When Recognition Matters

Candidate's Handbook

ISO/IEC 27034 LEAD AUDITOR

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 to show commitment and competence with internationally recognized standards by providing this assurance through the education, evaluation and certification against rigorous, internationally recognized competence requirements. 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.

Values 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

ISO/IEC 27034:2011 provides guidance to assist organizations in integrating security into the processes used for managing their applications.

ISO/IEC 27034 is applicable to in-house developed applications, applications acquired from third parties, and where the development or operation of the application is outsourced.

ISO/IEC 27034 offers guidance on information security to those specifying, designing/programming or procuring, implementing and using application systems, in other words business and IT managers, developers and auditors, and ultimately the end-users of application systems. The aim is to ensure that computer applications deliver the desired/necessary level of security in support of the organization's Application Security Management System.

The multi-part standard provides guidance on specifying, designing/selecting and implementing information security controls through a set of processes integrated throughout an organization's Lifecycle/s.
It is Process-oriented. It covers software applications developed internally, by external acquisition, outsourcing/offshoring or through hybrid approaches, and it addresses all aspects from determining information security requirements, to protecting information accessed by an application, as well as preventing unauthorized use and/or actions of an application.

Benefits:

- Ensuring access to information is appropriately authorized
- Safeguarding the accuracy and completeness of information and processing methods
- Ensuring that authorized users have access to information when they need it

Today's employers are not only seeking Service Management professionals, but also want proof that these professionals hold a predetermined set of knowledge and skills. Companies now consider a high degree of importance on hiring, contracting with, and promoting credentialed practitioners prepared to tackle today and tomorrow's Service challenges.

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, professional references and have passed a standardized exam in the certification area.

This document specifies the PECB ISO/IEC 27034 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, verify all eligibility requirements for the different ISO/IEC 27034 certifications and 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 course or program of study will significantly enhance your chance of passing a PECB certification examination. To learn more about exams, competency domains and knowledge statements please go to: https://pecb.com/examination.

3. Apply and schedule the exam

Candidates shall contact one of our partners, who provide training courses and exam sessions worldwide. To find training provider in your region, 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 such as a national ID card or driver's license 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). Thirty (30) minutes of additional time can be provided to candidates taking the exam in a language different than their mother tongue, when requested by the candidates, on the exam day.

There are two exam types:

- Multiple choice "closed book" exam, where the candidates are not authorized to use anything but the exam paper and a pen/pencil or,
- 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 4 to 8 weeks for participants to receive their results. All results are sent via email. The examination results will not include the exact grade 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 in order 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 online certification application form http://pecb.com/user/register, and fill out all the forms online (that can be accessed via their PECB online profile), including contact details of references who will be contacted to validate the candidates' professional experience. At the end before the submission, a candidate can choose to pay online or be billed. In case the candidate needs additional information, he/she should contact accounting@pecb.com and/or certification@pecb.com .

The validation of the application occurs as soon as the Certification Department estimates that you fulfil all the certification requirements regarding the credential you have applied for. In this occasion, an email will be sent to your email address which you provided during your application process. You will then be able to download your certificate from your member account.

7. Maintain your certification

The PECB certifications are valid for three years. To maintain the certification, the applicant shall demonstrate every year that he/she is still performing tasks that are related to the certification. 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 pay their yearly certification maintenance fees. A notification email is sent to our certified members, who are required to submit their CPD along with AMF a month before the annual date of their certification. The PECB certified members will then be able to submit their CPDs by visiting their account, and next to their certificates, there will be a CPD link displayed which they need to click and provide the required information.

ISO/IEC 27034 Lead Auditor

The ISO/IEC 27034 Auditor certifications are credentials for professionals needing to audit an Information technology – Security techniques – Application Security and, in case of the "ISO/IEC 27034 Lead Auditor" Certification, able to manage a team of auditors.

The principal competencies and knowledge skills needed by the market are the ability to proficiently plan and perform audits compliant with the certification process of the ISO/IEC 27034:2011 standard and to master the audit techniques and to manage (or be part of) audit teams and audit program.

Various professions may apply for this certification:

- Internal auditors.
- Auditors wanting to perform and lead IT - Security techniques – Application Security audit.
- Project managers or consultants who want to master the IT - Security techniques – Application Security audit process.
- CxO and senior managers responsible for the IT governance of an enterprise and the management of its risks.
- Members of an information security team.
- Expert advisors in Information Technology.
- Technical experts wanting to prepare for Application Security audit function.

The requirements for ISO 27034 Lead Auditor certification are:

Credential	Exam	Professional experience	MS audit/ assessment experience	Other requirements
PECB Certified ISO/IEC 27034 Lead Auditor	PECB Certified ISO/IEC 27034 Lead Auditor exam or equivalent	**Five years:** Two years of AS work experience	Audit activities totalling 300 hours	Signing the PECB code of ethics

For certification purposes, the following audit types constitute valid audit experience:

If an applicant doesn't have all requirements to apply for the credentials of ISO/IEC 27034 Lead Auditor he/she may apply for the credentials of ISO/IEC 27034 Auditor or ISO/IEC 27034 Provisional auditor.

1. Pre-assessment/pre-audit
2. Gap analysis
3. Internal audits
4. Second party audits
5. Third party/external audits
6. Opinion audit

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

1. Audit planning
2. Audit interview
3. Managing an audit program
4. Drafting audit reports
5. Drafting non-conformity reports
6. Drafting audit working documents
7. Documentation review
8. On-Site Audit
9. Non-conformity follow-up actions
10. Leading a team of auditors

General information

Applying for certification

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

- Two references, including their names and contact details.
- Their most recent CV.
- Their AS audit/project log.

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. A retake fee applies.
Only students, who have completed the full training but fail the written exam, are eligible to retake the exam for free, under one condition:
"A student can only retake an exam once and this retake must occur within 12 months from the initial exam's date." When candidates fail the same examination for the second time, their file is automatically closed for 1 year.

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 reference contacts shall be the individuals who have professionally worked with you and can validate your Service expertise, current and previous work history, as well as your job performance. You cannot use anyone as a reference who falls under your supervision, or who is a relative. The candidates shall provide two references for each certification application.

Professional experience
Complete information is required: including job title, commence and end dates, job description and more. Summarize each assignment, providing sufficient details to describe the nature of the responsibilities that you have had. The detailed information is advised to be included in the resume.

AS Audit experience
The candidate's audit log will be checked to ensure that the applicant has the required number of audit-hours. The following audit types constitute valid audit experience: pre-assessment/pre-audit, gap analysis, internal audits, second party audits, third/external audits or opinion audit. This information can be detailed in your resume.

AS project experience
The candidate's implementation log will be checked to ensure that the applicant has the required number of implementation-hours. The following implementation types constitute valid implementation experience: internal implementation, external/consulting implementation or partial implementation of an AS. This information can be detailed in your resume.

Evaluation of Certification Applications
Certification Department will evaluate each application with purpose to validate the candidate's eligibility to certification. A candidate whose application is being reviewed will be notified in writing office 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 time frame, he/she may 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 maintain your credentials active, there is an annual renewal fee for each calendar year. Registrants who pay their annual renewal fee will appear online in the PECB Directory of Certified Professional.

Recertification
The PECB designations are valid for three years. To maintain his/her certification, the applicant must demonstrate every year that he/she is still performing tasks that are related to the certification. Three months before expiration date of the certification, the certified member will be informed via email that he/she can submit their final CPD information along with AMF and a renew link will be displayed on his/her dashboard, next to his/her specific certificate. PECB certified professional who fails to provide the required CPD hours will have his/her PECB credentials downgraded. To find out more about Certification maintenance and re-certification process, please visit: https://pecb.com/certification-maintenance.

Upgrade of credentials
Professional can apply for a higher credential as soon as they can document that they fulfill the requirements. In order to apply for upgrade the certified members are advised to visit their dashboard and click upgrade link, which is located next to their certificates.
As an example, a professional that has been certified as ISO 27034 Auditor within a year makes additional 100 hours (200 are the minimum for Certified Auditor) and he/she already has 5 years of work experience, two of which related to AS, he/she can apply to be upgraded to ISO 27034 Lead Auditor certified member.

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. 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 27034 examinations provided by organizations certified by recognized accredited certification bodies. An example of these would be certified ISO/IEC 27034 courses provided by BSI, or any other accredited provider.

Whenever someone applies for such 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

United Kingdom
6 George Street, Driffield,
East Riding of Yorkshire,
YO25 6RA,
United Kingdom

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

Copyright © 2016 PECB. Reproduction or storage in any form for any purpose is not permitted without a PECB prior written permission. No other right or permission is granted with respect to this work. All rights reserved.