of the MEHARI approach 6. Knowledge of the five modules of EBIOS risk assessment methodology 7. Knowledge of the relationship between EBIOS & ISO/IEC 27005 8. Knowledge of the five phases of Harmonized Threat and Risk Assessment (TRA) methodology

Based on these six domains and their relevance, twelve (12) questions are included in the exam, as summarized in the following table:

			Leve I 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		1	8.33	5	6.66
	Implementation of an Information Security Risk Management program	5	X		1	8.33	5	6.66
	Information security risk assessment	10		X	3	25	25	33.33
		5	X					
		10	X					
	Information security risk treatment	5		X	3	25	15	20
		5	X					
		5	X					
	Information security risk communication, monitoring and improvement	10		X	3	25	20	26.66
		5		X				
		5		X				
	Information security risk assessment methodologies	5	X		1	8.33	5	6.66
Total points		75						
Number of Questions per level of understanding			7	5				
% of Test Devoted to each level of understanding (cognitive/taxonomy)			58.33	41.66				

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 27005 Lead Risk Manager, depending on their level of experience.

TAKE THE 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 (3) hours.

The questions are essay type questions. This type of format was chosen because the intent is to determine whether an examinee can write a clear coherent answer/argument and to assess problem solving techniques. Because of this particularity, the exam is set to be "open book" and does not measure the recall of data or information. The examination evaluates, instead, comprehension, application, analysis, synthesis and evaluation, which mean that even if the answer is in the course material, candidates will have to justify and give explanations, to show they really understood the concepts. At the end of this document, you will find sample exam questions and their possible answers.

As the exams are "open book"; candidates are only authorized to use:

- A copy of the ISO/IEC 27005:2011 standard,
- Course notes from the Participant Handout,
- Any personal notes made by the student during the course and
- A hard copy dictionary.

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

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 6 to 8 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 limit on the number of times a candidate may retake an exam. However, there are some limitations in terms of 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: *Students, 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 candidate to sit again for 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 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 POSSIBLE ANSWERS

1. Framework and information security risk management process

Being a specialist with an advisory role in the information security risk management system, please describe briefly the most important steps that you should take into consideration when trying to achieve a better implementation of the information security risk management framework?

Possible answer:

Information Security Risk Management framework is a necessary part of planning, preparing, and executing organizational missions. Therefore the most important steps can be the following:

1. Uncover, recognize and describe all the risk that might affect outcomes of the company using different techniques.
2. After identification, determine the likelihood and consequence of each risk and their potential consequence.
3. Address the risk and make a plan of risk identification
4. Improve the managing of any risk that affects the organization.
5. Evaluate the risk by determining risk magnitude, and set out a plan how to treat and modify them to be on an acceptable level.

2. Identification of assets

Identify whether the following assets are primary or supporting assets. Also, explain the justification of their value to the organization.

Asset 1: Website
Asset 2: Organization’s owners

Possible answers:

Asset 1: Website - Primary asset

Justification of the value: The website of the company is the main marketing tool and supports the selling process.

Asset 2: Organization’s owners - Supporting asset

Justification of the value: They are the ones creating original and innovative products.