PECB BEYOND RECOGNITION

Exam Preparation Guide

ISO/IEC 27005 Lead Risk Manager

GENERAL

The objective of the "PECB Certified ISO/IEC 27005 Lead Risk Manager" exam is to ensure that the candidate has the necessary expertise 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 standard as a reference framework.

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

- Risk managers
- Auditors seeking to understand the implementation of the 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 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 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 an information security risk management **Main objective:** Ensure that the candidate can understand, and is able to interpret the main information security risk management guidelines and concepts related to the risk management framework based on ISO/IEC 27005	
Competencies	**Knowledge statements**
1. Ability to 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 31000 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 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 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: Ensure that the candidate can perform a risk assessment according to the 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. 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: Ensure that the 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: Ensure that the 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. 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: 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: 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 the above-mentioned domains and their relevance, 12 questions are included in the exam, as summarized in the table below:

			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		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 exam passing score is **70%**

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

Taking the Exam

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

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: Framework and information security risk management process

XBeing a specialist with an advisory role in the information security risk management system, can you 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***

Evaluate the risk by determining risk magnitude, and set out a plan how to treat and modify them to be on an acceptable level

Question 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 answer:

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

© 2020 PECB

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

Copyright © 2020 PECB. Reproduction or storage in any form for any purpose is not permitted without a PECB prior written permission.