

Candidate Handbook

ISO/IEC 27001 LEAD AUDITOR



TABLE OF CONTENTS

ABOUT PECB	3
VALUE OF PECB CERTIFICATION	4
Why Choose PECB as Your Certification Body?	4
PECB CODE OF ETHICS	5
INTRODUCTION.....	6
PECB CERTIFICATION PROCESS STEPS.....	7
1. Decide which certification is right for you	7
2. Prepare for the exam	7
3. Apply and schedule the exam.....	7
4. Take the exam	7
5. Receive your exam results.....	7
6. Apply for certification.....	8
7. Maintain your certification.....	8
ISO/IEC 27001 LEAD AUDITOR	9
GENERAL INFORMATION	11
Applying for Certification	11
About Application.....	11
ABOUT EXAMINATION	12
ABOUT CERTIFICATION.....	14
ABOUT PECB GENERAL POLICIES.....	16

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, Information Technology, Business Continuity, Service Management, Quality Management, 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 internationally recognized standards. Our mission is to provide our clients with comprehensive services that inspire trust, demonstrate recognition, and benefit the society as a whole.

The principal objectives of PECB include:

1. Establishing the minimum requirements necessary to certify professionals, organizations, and products
2. Reviewing and verifying the qualifications of candidates to ensure that they are eligible to apply for a PECB certificate
3. Developing and maintaining reliable, valid, and current PECB certificate application processes
4. Granting certificates to qualified candidates, organizations, and products; maintaining records; and publishing a directory of the candidate who hold valid PECB certificates
5. Establishing requirements for the periodic renewal of PECB certificates and ensuring compliance with those requirements
6. Ascertaining that certified individuals meet ethical standards and adhere to the PECB Code of Ethics
7. Promoting the benefits of certification for organizations, employers, public officials, practitioners in related fields, and the public

VALUE OF PECB CERTIFICATION

Why Choose PECB as Your Certification Body?

Global Recognition

Selecting the right certification body that offers qualitative and credible training and certification services can be challenging. However, by choosing an accredited certification body such as PECB proves that you are compliant with best practices, up to date, and trustworthy.

Individuals who obtain a PECB certificate will benefit from the recognition in domestic and overseas markets. Being accredited by some of the most reputable accreditation bodies in the world gives us global recognition.

Competent Personnel

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

Compliance with Standards

Certification is proof of compliance with a particular standard. It proves that the standard requirements have been fulfilled and validated with adequate consistency, professionalism, and impartiality. PECB certifications are evidence of compliance with standards and their requirements, therefore reflecting safety, reliability, and superior quality.

Reasonable Fees

Apart from being the lowest charging organization for professional training and certification services, including both the examination and certification processes, PECB also charges the lowest certification maintenance fees in the industry.

Why not benefit from the opportunity of attaining accredited professional certifications that are globally recognized, fully compliant with standards, and affordable? PECB certifications have proven to be effective instruments for the validation of knowledge, skills, and experience in a rapidly changing economy. By holding a PECB certification, you will demonstrate that you have the necessary capabilities to safeguard 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 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 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 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: <https://pecb.com/en/pecb-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 all the organizations regardless of their size and complexity. Also, both consumers and legislators are expecting additional protection of information from the organizations they deal with. The need for information security is greater than ever and is expected to constantly increase.

To answer these issues, the International Organization for Standardization (ISO) jointly with the International Electro technical Commission (IEC) has developed the ISO/IEC 27001:2013 standard for information security. ISO/IEC 27001:2013 provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS).

Since 2005, when the first ISO/IEC 27001 certification for an organization was granted, there is a lack of available qualified and certified ISMS professionals. Today's employers are not just seeking information security 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 certified security practitioners prepared to tackle today's and tomorrow's security challenges.

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 competences. 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 27001 certification scheme in compliance with ISO/IEC 17024:2012 (Conformity assessment – General requirements for bodies operating certification of persons). 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 questions arise after reading this candidate handbook, please contact the PECB international office at certification@pecb.com.

PECB CERTIFICATION PROCESS STEPS

1. Decide which certification is right for you

Each PECB certification has specific education and professional experience requirements. To determine which credential is right for you, verify the eligibility criteria for the various ISO/IEC 27001 certifications and your professional needs.

2. Prepare for the exam

All candidates are responsible for their own study and preparation for the exam. No specific set of training courses or curriculum of study is required as part of the certification process. Likewise, the completion of a training course will significantly enhance your chance of successfully passing a PECB exam. To learn more about exams, competency domains, and knowledge statements, please go to: [Exam Preparation Guides](#).

3. Apply and schedule the exam

To schedule an exam:

- a) Candidates can contact one of our resellers who provide training courses and exam sessions. To find a training course provider in your region, please follow this link: https://pecb.com/reseller/active_resellers. The PECB training course schedule is also available here: <https://pecb.com/events>.
- b) Candidates can also take a PECB exam remotely at the convenience of their own home through the PECB Exam application, which can be accessed here: <https://pecb.com/en/eventExamList/schedule>

4. Take the exam

Candidates will be required to arrive at least 30 minutes before the exam starts. Candidates arriving late will not be given additional time to compensate for the late arrival and may be denied entry to the exam. All candidates are required to present a valid identity card such as the national ID card, the driver's license, or the passport to the invigilator. The duration of the exam varies depending on the type of the exam (find below the description of the different exam types for more details). Additional time can be given to candidates taking the exam in a language other than their first language (if requested by the candidates on the exam day).

Exam type:

In essay type exams, also known as "open book" exams, the candidates are authorized to use the following reference materials:

- A copy of the ISO/IEC 27001 standard
- Any personal notes made by the candidate during the training course session
- A hard copy dictionary

For more information about exam details, please visit [Examination Rules and Policies](#).

5. Receive your exam results

Results will be communicated via email within a period of six to eight weeks from the exam date. The candidate will be provided with only two possible exam results: pass or fail, rather than an exact grade.

In case of exam failure, the results will be accompanied with the list of domains in which the candidate has failed to fully answer the question(s). This can help the candidate better prepare for a retake exam. Candidates who disagree with the exam results may file a complaint by writing to examination@pecb.com.

6. 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 <https://pecb.com/en/user/checkEmail>, and fill out all other online forms (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. Lastly, before submitting the application, the candidate can choose to pay online or be billed. For additional information, the candidate can contact accounting@pecb.com or certification@pecb.com.

The approval of the application occurs as soon as the Certification Department validates that the candidate fulfils all the certification requirements regarding the respective credential. An email will be sent to the email address you provided during your application process to communicate your application status. If approved, the candidate will then be able to download the certificate from their PECB Account.

7. Maintain your certification

PECB certifications are valid for three years. To maintain the certification, the candidates shall demonstrate every year that they are still performing tasks that are related to the certification. PECB certified professionals shall annually provide PECB with the number of hours of auditing that they have performed, along with the contact details of individuals who can validate the accomplishment of such tasks. Additionally, certified professionals should regularly pay the fee for the annual maintenance of their certification.

A notification email is sent to the certified members, who are required to submit their Continuing Professional Development (CPD) hours along with the Annual Maintenance Fee (AMF) three months before the annual date of their certification. The PECB certified members will then be able to submit their CPD hours by visiting their account and providing the required information for the respective certification.

ISO/IEC 27001 LEAD AUDITOR

The “ISO/IEC 27001 Lead Auditor” credential is a professional certification for individuals aiming to demonstrate the competence to audit the information security management system and lead an audit team.

The most important skills required in the market are the ability to effectively plan and perform audits in conformance with the certification process of ISO/IEC 27001, master audit techniques, and manage (or be part of) audit teams and audit programs.

The ISO/IEC 27001 Lead Auditor certification is intended for:

- Auditors seeking to perform and lead information security management system (ISMS) audits
- Managers or consultants seeking to master the information security management system audit process
- Individuals responsible to maintain conformity with the ISMS requirements in an organization
- Technical experts seeking to prepare for the information security management system audit
- Expert advisors in information security management

The certification requirements are:

Credential	Exam	Professional experience	MS audit/assessment experience	Other requirements
PECB Certified ISO/IEC 27001 Provisional Auditor	PECB Certified ISO/IEC 27001 Lead Auditor Exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27001 Auditor	PECB Certified ISO/IEC 27001 Lead Auditor Exam or equivalent	Two years: One year of work experience in Information Security Management	Audit activities: a total of 200 hours	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27001 Lead Auditor	PECB Certified ISO/IEC 27001 Lead Auditor Exam or equivalent	Five years: Two years of work experience in Information Security Management	Audit activities: a total of 300 hours	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27001 Senior Lead Auditor	PECB Certified ISO/IEC 27001 Lead Auditor Exam or equivalent	Ten years: Seven years of work experience in Information Security Management	Audit activities: a total of 1,000 hours	Signing the PECB Code of Ethics

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

1. Planning an audit
2. Managing an audit program
3. Drafting audit reports
4. Drafting nonconformity reports
5. Drafting audit working documents
6. Documented information review
7. On-site audit
8. Following up on nonconformities
9. Leading an audit team

GENERAL INFORMATION

Applying for Certification

Candidates who apply for the PECB certificate will need to provide the following:

- Two references, including their names and contact details
- Their most recent CV
- Their information security audit log

PECB will validate a candidate's professional experience with the references to ensure the accuracy of the application.

About Application

Language

PECB provides support in both English and French languages.

Application Fees for Certification

The application fee for certification is \$500.

For all the candidates that have followed the training course and 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.

Exam Cancellations

Please contact your reseller for any changes regarding the exam date, time, location, or other details.

ABOUT EXAMINATION

Admission Rules to Examination

Candidates shall comply with all the security rules established for the 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 the PECB website: <https://pecb.com/en/exam-preparation-guides>.

Examination Security

A significant component of a successful and respected professional certification credential is maintaining the security and confidentiality of the exam. PECB relies upon the ethical behaviour of certificate holders and applicants to maintain the security and confidentiality of PECB exams. If candidates or someone who holds PECB credentials reveal information about PECB exam 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 and avoid excessive stimulants such as caffeine
4. Read and follow the instructions carefully; ask the invigilator 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.) and pay attention to the remaining time to finish the exam
6. Your exam score will be determined by the number of questions you answer correctly. You will not be deducted any points from incorrect answers, therefore try answering every question.

Exam Scores and Scoring Method

PECB evaluates all applications fairly. PECB does not impose limitations on the number of candidates that will pass. Exam scores are based on the number of questions answered correctly.

Exam Results

Scores are strictly confidential and they cannot be obtained over the phone or sent to a third party. If you have any questions concerning your exam results, you should direct them in writing to examination@pecb.com.

Exam Retake Policy

There is no limit on the number of times a candidate may retake an exam. However, there are some limitations in terms of the allowed time frame in between exam retakes, such as:

- If a candidate does not pass the exam on the first attempt, the candidate must wait 15 days (from the initial date of the exam) for the next attempt (first retake). The retake fee applies.

PECB

Note: Candidates who have completed the full training course 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, the candidate must wait three months (from the initial date of the exam) for the next attempt (second retake). The retake fee applies.
- If a candidate does not pass the exam on the third attempt, the candidate must wait six months (from the initial date of the exam) for the next attempt (third retake). The retake fee applies.
- After the fourth attempt, a waiting period of 12 months from the last session date is required, in order for the candidate to retake the same exam. The regular fee applies.

For the candidates that fail the exam in the second retake, PECB recommends to attend an official training course in order to be better prepared for the exam.

To arrange exam retakes (date, time, place, and costs), the candidate needs to contact the PECB reseller who has initially organized the training course session.

Closing a Case

If a candidate does not apply for the certificate within three years, their case will be closed. Even though the certification period expires, the candidate has the right to reopen their case. However, PECB will no longer be responsible for any changes regarding the conditions, standards, policies, candidate handbook or exam preparation guide that were applicable before the case was closed. A candidate requesting their case to reopen must do so in writing, and pay the required fees.

ABOUT CERTIFICATION

Professional References

For each certification application, two professional references are required. Professional references shall be the individuals who have worked with you in a professional environment and can validate your information security audit experience, current, and previous work history. You cannot use as a professional reference the persons who fall under your supervision or are a relative of yours.

Professional Experience

Candidates shall provide complete information regarding their professional experience, including job title(s), commencement 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 that they have had. More detailed information can be included in the résumé.

ISMS Audit Experience

The candidate's audit log will be checked to ensure that the candidate has the required number of audit hours. The following audit types constitute valid audit experience: pre-audit, gap analysis, internal audits, second party audits, third party audits, or opinion audits.

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 given a reasonable time frame to provide any additional documentation if necessary. 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 the downgrade of it 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

Any concerns regarding the denial of certification can be appealed in writing to the Certification Board.

The application payment for the certificate is non-refundable. This is because of the process of verifying the application, verifying the evidence submitted by the candidates, and verifying the engagement of the relevant units in this process.

Suspension of Certification

PECB can temporarily suspend certification if the candidate fails to satisfy the requirements of PECB. Additional reasons for suspending certification can be if:

- PECB receives excessive or serious complaints by interested parties (Suspension will be applied until the investigation has been completed.).
- The logos of PECB or Accreditation Bodies are wilfully misused.
- The candidate fails to correct the misuse of a certification mark within the determined time by PECB.

PECB

- The certified individual has voluntarily requested a suspension.
- PECB deems appropriate other conditions for suspension of certification.

Revocation of Certification

PECB can revoke (that is, to withdraw) certification if the candidate fails to satisfy the PECB requirements. Candidates are then no longer allowed to represent themselves as PECB certified professionals. Additional reasons for revoking certification can be if candidates:

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

Annual Maintenance Fee for Certification

To maintain their credentials, candidates should pay the Annual Maintenance Fee (AMF) every year. Only the candidates who pay the AMF will appear online in the PECB Directory of Certified Professional.

Recertification

PECB certificates are valid for three years. In order to maintain a certificate, candidates are required to provide evidence that they are performing activities related to the respective certification on an annual basis. In addition, candidates are also required to pay the Annual Maintenance Fee (AMF).

After successfully maintaining a PECB certificate for three years, candidates can then apply for a renewal of their certificate.

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

To find out more about the Recertification process, please visit:

<https://pecb.com/en/certification-maintenance>.

Upgrade of Credentials

Professionals can apply to upgrade to a higher credential as soon as they can prove that they fulfil the requirements.

In order to apply for an upgrade, please log in to your PECB Account, visit the “My Certifications” tab, and click on the “Upgrade” link. The upgrade application fee is \$100.

For example, if an individual has been certified as an ISO/IEC 27001 Auditor and has five years of work experience, two of which are related to the ISMS audit, and a total of 200 hours of information security audit activities, and within a year the person makes an additional 100 hours, adding up to a total of 300 hours of information security audit activities, the professional can apply to be upgraded to ISO/IEC 27001 Lead Auditor.

ABOUT PECB GENERAL POLICIES

PECB Code of Ethics

You can find the PECB Code of Ethics at: <https://pecb.com/en/pecb-code-of-ethics>. Adherence to the 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 of this Code, but also each member should encourage and support adherence by other members.

Other Exams and Certifications

PECB does accept certifications and exams provided 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 certificate (e.g., ISO/IEC 27001 Lead Auditor certificate).

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 accommodation ⁽¹⁾ as required by the Americans with Disabilities Act (ADA) ⁽²⁾ or an equivalent National Law. A candidate who needs special accommodation must make the request in writing and allow an extra two weeks for the processing of the application. Click here to download [Special Accommodations for Candidates with Disabilities Form](#). 

Complaints and Appeals

Any complaint that a candidate has must be made no later than 30 days after their certification has been denied. Within 30 working days after receiving the complaint, PECB will provide a written response to the candidate. Should the response from PECB not be satisfactory, the candidate has the right to file an appeal. You can read more about the complaint and appeal procedures by visiting the following link: <https://pecb.com/en/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 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. Visit Help Center here: www.pecb.com/help

Emails:

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

Copyright © 2019 PECB. Reproduction or storage in any form for any purpose is not permitted without a PECB prior written permission.

www.pecb.com