PECB BEYOND RECOGNITION

Candidate Handbook

ISO/IEC 27005 LEAD RISK MANAGER

PECB

Table of Contents

SECTION I: INTRODUCTION

About PECB

PECB is a certification body which provides education[1] and certification in accordance with ISO/IEC 17024 for individuals on a wide range of disciplines.

We help professionals show commitment and competence by providing them with valuable evaluation and certification services against internationally recognized standards. Our mission is to provide services that inspire trust and continual improvement, demonstrate recognition, and benefit the society as a whole.

The key objectives of PECB are:

1. Establishing the minimum requirements necessary to certify professionals
2. Reviewing and verifying the qualifications of applicants to ensure they are eligible to apply for certification
3. Developing and maintaining reliable certification evaluations
4. Granting certifications to qualified candidates, maintaining records, and publishing a directory of the holders of a valid certification
5. Establishing requirements for the periodic renewal of certification and ensuring compliance with those requirements
6. Ensuring that candidates meet ethical standards in their professional practice
7. Representing its members, where appropriate, in matters of common interest
8. Promoting the benefits of certification to organizations, employers, public officials, practitioners in related fields, and the public

[1] Education refers to training courses developed by PECB, and offered globally through our network of resellers.

The Value of PECB Certification

Why Choose PECB as Your Certification Body?

Global Recognition
Our certifications are internationally recognized and accredited by the International Accreditation Service (IAS); signatory of IAF Multilateral Recognition Arrangement (MLA) which ensures mutual recognition of accredited certification between signatories to the MLA and acceptance of accredited certification in many markets. Therefore, professionals who pursue a PECB certification credential will benefit from PECB's recognition in domestic and international markets.

Competent Personnel
The core team of PECB consists of competent individuals who have relevant sector-specific experience. All of our employees hold professional credentials and are constantly trained to provide more than satisfactory services to our clients.

Compliance with Standards
Our certifications are a demonstration of compliance with ISO/IEC 17024. They ensure that the standard requirements have been fulfilled and validated with the adequate consistency, professionalism, and impartiality.

Customer Service
We are a customer-centered company and treat all our customers with value, importance, professionalism, and honesty. PECB has a team of experts dedicated to support customer requests, problems, concerns, needs, and opinions. We do our best to maintain a 24-hours maximum response time without compromising the quality of the service.

PECB Code of Ethics

PECB professionals will:

1. Conduct themselves professionally, with honesty, accuracy, fairness, responsibility, and independence
2. Act at all times solely in the best interest of their employer, their clients, the public, and the profession, by adhering to the professional standards and applicable techniques while offering professional services
3. Maintain competency in their respective fields and strive to constantly improve their professional capabilities
4. Offer only professional services for which they are qualified to perform, and adequately inform clients about the nature of the proposed services, including any relevant concerns or risks
5. Inform each employer or client of any business interests or affiliations that might influence their judgment or impair their fairness
6. Treat in a confidential and private manner the information acquired during professional and business dealings of any present or former employer or client
7. Comply with all laws and regulations of the jurisdictions where professional activities are conducted
8. Respect the intellectual property and contributions of others
9. Not, intentionally or otherwise, communicate false or falsified information that may compromise the integrity of the evaluation process of a candidate for a professional designation
10. Not act in any manner that could compromise the reputation of PECB or its certification programs
11. Fully cooperate on the inquiry following a claimed infringement of this Code of Ethics

The full version of the PECB Code of Ethics can be downloaded here.

Introduction to ISO/IEC 27005 Lead Risk Manager

ISO/IEC 27005 provides the guidelines for managing information security risks. It also supports the general concepts of information security specified in ISO/IEC 27001. As the cyberspace grows increasingly dangerous, protecting against information security threats has become essential for most organizations. A core component of information security is risk management. Thus, one of the most on-demand skills in the market is the ability to establish and implement a systematic approach to information security risk management.

The "ISO/IEC 27005 Lead Risk Manager" credential is a professional certification for individuals aiming to demonstrate the competence to effectively manage information security risks. An internationally recognized certification add great value to your career and will help you reach your professional objectives.

It is important to understand that PECB certifications are not a license or simply a membership. They represent peer recognition that an individual has demonstrated proficiency in, and comprehension of, a set of competencies. PECB certifications are awarded to candidates that can demonstrate experience and have passed a standardized exam in the certification area.

This document specifies the PECB ISO/IEC 27005 Lead Risk Manager certification scheme in compliance with ISO/IEC 17024:2012. This candidate handbook also contains information about the process by which candidates may earn and maintain their credentials. It is very important that you read all the information included in this candidate handbook before completing and submitting your application. If you have questions after reading it, please contact the PECB international office at certification@pecb.com.

SECTION II: PECB CERTIFICATION PROCESS AND EXAMINATION PREPARATION, RULES, AND POLICIES

Decide Which Certification Is Right for You

All PECB certifications have specific education and professional experience requirements. To determine the right credential for you, verify the eligibility criteria for various certifications and your professional needs.

Prepare and Schedule the Exam

All candidates are responsible for their own study and preparation for certification exams. No specific set of training courses or curriculum of study is required as part of the certification process. Nevertheless, attending a training course can significantly increase candidates' chances of successfully passing a PECB exam.

To schedule an exam, candidates have two options:

1. Contact one of our resellers who provide training courses and exam sessions. To find a training course provider in a particular region, candidates should go to Active Resellers. The PECB training course schedule is also available on Training Events.
2. Take a PECB exam remotely from their home or any location they desire through the PECB Exam application, which can be accessed here: Exam Events.

To learn more about exams, competency domains, and knowledge statements, please refer to *Section III* of this document.

Application Fees for Examination and Certification

PECB offers direct exams, where a candidate can sit for the exam without attending the training course. The applicable prices are as follows:

- Lead Exam: $1000
- Manager Exam: $700
- Foundation and Transition Exam: $500

The application fee for certification is $500.

For all candidates that have followed the training course and taken the exam with one of PECB's resellers, the application fee includes the costs associated with examination, application for certification, and the first year of Annual Maintenance Fee (AMF) only.

Competency Domains

The objective of the **"PECB Certified ISO/IEC 27005 Lead Risk Manager"** exam is to ensure that the candidate has acquired the necessary expertise to support an organization in establishing, implementing, and managing an information security risk management program.

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

- Managers or consultants involved in or responsible for information security in an organization
- Individuals responsible for managing information security risks
- Members of information security teams, IT professionals, and privacy officers
- Individuals responsible for maintaining conformity with the information security requirements of ISO/IEC 27001 in an organization

- Project managers, consultants, or expert advisers seeking to master the management of information security risks

The exam covers the following competency 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

Domain 1: Fundamental principles and concepts of information security risk management **Main objective:** Ensure that the candidate understands and is able to interpret the main principles and concepts of information security risk management	
Competencies	**Knowledge statements**
1. Ability to understand and explain the structure of ISO/IEC 27005 2. Ability to understand the relation between ISO/IEC 27005 and other risk management frameworks 3. Ability to understand and explain the concept of information security 4. Ability to understand the principles of information security: confidentiality, integrity, and availability 5. Ability to understand and interpret the definition of risk 6. Ability to understand the main concepts and principles of risk management 7. Ability to understand information security vulnerabilities and threats 8. Ability to understand the differences between the concepts of risks and opportunities 9. Ability to understand the classification of security controls by type and function 10. Ability to understand the role of the risk owner	1. Knowledge of the main concepts and terminology of ISO/IEC 27005 2. Knowledge of the main standards of the ISO/IEC 27000 family 3. Knowledge of international and industry standards and frameworks for information security and risk management 4. Knowledge of information security risks and opportunities 5. Knowledge of the definition of vulnerability 6. Knowledge of threats and threat sources related to information security 7. Knowledge of confidentiality, integrity, and availability of information 8. Knowledge of the type and function of security controls 9. Knowledge of risk management principles 10. Knowledge of the roles and responsibilities of the risk owner 11. Knowledge of risk management advantages

PECB

Domain 2: Implementation of an information security risk management program

Main objective: Ensure that the candidate understands and is able to initiate the implementation of a risk management program based on ISO/IEC 27005

Competencies

1. Ability to understand the integration of the PDCA cycle into the information security risk management program
2. Ability to understand and explain the main steps needed for establishing and implementing an information security risk management program
3. Ability to identify the roles and responsibilities of key stakeholders during and after the implementation and operation of an information security risk management program
4. Ability to understand the concept of risk assessment
5. Ability to define an appropriate risk assessment approach based on the organization's context
6. Ability to identify the resources required for the implementation of a risk management program
7. Ability to understand the importance of a risk management policy
8. Ability to analyze and consider the internal and external context of an organization
9. Ability to understand key processes and activities of an organization
10. Ability to understand and set objectives for the risk management program
11. Ability to define and justify the information security risk management process scope and adapt it to organization's objectives

Knowledge statements

1. Knowledge of the risk management process
2. Knowledge of how the top management can demonstrate leadership and commitment regarding risk management
3. Knowledge of the roles and responsibilities of a risk manager regarding the risk management program
4. Knowledge of the roles and responsibilities of key stakeholders in the implementation of a risk management program
5. Knowledge of the approaches and methodologies used for information security risk assessment
6. Knowledge of what typically constitutes an organization's internal and external context
7. Knowledge of the importance of understanding key processes and activities of an organization in risk management
8. Knowledge of the main steps for planning risk assessment activities
9. Knowledge of risk assessment objectives and how to achieve specific results
10. Knowledge of the characteristics of an information security risk management program
11. Knowledge of how the risk evaluation criteria and impact criteria are defined
12. Knowledge of the applicability of quantitative and qualitative analysis in determining risk acceptance criteria
13. Knowledge of the resources required for information security risk management
14. Knowledge of the information security risk management scope and boundaries

PECB

Domain 3: Information security risk assessment **Main objective:** Ensure that the candidate is able to identify, analyze, and evaluate risks based on ISO/IEC 27005	
Competencies	**Knowledge statements**
1. Ability to understand the processes of information security identification, analysis, and evaluation 2. Ability to understand and interpret information gathering techniques 3. Ability to identify assets, threats, existing controls, vulnerabilities, and consequences 4. Ability to understand the types of assets, as defined in ISO/IEC 27005 5. Ability to understand the role of asset owners 6. Ability to understand the process of asset valuation 7. Ability to identify the types of threats and vulnerabilities, as defined in ISO/IEC 27005 8. Ability to understand various methods for identifying existing controls 9. Ability to understand and explain the methods for vulnerability assessment 10. Ability to understand and interpret risk analysis methodologies 11. Ability to understand how consequences can be defined based on nonnumerical categories, numerical rating scales, and practical values 12. Ability to understand and perform assessment of consequences and incident likelihood and determine the level of risk 13. Ability to understand the types of risk ratings: inherent, residual, and target risk 14. Ability to evaluate the levels of risk based on the risk evaluation criteria 15. Ability to compare the results of the risk analysis with the established risk criteria to determine if an additional action is required 16. Ability to understand risk prioritization	1. Knowledge of information security risk assessment processes, including risk identification, analysis, and evaluation 2. Knowledge of the methods to perform information security risk assessment and information gathering techniques 3. Knowledge of the definition of an asset and the identification of primary and supporting assets 4. Knowledge of the relationship of primary and supporting assets 5. Knowledge of the process of asset valuation and inventory of assets 6. Knowledge of the identification and classification of threats 7. Knowledge of the identification of existing controls 8. Knowledge of how vulnerabilities should be identified using vulnerability assessment techniques 9. Knowledge of the relationship between assets, vulnerabilities, and threats 10. Knowledge of the identification of consequences that may affect availability, confidentiality, integrity 11. Knowledge of risk analysis methodologies 12. Knowledge of how consequences and incident likelihood should be assessed and how the level of risk should be determined 13. Knowledge of the evaluation of the levels of risk based on risk evaluation criteria 14. Knowledge of risk evaluation approaches 15. Knowledge of inherent, residual, and target risks, and their relationship 16. Knowledge of risk prioritization 17. Knowledge of the main concepts of quantitative risk assessment

PECB

Domain 4: Information security risk treatment **Main objective:** Ensure that the candidate is able to treat the identified risks as part of the information security risk management process	
Competencies	**Knowledge statements**
1. Ability to understand the risk treatment process based on ISO/IEC 27005 2. Ability to understand and interpret risk treatment options 3. Ability to understand how the risk level can be reduced through the selection of security controls 4. Ability to select appropriate controls to reduce, retain, avoid, or share the risks 5. Ability to draft and implement risk treatment plans 6. Ability to evaluate the residual risk 7. Ability to understand and explain information security risk acceptance 8. Ability to calculate residual risk 9. Ability to understand the processes of risk treatment plan acceptance and residual risk acceptance 10. Ability to understand the management of residual risk	1. 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 how the risk level can be reduced through the selection of adequate security controls 4. Knowledge of the best practices related to risk treatment options 5. Knowledge of how a risk treatment plan should be prepared 6. Knowledge of the implementation of risk treatment plans 7. Knowledge of how residual risks are evaluated 8. Knowledge of information security risk acceptance 9. Knowledge of how the criteria of risk acceptance should be determined 10. Knowledge of the acceptance of residual risk 11. Knowledge of the management of residual risk

PECB

Domain 5: Information security risk communication, monitoring, and improvement

Main objective: Ensure that the candidate understands and is able to apply processes for information security risk management communication, consultation, monitoring, and review based on ISO/IEC 27005

Competencies

1. Ability to comprehend and interpret the concept of risk communication and consultation
2. Ability to understand and interpret principles of effective communication
3. Ability to understand the objectives of a risk communication
4. Ability to establish a risk communication plan to assist in the understanding of an organization's information security issues, policies, and performance and providing inputs or suggestions for improving the performance of the information security risk management program
5. Ability to understand and establish internal and external communication
6. Ability to ensure communication and consultation between decision-makers and external and internal stakeholders
7. Ability to understand communication methods and tools
8. Ability to record the information security risk management decisions and activities
9. Ability to monitor and evaluate the effectiveness of an information security risk management program
10. Ability to understand the concept of continual improvement and its advantages regarding risk management
11. Ability to advise an organization on how to continually improve the effectiveness and efficiency of an information security risk management program
12. Ability to determine the appropriate tools to support the continual improvement of an organization

Knowledge statements

1. Knowledge of the information security risk communication process
2. Knowledge of the principles of an efficient communication strategy
3. Knowledge of how the risk communication plan should be established
4. Knowledge of the communication objectives, activities, and interested parties to enhance their support and confidence
5. Knowledge of how internal and external communication should be established
6. Knowledge of risk communication principles and objectives
7. Knowledge of the best practices and techniques used to monitor and evaluate the effectiveness of an information security risk management program
8. Knowledge of the concepts related to measurement and evaluation
9. Knowledge of the main concepts related to continual improvement
10. Knowledge of the processes related to the continual monitoring of change factors
11. Knowledge of the maintenance and improvement of an information security risk management program

PECB

Domain 6: Information security risk assessment methodologies

Main objective: Ensure that the candidate can utilize risk assessment methodologies and frameworks, such as OCTAVE, MEHARI, EBIOS, NIST, Harmonized TRA, and CRAMM

Competencies	Knowledge statements
1. Ability to understand and interpret OCTAVE methodologies: OCTAVE method, OCTAVE-S, and OCTAVE-Allegro 2. Ability to conduct information security risk assessment based on the OCTAVE Allegro methodology 3. Ability to analyze and manage risks based on the MEHARI method 4. Ability to understand and utilize EBIOS method for conducting risk assessments 5. Ability to identify NIST publications for risk management 6. Ability to understand and interpret the NIST risk management framework and utilize it in managing information security risks 7. Ability to understand and interpret CRAMM methodology for risk management 8. Ability to understand and explain how Harmonized Threat and Risk Assessment (TRA) method can be utilized for conducting risk assessment	1. Knowledge of the three phases of the OCTAVE method 2. Knowledge of the OCTAVE-S phases for conducting risk assessment 3. Knowledge of how OCTAVE-Allegro phases can be utilized to conduct an information security risk assessment 4. Knowledge of how information security risks can be analysed and managed using MEHARI 5. Knowledge of EBIOS risk assessment methodology and its five workshops and modules 6. Knowledge of the relationship between EBIOS and ISO/IEC 27005 7. Knowledge of the NIST publications for risk management 8. Knowledge of the seven steps of the NIST risk management framework 9. Knowledge of CRAMM risk analysis and management methodology and tool 10. Knowledge of the five phases of Harmonized Threat and Risk Assessment (TRA) methodology

Based on the abovementioned domains and their relevance, 80 questions are included in the exam, as summarized in the table below:

				Level of understanding (Cognitive/Taxonomy) required	
		Number of questions/points per competency domain	% of the exam devoted/points to/for each competency domain	Questions that measure comprehension, application, and analysis	Questions that measure synthesis and evaluation
Competency domains	Fundamental principles and concepts of information security risk management	13	16.25	X	
	Implementation of an information security risk management program	7	8.75	X	
	Information security risk assessment	20	25	X	
	Information security risk treatment	15	18.75		X
	Information security risk communication, monitoring, and improvement	10	12.5		X
	Information security risk assessment methodologies	15	18.75		X
	Total	**80**	**100%**		
	Number of questions per level of understanding			**40**	**40**
	% of the exam devoted to each level of understanding (cognitive/taxonomy)			**50%**	**50%**

The passing score of the exam 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 contains multiple-choice questions: This format has been chosen because it has proven to be effective and efficient for measuring and assessing learning outcomes related to the defined competency domains. The multiple-choice exam can be used to evaluate a candidate's understanding on many subjects, including both simple and complex concepts. When answering these questions, candidates will have to apply various principles, analyze problems, evaluate alternatives, combine several concepts or ideas, etc. The multiple-choice questions are scenario based, which means they are developed based on a scenario that candidates are asked to read and are expected to provide answers to one or more questions related to that scenario. This multiple-choice exam is "open book", due to the context-dependent characteristic of the questions. You will find a sample of exam questions provided below.

Since the exam is "open book," candidates are authorized to use the following reference materials:
- A hard copy of ISO/IEC 27005
- Training course materials (accessed through PECB Exams app and/or printed)
- Any personal notes during the training course (accessed through the 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. To learn if the exam is available 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.

Sample Exam Scenario-based Questions

Techonics is a technology company that specializes in computer software and consumer electronics. They conduct risk assessments regularly to ensure information security. Through its well-established information security risk management process, *Techonics* is able to identify potential risks associated with information assets and find solutions. Their risk management framework is based on ISO/IEC 27005 guidelines.

The last information security risk assessment process in *Techonics* took place last month. It was conducted by *Techonics*'s risk manager, Lana, and its results highlighted some new risks related to the password policy. Following *Techonics*'s risk management framework, the risk assessment process was initiated by a thorough analysis of the company and its objectives. Then, the basic criteria regarding risk management were defined.

Lana, conducted interviews with the key personnel. She found out that most of *Techonics*'s employees were aware that the password policy requires them to change their passwords once every three months. However, most of them did not follow the rule, as the system would not enforce it.

In addition, she found out that employees tend to use weak passwords, like their name and surname. Considering that weak passwords are easily guessed, this could become a serious concern for *Techonics*'s security. Lana identified several risk scenarios regarding the identified situation, from which two had a "high" level of occurring.

Sam, the information security manager, proposed the implementation of a cloud cross-platform password manager. The platform could be used by all employees to generate complex passwords and store them in a secured database. *Techonics* accepted his recommendation and started to use the platform so the risk related to weak passwords could be minimized. In addition, it was decided that Sam would organize information security training to educate the staff regarding the importance of password protection.

Based on the scenario above, answer the following questions:

1. ***Techonics* used ISO/IEC 27005 as a guideline for establishing its information security risk management framework. Is this acceptable?**
   A. No, ISO/IEC 27005 specifies the requirements for achieving information security through the implementation of an ISMS
   B. Yes, ISO/IEC 27005 is applicable to any type of risk, regardless of its nature or consequences
   C. **Yes, ISO/IEC 27005 provides guidance to assist organizations to perform information security risk management activities**

2. **Lana, the risk manager, found out that *Techonics*' employees did not change their passwords, as required by the password policy. Which step of risk identification has been performed in this case?**
   A. **Identification of vulnerabilities**
   B. Identification of threats
   C. Identification of risks

3. **Sam, the information security manager, proposed a solution for managing the risk associated with the password policy. How do you define this situation?**
   A. **Acceptable, the information security manager may identify and propose appropriate controls to manage risk**
   B. Unacceptable, the information security manager should not be involved in information security risk assessment activities
   C. Unacceptable, only the top management can propose and approve technical solutions for minimizing risk

4. **Which risk treatment option was proposed to treat the identified risks regarding the use of passwords?**
   A. Risk avoidance
   B. **Risk modification**
   C. Risk retention

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 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.

Exam Retake Policy

There is no limit to the number of times a candidate can retake an exam. However, there are certain limitations in terms of the allowed time span 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.

Exam Security

A significant component of a professional certification credential is maintaining the security and confidentiality of the exam. PECB relies upon the ethical behavior of certification holders and applicants to maintain the security and confidentiality of PECB exams. Any disclosure of information about the content of PECB exams is a direct violation of PECB's Code of Ethics. PECB will take action against any individuals that violate such rules and policies, including permanently banning individuals from pursuing PECB credentials and revoking any previous ones. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

Reschedule the Exam

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

Apply for Certification

All candidates who successfully pass the exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credentials they were examined for. Specific educational and professional requirements need to be fulfilled in order to obtain a PECB certification. Candidates are required to fill out the online certification application form (that can be accessed via their PECB online profile), including contact details of references who will be contacted to validate the candidate's professional experience. Candidates can submit their application in various languages. Candidates can choose to either pay online or be billed. For additional information, contact certification@pecb.com.

The online certification application process is very simple and takes only a few minutes, as follows:

- Register your account
- Check your email for the confirmation link
- Log in to apply for certification

For more information about the application process, follow the instructions on this manual Apply for Certification.

The application is approved as soon as the Certification Department validates that the candidate fulfills all the certification requirements regarding the respective credential. An email will be sent to the email address provided during the application process to communicate the application status. If approved, candidates will then be able to download the certification from their PECB Account.

PECB provides support in both English and French.

Renew your Certification

PECB certifications are valid for three years. To maintain them, candidates must demonstrate every year that they are still performing tasks that are related to the certification. PECB certified professionals must annually provide Continual Professional Development (CPD) credits and pay $100 as the Annual Maintenance Fee (AMF) to maintain the certification. For more information, please visit the Certification Maintenance page on the PECB website.

Closing a Case

If candidates do not apply for certification within three years, their case will be closed. Even though the certification period expires, candidates have the right to reopen their case. However, PECB will no longer be responsible for any changes regarding the conditions, standards, policies, and candidate handbook 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.

PECB

SECTION III: CERTIFICATION REQUIREMENTS

ISO/IEC 27005 Lead Risk Manager

The requirements for PECB ISO/IEC 27005 risk manager certifications are:

Credential	Exam	Professional experience	Risk management experience	Other requirements
PECB Certified ISO/IEC 27005 Provisional Risk Manager	PECB Certified ISO/IEC 27005 Lead Risk Manager exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27005 Risk Manager	PECB Certified ISO/IEC 27005 Lead Risk Manager exam or equivalent	Two years: One year of work experience in information security risk management	Information security risk management activities: a total of 200 hours	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27005 Lead Risk Manager	PECB Certified ISO/IEC 27005 Lead Risk Manager exam or equivalent	Five years: Two years of work experience in information security risk management	Information security risk management activities: a total of 300 hours	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27005 Senior Lead Risk Manager	PECB Certified ISO/IEC 27005 Lead Risk Manager exam or equivalent	Ten years: Seven years of work experience in information security risk management	Information security risk management activities: a total of 1,000 hours	Signing the PECB Code of Ethics

To be considered valid, the implementation activities should follow best implementation and management practices and include the following:

1. Defining a risk management approach
2. Determining the risk management objectives and scope
3. Performing risk assessment
4. Developing a risk management program
5. Defining risk evaluation and risk acceptance criteria
6. Evaluating risk treatment options
7. Monitoring and reviewing the risk management program

PECB

SECTION IV: CERTIFICATION RULES AND POLICIES

Professional References

For each application, two professional references are required. They must be from individuals who have worked with the candidate in a professional environment and can validate their information security risk management experience, as well as their current and previous work history. Professional references of persons who fall under the candidate's supervision or are their relatives are not valid.

Professional Experience

Candidates must provide complete and correct information regarding their professional experience, including job title(s), start and end date(s), job description(s), and more. Candidates are advised to summarize their previous or current assignments, providing sufficient details to describe the nature of the responsibilities for each job. More detailed information can be included in the résumé.

Risk Management Experience

The candidate's risk management project log will be checked to ensure that they have the required number of risk management hours.

Evaluation of Certification Applications

The Certification Department will evaluate each application to validate the candidate's eligibility for certification. A candidate whose application is being reviewed will be notified in writing and, if necessary, given a reasonable time frame to provide any additional documentation. If a candidate does not respond by the deadline or does not provide the required documentation within the given time frame, the Certification Department will validate the application based on the initial information provided, which can eventually lead to its downgrade to a lower credential.

Denial of Certification

PECB can deny certification if candidates:

- Falsify the application
- Violate the exam procedures
- Violate the PECB Code of Ethics
- Fail the exam

For more detailed information, refer to "Complaint and Appeal" section.

The application payment for the certification is non-refundable.

Suspension of Certification

PECB can temporarily suspend certification if the candidate fails to satisfy the requirements. Other reasons for suspending certification include:

- PECB receives large amounts of or serious complaints by interested parties (Suspension will be applied until the investigation has been completed.).
- The logos of PECB or accreditation bodies are intentionally misused.
- The candidate fails to correct the misuse of a certification mark within the time frame determined by PECB.
- The certified individual has voluntarily requested a suspension.
- PECB deems appropriate other conditions for suspension of certification.

Revocation of Certification

PECB can revoke certification if the candidate fails to fulfill the PECB requirements. Candidates are then no longer allowed to represent themselves as PECB certified professionals. Other reasons for revoking certification can be if candidates:

- Violate the PECB Code of Ethics
- Misrepresent and provide false information of the scope of the certification
- Break any other PECB rules

Upgrade of Credentials

Professionals can apply to upgrade to a higher credential as soon as they can demonstrate that they fulfill the requirements.

In order to apply for an upgrade, candidates need to login in to their PECB Account, visit the "My Certifications" tab, and click on the "Upgrade" link. The upgrade application fee is $100.

Downgrade of Credentials

A PECB Certification can be downgraded to a lower credential due to the following reasons:

- The AMF has not been paid.
- The CPD hours have not been submitted.
- Insufficient CPD hours have been submitted.
- Evidence on CPD hours has not been submitted upon request.

Note: *PECB certified professionals who hold Lead Certifications and fail to provide evidence of certification maintenance requirements will have their credentials downgraded. On the other hand, the holders of Master Certifications who fail to submit CPDs and pay AMFs will have their certifications revoked.*

Other Statuses

Besides being active, suspended, or revoked, a certification can be voluntarily withdrawn or designated as Emeritus. More information about these statuses and the permanent cessation status, and how to apply, please visit Certification Status Options.

SECTION V: PECB GENERAL POLICIES

PECB Code of Ethics

Adherence to the PECB Code of Ethics is a voluntary engagement. It is important that PECB certified professionals not only adhere to the principles of this Code, but also encourage and support the same from others. More information can be found here.

Other Exams and Certifications

PECB accepts certifications and exams from other recognized accredited certification bodies. PECB will evaluate the requests through its equivalence process to decide whether the respective certification(s) or exam(s) can be accepted as equivalent to the respective PECB certification (e.g., ISO/IEC 27001 Lead Auditor certification).

Non-discrimination and Special Accommodations

All candidate applications will be evaluated objectively, regardless of the candidate's age, gender, race, religion, nationality, or marital status.

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations for candidates, when appropriate. If candidates need special accommodations because of a disability or a specific physical condition, they should inform the Reseller/Distributor in order for them to make proper arrangements. Any information candidates provide regarding their disability/need will be treated with strict confidentiality.

Click here to download the Candidates with Disabilities Form.

Complaints and Appeals

Any complaints must be made no later than 30 days after receiving the certification decision. PECB will provide a written response to the candidate within 30 working days after receiving the complaint. If they do not find the response satisfactory, the candidate has the right to file an appeal. For more information about the complaints and appeal procedures, click here.

(1) According to ADA, the term "reasonable accommodation" may include: (A) making existing facilities used by employees readily accessible to and usable by individuals with disabilities; and (B) job restructuring, part-time or modified work schedules, reassignment to a vacant position, acquisition or modification of equipment or devices, appropriate adjustment or modifications of examinations, training materials or policies, the provision of qualified readers or interpreters, and other similar accommodations for individuals with disabilities.

(2) ADA Amendments Act of 2008 (P.L. 110-325) Sec. 12189. Examinations and courses. [Section 309]: Any person that offers examinations or courses related to applications, licensing, certification, or credentialing for secondary or post-secondary education, professional, or trade purposes shall offer such examinations or courses in a place and manner accessible to persons with disabilities or offer alternative accessible arrangements for such individuals.

Address:
Headquarters
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.

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