PECB

When Recognition Matters

Candidate's Handbook

ISO/IEC 27005 Lead Risk Manager

Table of Contents

About PECB

PECB is a certification body for persons, management systems, and products on a wide range of international standards. As a global provider of training, examination, audit, and certification services, PECB offers its expertise on multiple fields, including but not limited to Information Security, IT, Business Continuity, Service Management, Quality Management Systems, Risk & Management, Health, Safety, and Environment.

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

Our principal objectives and activities are:

1. Establishing the minimum requirements necessary to certify professionals, organizations and products.
2. Reviewing and verifying the qualifications of applicants for eligibility to be considered for the certification evaluation.
3. Developing and maintaining reliable, valid, and current certification examinations.
4. Granting certificates to qualified candidates, organizations and products, maintaining records, and publishing a directory of the holders of valid certificates.
5. Establishing requirements for the periodic renewal of certification and determining compliance with those requirements.
6. Ascertaining that our clients 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.

Value of PECB certification

Why choose PECB as your preferred certification body?

Global recognition
Selecting the right organization to offer the finest qualitative training and to carry out your certification can be a great challenge. However, by choosing a certification body that is accredited, such as PECB, proves that we comply with the best practices. Professionals who pursue a PECB certification credential will benefit from recognition in domestic and overseas markets. Being accredited by some of the toughest and most reputable accreditation bodies in the world gives us global recognition.

Competent personnel
PECB is acknowledged by technically competent people it comprises that have relevant sector experience. All our personnel hold professional credentials and are constantly trained and monitored to ensure more than satisfactory outcomes for our clients.

Compliance to standard
It is essential for a certification to prove compliance to a particular standard, to ensure the fulfillment of principles and requirements, consistency and impartiality of certification and audit of management systems services. PECB accredited certifications are evidence of severe compliance with Standards and their conditions, therefore reflecting safety, reliability and superior quality.

Reasonable fees
Being able to afford the most professional and recognizable certification services nowadays may be a struggle. By including both examination and certification processes into the training course fee, not only does PECB hold the lowest charging rate of professional training certification services, it also concludes with providing the lowest certification maintenance fees in the industry. Why not benefit from the opportunity of attaining accredited professional certifications that are globally recognized, fully comply with standards, and most importantly you can essentially meet the expense for?

PECB Certifications have proven to be effective instruments of confirmation for knowledge, skills and experience in a rapid changing community. By holding a PECB Certification, you will demonstrate that you have the necessary capabilities of shielding yourself and your organization against persistent, changing and undefined threats in a moderately challenging environment over a short period of time.

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 acting in accordance with the professional standards and applicable techniques while performing professional services.
3. Maintain competency in their respective fields and strive to constantly improve their professional skills.
4. Offer only professional services for which they are qualified to perform, and adequately inform clients and consumers about the nature of proposed services, including any relevant concerns or risks.
5. Inform each employer or client of any business interests or affiliations which might influence their judgment or impair their fairness.
6. Treat in confidential and private manner information acquired during professional and business dealings of any present or former employer or client without its proper consent.
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 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 for persons and will fully cooperate on the inquiry following a claimed infringement of this Code of Ethics.

Introduction

As both consumers and organizations are facing an increasing number of threats and attacks against their personal and financial data, information security has become more and more important for organizations of all size. Also, both consumers and legislators are expecting additional protection of this information from the organizations they deal with. The need for information security is greater than ever and is expected to constantly increase.

ISO/IEC 27005, part of the growing family of ISO/IEC 27000 series, is an information security standard published by the International Organization for Standardization (ISO) and the International Electro - Technical Commission (IEC). Its full title is ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management.
In 2011, ISO released a new version of the ISO/IEC 27005.

The purpose of ISO/IEC 27005 is to provide guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27005 and is designed to assist the satisfactory implementation of information security based on a risk management approach. It does not specify, recommend or even name any specific risk analysis method, although it does specify a structured, systematic and rigorous process from analyzing risks to creating the risk treatment plan.

Today's employers are not just seeking Information Security Risk Management professionals, but want proof that these professionals hold a predetermined set of knowledge and skills. Companies now place a high degree of importance on hiring, contracting with, and promoting credentialed practitioners prepared to tackle today and tomorrow's information security risks.

PECB is the only North American organization that certifies ISRM professionals. It is important to understand that PECB certifications are not a license or simply a membership. It is peer recognition that an individual has demonstrated proficiency in, and comprehension of, a series of competencies. PECB certifications are awarded to candidates that can provide proof of experience and have passed a standardized exam in the certification area.

This document specifies the PECB ISO/IEC 27005 certification schemes in compliance with the ISO/IEC 17024:2012 standard (Conformity assessment — General Requirements for bodies operating certification of persons). Also, this handbook contains information about the process by which candidates may earn and maintain their credentials. It is very important that you read all the information contained in this booklet before completing and submitting your application. If questions arise after reading this application handbook, please contact the PECB international office at certification@pecb.com.

Eric Lachapelle
Chief Executive Officer

Faton Aliu
President and Chief Operating Officer

PECB certification process steps

1. Decide which certification is right for you
Each PECB certification has specific education and experience requirements. To determine which certification product is right for you, you must verify all eligibility requirements for the different ISO/IEC 27005 certifications as well as your professional needs.

2. Prepare for the exam
All certification candidates are responsible for their own study and preparation for the examination. No specific set of courses or curriculum of study is required as part of the certification process. Likewise, the completion of a recognized PECB course or program of study will significantly enhance your chance of passing a PECB certification examination. You can verify the list of recognized organization that offers PECB official training sessions.

3. Apply and schedule the exam
Candidates shall contact one of our partners, who provide training courses and exam sessions worldwide. To find a training provider in your region, please check here https://pecb.com/partner/active_partners. Also, PECB training schedule is available here https://pecb.com/events.

4. Take the exam
Candidates will be required to arrive at least 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 examination room. All candidates will need to present a valid identity card (driver's license, or passport) to the invigilator and the exam confirmation letter. The duration of the exam varies according to the type of examination taken (see description of the different exams for more details).

Exam type:
Essay type "open book" exam, where the candidates are only authorized to use the following reference materials:

- A copy of the standard in paper hardcopy;
- Course notes from the Participant Handout;
- Any personal notes made by the student during the course;
- A hard copy dictionary.

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

5. Receive your exam results
It takes 6 to 8 weeks for participants to receive their results. All results are sent via email. The examination results will not include an exact numerical score (mark); rather the candidate will only be given a pass or fail status in their email. In the case of a failure, the results will be accompanied with the list of domains in which you had a mark lower than the passing grade to provide guidance to prepare yourself to retake the exam. Candidates, who disagree with the exam results, may file a complaint by writing to examination@pecb.com.

6. Apply for certification
All participants who successfully pass their certification exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credentials they were examined for. Specific educational and professional requirements may be needed for you to be PECB certified. Candidates will need 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.

Once PECB has validated that you fulfilled all certification requirements, you will be informed by e-mail of our decision.

The application payment for the certificate is not refundable.

This is due to the initiation of the procedures concerning the verification of the application, verification of the evidence submitted by the candidates, as well as the engagement of the relevant units in this process..

7. Maintain your certification

PECB certificates are valid for three years. In order to maintain a PECB certificate, it is required from the candidate to demonstrate that he/she is performing certification related activities on an annual basis. In addition, the candidate is required to pay an Annual Maintenance Fee (AMF). Every year, PECB certified professionals will need to provide PECB with the number of hours of auditing and/or implementation related tasks they have performed with the contact details of individuals who can validate these tasks, as well as paying their yearly certification maintenance fees. PECB will randomly select some referrals to contact to validate this experience and education.

ISO/IEC 27005 Lead Risk Manager

ISO/IEC 27005 Risk Manager credentials are professional certifications for candidates who intend to demonstrate the competence implement maintain and manage an information security risk management program in accordance with ISO/IEC 27005.

The principal competencies and knowledge skills needed in the market are the ability to support an organization in implementing and managing a risk management framework as specified in ISO/IEC 27005. The implementation of a risk management program includes risk identification, risk analysis, risk evaluation, risk treatment, acceptance of risk, and management of residual risks, communicating, monitoring and reviewing risk.

Various professions may apply for this certification:

- Information Security risk managers
- Information Security team members
- Individuals responsible for Information Security, compliance, and risk within an organization
- Individuals implementing ISO/IEC 27001, seeking to comply with ISO/IEC 27001 or individuals who are involved in a risk management program
- IT consultants
- IT professionals
- Information Security officers
- Privacy officers

The requirements for 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 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 Risk Manager Exam or equivalent	Two years: One year of work experience in ISRM	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 ISRM	Information Security Risk Management activities: a total of 300 hours	Signing the PECB Code of Ethics

If an applicant doesn't fulfil all the requirements to apply for the credential of ISO/IEC 27005 Lead Risk Manager, he/she may apply for the ISO/IEC 27005 Risk Manager or ISO/IEC 27005 Provisional Risk Manager credentials.

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

1. Defining a risk management approach
2. Determining the basic criteria, objectives, scope and boundaries
3. Identifying assets, threats, existing controls, vulnerabilities and consequences (impacts)
4. Assessing consequences and incident likelihood
5. Performing risk assessment
6. Designing and implementing an overall risk management process for an organization
7. Defining risk evaluation criteria
8. Evaluating risk treatment options
9. Determining the risk acceptance criteria
10. Selecting and implementing Information Security controls
11. Determining the risk communication plans and objectives
12. Performing risk management monitoring and reviews

General Information

Applying for certification

Candidates who apply for PECB certification will need to be prepared to provide the following:

- Fill in the online application form;
- Provide two reference details;
- Provide an updated CV

PECB will validate professional experience with your references to ensure the accuracy of all applications.

About application

Language

PECB provides support in English and French.

Application for certification fees

The application fee for certification is USD 500.

For all the candidates that have followed the training and the examination with one of the PECB's Partners, application fees include examination, application for certification and one year of Annual Maintenance Fee (AMF).

Examination cancellations
Please contact your partner for any changes regarding examination date, time, location, or other details.

About examination

Admission rules to examination
Each candidate must present valid photo identification to be admitted to the examination site and the exam confirmation letter. Candidates shall comply with all security rules established for testing. Candidates will be allowed no more than the specified time to complete their examination.

For more specific information about this exam, please contact examination@pecb.com to request a copy of the corresponding exam preparation guide, or download it from PECB's website

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 behavior of certificate holders and applicants to maintain the security and confidentiality of PECB examinations. When someone who holds PECB credentials reveal 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.

Exam tips
On the day of the exam:

1. Plan to arrive at the exam site at least 30 minutes prior to your appointment.
2. Get a good night's rest the night before.
3. Eat a well-balanced meal prior to reporting to the exam center. Avoid excessive stimulants such as caffeine.
4. Read and follow the instructions carefully. Ask the Proctor for clarification if you are not sure about the instructions.
5. Periodically check your progress. This will allow you to make any adjustments in time. Pay attention to the time you have left to finish the exam.
6. Only the questions you answer correctly are scored. There are no penalties for answering a question incorrectly, so answer as many questions as you can. If you are unsure of a response, eliminate as many options as possible, and choose an option from those that remain

Examination scores and scoring method
PECB grades all examinations fairly. There is no predetermined percentage of participants who fail and pass, so candidates do not compete against each other. Test scores are based on the number of items answered correctly.

Examination results
Scores are strictly confidential and they cannot be obtained over the phone or sent to a third-party. If you have questions concerning your test results, you should direct them in writing to examination@pecb.com. The examination results will not include the exact grade that you had in numbers or percentage, only a mention of pass or fail. In the case of a failure, the results will be accompanied with the list of domains in which you had failed to pass in order to provide guidance to prepare yourself to retake the exam.

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.

About certification

Professional references
Professional references must be from individuals who have professionally worked with you and can validate your Information Security Risk Management expertise, current and previous work history, as well as your job performance. You cannot use anyone as a reference who falls under your supervision nor is a relative. The candidate shall provide two professional references.

Professional experience
Complete information is required: including job title, begin dates, end dates, responsibilities and more. Summarize each assignment, providing sufficient detail to describe the nature of the responsibilities that you had. This information can be detailed in your resume.

Information Security Risk Management experience
The candidate's application and CV will be checked to ensure that the applicant has achieved the minimal required number of project-hours. The following risk assessment type constitute valid project experience: establishing an information security risk management framework, assessing the consequences of incident likelihood, determining the risk acceptance criteria, risk evaluation or risk management review. This information can be detailed in your resume.

Evaluation of certification applications
PECB randomly audits applications to validate the candidate's eligibility for certification. A candidate whose application is being audited will be notified in writing and given a reasonable timeframe to provide any additional documentation if required. If a candidate does not respond by the deadline, or does not provide the required documentation within the given timeframe, the application will be declared ineligible.

Denial and revocation of certification
Certification will be denied or revoked for any of the following reasons:

- Falsification of application
- Violation of testing procedures
- Misrepresentation
- Failure to pass the examination

Denials or revocations of certification may be appealed to the Certification Board in writing.

The application payment for the certificate is not refundable.

This is due to the initiation of the procedures concerning the verification of the application, verification of the evidence submitted by the candidates, as well as the engagement of the relevant units in this process.

Annual renewal certification fee
To keep your credentials active, there is an annual renewal fee for each calendar year. Candidates who pay their annual renewal fee will be considered valid in the PECB Directory of Certified Professional.

Recertification
In order to renew a PECB Certificate, candidates will need to demonstrate that they have maintained their certificate(s) on yearly basis. However, candidates are not required to fulfill the requirements every year, but they need to have performed a respective amount of activity hours within three years.

As an example, a professional who holds a Lead certificate performed 20 hours of certification-related professional activities in year 1, 10 hours of certification-related professional activities in year 2 and 60 hours of certification-related professional activities in year 3. Although during the first and second year the professional did not perform enough certification-related professional activities, his/her tri-annual total is equal to the minimal tri-annual requirements. So this professional would be re-certified.

For professionals such as university professors and professional trainers a requirement for experience can be fulfilled with their work experience on the subject.

PECB Certified Persons who fail to provide evidence of certification maintenance requirements will have their PECB credentials downgraded. The holders of Master certificates who fail to submit their CPD and AMF will have their Master credentials revoked and will no longer be allowed to present themselves as certified PECB professionals.

Downgrade of credential
A credential of Lead Implementer, Implementer, Lead Auditor, and Auditor will be downgraded to Provisional if the following requirements are not meet:

• Continuing Professional Development (CPD) credits not submitted,
• Annual Maintenance Fee (AMF) not paid,

• Breach of PECB's Code of Ethics

About PECB general policies

PECB Code of Ethics
The PECB Code of Ethics can be found at www.PECB.com. Adherence of professionals to PECB code of ethics is a voluntary engagement. However, if a member does not follow this code by engaging in gross misconduct, PECB membership may be terminated and certifications revoked. Not only is it important for PECB certified professionals to adhere to the principles expressed in this Code, each member should encourage and support adherence by other members.

Other exams and certifications:
PECB has reviewed and validated the organizations below and certifications as equivalent in competency domains, difficulty and content coverage.

Planned equivalencies include only the following:

1. The applicant has successfully been certified to a certification that is considered to be equivalent. Whenever someone applied for such an equivalencies, the certification will have to be evaluated by PECB staff to determine if it is a valid equivalency or not. If it is deemed to be, the name of this certification will be added to PECB's documentation and website as a valid equivalent.

2. The applicant has successfully passed an examination that is considered to be equivalent. These may be ISO/IEC 27005 Lead Risk Manager examinations provided by organizations certified by recognized accredited certification bodies

Whenever someone applies for such an equivalencies, the application for certification will have to be evaluated by PECB staff to determine if it is a valid equivalency or not. If it is deemed to be, the name of this certification will be added to PECB's documentation and website as a valid equivalent.

Non-discrimination and Special Accommodations
All candidate applications shall be evaluated objectively without regard to age, sex, race, religion, national origin, or marital status. PECB will allow for reasonable accommodations [1] as required by the Americans with Disabilities Act (ADA) [2] or an equivalent National Law. A candidate who needs special accommodations must make the request in writing and allow an extra two weeks for processing of the application. Click here to download Special Accommodations for Candidates with Disabilities Form

Complaints and appeals
Requests for an appeal must be made no later than 30 days after the applicant is denied certification. Within 30 days after the receipt of the written appeal, PECB must provide the applicant with a written response. You can read more about complaint and appeal procedure by visiting the following link: https://pecb.com/complaint-and-appeal-procedure.

(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
(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 postsecondary 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:
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

Website: www.pecb.com