PECB BEYOND RECOGNITION

Candidate Handbook

ISO/IEC 27001 LEAD IMPLEMENTER

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 applicant 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

This certification is internationally recognized and accredited under ISO/IEC 17024 – Requirements for bodies operating certification of persons, by the International Accreditation Service (IAS), and by the United Kingdom Accreditation Service (UKAS); signatories 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 27001 Lead Implementer

ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). The most important skills required in the market are the ability to effectively implement and manage the ISMS, assess and treat the information security risks, and manage (or be part of) ISMS implementation teams.

The "ISO/IEC 27001 Lead Implementer" credential is a professional certification for individuals aiming to demonstrate the competence to implement the information security management system and lead an ISMS implementation team.

Considering that implementing is one of the most in-demand professions, an internationally recognized certification can help you exploit your career potential and 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 competences. 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 27001 Lead Implementer 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 ISO/IEC 27001 Lead Implementer" exam is to ensure that the candidate has acquired the knowledge to support an organization in effectively planning, implementing, managing, monitoring, and maintaining the information security management system (ISMS).

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

- Managers or consultants involved in and concerned with the implementation of an information security management system in an organization
- Individuals responsible for maintaining conformity with the information security requirements in an organization
- Members of an ISMS implementation team

The exam covers the following competency domain:

- **Domain 1:** Fundamental principles and concepts of an information security management system (ISMS)
- **Domain 2:** Information security management system (ISMS)
- **Domain 3:** Planning an ISMS implementation based on ISO/IEC 27001
- **Domain 4:** Implementing an ISMS based on ISO/IEC 27001
- **Domain 5:** Monitoring and measurement of an ISMS based on ISO/IEC 27001
- **Domain 6:** Continual improvement of an ISMS based on ISO/IEC 27001
- **Domain 7:** Preparing for an ISMS certification audit

Domain 1: Fundamental principles and concepts of an information security management system (ISMS)

Main objective: Ensure that the candidate understands and is able to interpret ISO/IEC 27001 principles and concepts

Competencies	Knowledge statements
1. Ability to understand and explain the main concepts of information security 2. Ability to explain the difference and relationship between information and asset 3. Ability to understand the difference between documents, specifications, and records 4. Ability to understand the relationship between the concepts of vulnerability, threat, risk, and their impact 5. Ability to understand the concept of confidentiality, integrity, and availability of information 6. Ability to understand and interpret the classification of security controls and their objectives 7. Ability to understand the relationship between assets, risks, threats, vulnerabilities, and controls	1. Knowledge of the information security laws, regulations, international and industry standards, contracts, market practices, internal policies, best practices, etc., an organization must comply with 2. Knowledge of the main concepts and terminology of ISO/IEC 27001 3. Knowledge of information security risk and its importance in an ISMS 4. Knowledge of confidentiality, integrity, and availability of information 5. Knowledge of information security vulnerabilities, threats, and risks 6. Knowledge of the difference and characteristics of security objectives 7. Knowledge of the difference between security control types and their function

PECB

Domain 2: Information security management system (ISMS) **Main objective:** Ensure that the candidate understands and is able to implement the security controls listed in Annex A of ISO/IEC 27001	
Competencies	**Knowledge statements**
1. Ability to select, design, and describe information security controls 2. Ability to define the organization's security architecture 3. Ability to identify and illustrate the activities involved in developing and deploying information systems 4. Ability to understand, interpret, and analyze Annex A controls of ISO/IEC 27001 5. Ability to implement Annex A controls based on ISO/IEC 27001 and best practices	1. Knowledge of common security services such as access control services, integrity services, and cryptographic services 2. Knowledge of common architecture frameworks 3. Knowledge of the Annex A controls of ISO/IEC 27001

PECB

Domain 3: Planning an ISMS implementation based on ISO/IEC 27001 **Main objective:** Ensure that the candidate is able to plan the implementation of the ISMS based on ISO/IEC 27001	
Competencies	**Knowledge statements**
1. Ability to collect, analyze, and interpret the information required to plan an ISMS implementation 2. Ability to understand and set information security and ISMS objectives 3. Ability to identify and interpret ISMS risks and their impacts 4. Ability to analyze and consider the internal and external context of an organization 5. Ability to identify the resources required for the ISMS implementation 6. Ability to manage, estimate, and monitor the required resources for the ISMS implementation 7. Ability to identify the roles and responsibilities of key interested parties during and after the implementation and operation of an ISMS 8. Ability to draft, file, and review an ISMS project plan 9. Ability to perform a gap analysis and clarify the information security management objectives 10. Ability to define and justify an ISMS scope adapted to the organization's specific information security objectives 11. Ability to develop and establish an ISMS policy 12. Ability to perform the different steps of the risk assessment process 13. Ability to understand and draft the Statement of Applicability document	1. Knowledge of the main project management concepts, terminology, processes, and best practices 2. Knowledge of the principal approaches and methodology used to implement an ISMS 3. Knowledge of typical information security and ISMS objectives and how to achieve specific results 4. Knowledge of what typically constitutes an organization's internal and external context 5. Knowledge of the approaches used to understand the context of an organization 6. Knowledge of the techniques used to gather information on an organization and to perform a gap analysis of a management system 7. Knowledge of an ISMS project plan and a ISMS project team 8. Knowledge of the resources required for an ISMS implementation 9. Knowledge of the main organizational structures applicable for an organization to manage an ISMS 10. Knowledge of the characteristics of an ISMS scope in terms of organizational, technological, and physical boundaries 11. Knowledge of the best practices and techniques used to draft and establish information security policies and procedures 12. Knowledge of the different approaches and methodologies used to perform the risk assessment process 13. Knowledge of the characteristics of the Statement of Applicability document

PECB

Domain 4: Implementing an ISMS based on ISO/IEC 27001 **Main objective:** Ensure that the candidate is able to implement an ISMS based on the requirements of ISO/IEC 27001	
Competencies	**Knowledge statements**
1. Ability to manage capacity building processes for the successful implementation of an ISMS 2. Ability to define the documentation and record management processes needed to support the implementation and operations of an ISMS 3. Ability to define, design and implement processes necessary for the operation of an ISMS and properly document them 4. Ability to understand, manage, and evaluate organizational knowledge 5. Ability to understand today's world trends and technologies such as big data, artificial intelligence, machine learning, cloud computing, and outsourced operations 6. Ability to define and implement appropriate information security training and awareness programs, and communication plans 7. Ability to establish an ISMS communication plan to assist in the understanding of an organization's information security issues, policies, performance, and providing inputs or suggestions for improving the performance of the ISMS 8. Ability to establish an incident management policy and incident response team 9. Ability to understand the difference between business continuity and disaster recovery	1. Knowledge of the best practices on documented information life cycle management 2. Knowledge of the characteristics and the differences between the different documented information related to an ISMS policy, procedure, guideline, standard, baseline, worksheet, etc. 3. Knowledge of the three V's of big data: volume, variety, and velocity 4. Knowledge of weak and strong artificial intelligence, machine learning 5. Knowledge of cloud computing services: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) 6. Knowledge of the impact of new technologies in information security 7. Knowledge of the characteristics and the best practices of implementing information security training and awareness programs and communication plans 8. Knowledge of the communication objectives, activities, and interested parties to enhance their support and confidence 9. Knowledge of the incident management process based on information security best practices 10. Knowledge of business continuity and disaster recovery

Domain 5: Monitoring and measurement of an ISMS based on ISO/IEC 27001 **Main objective:** Ensure that the candidate is able to analyse, evaluate, monitor, and measure the performance of an ISMS	
Competencies	**Knowledge statements**
1. Ability to monitor and evaluate the effectiveness of an ISMS 2. Ability to verify to what extent the identified ISMS objectives have been met 3. Ability to define and implement an ISMS internal audit program 4. Ability to perform regular and methodical reviews to ensure the suitability, adequacy, effectiveness, and efficiency of an ISMS based on the policies and objectives of the organization 5. Ability to define and perform a management review process	1. Knowledge of the best practices and techniques used to monitor and evaluate the effectiveness of an ISMS 2. Knowledge of the concepts related to measurement and evaluation 3. Knowledge of the main concepts and components related to the implementation and operation of an ISMS internal audit program 4. Knowledge of the difference between a major and a minor nonconformity 5. Knowledge of the guidelines and best practices to draft a nonconformity report 6. Knowledge of the best practices used to perform management reviews

Domain 6: Continual improvement of an ISMS based on ISO/IEC 27001 **Main objective:** Ensure that the candidate is able to provide guidance on the continual improvement of an ISMS	
Competencies	**Knowledge statements**
1. Ability to track and take action on nonconformities 2. Ability to identify and analyze the root causes of nonconformities, and propose action plans to treat them 3. Ability to counsel an organization on how to continually improve the effectiveness and efficiency of an ISMS 4. Ability to implement continual improvement processes in an organization 5. Ability to determine the appropriate tools to support the continual improvement processes of an organization	1. Knowledge of the main processes, tools, and techniques used to identify the root causes of nonconformities 2. Knowledge of the treatment of nonconformities process 3. Knowledge of the main processes, tools, and techniques used to develop corrective action plans 4. Knowledge of the main concepts related to continual improvement 5. Knowledge of the processes related to the continual monitoring of change factors 6. Knowledge of the maintenance and improvement of an ISMS

Domain 7: Preparing for an ISMS certification audit

Main objective: Ensure that the ISO/IEC 27001 Lead Implementer candidate is able to prepare an organization for the certification against ISO/IEC 27001

Competencies	Knowledge statements
1. Ability to understand the main steps, processes, and activities related to the ISO/IEC 27001 certification audit 2. Ability to understand, explain, and illustrate the audit evidence approach in an ISMS audit 3. Ability to counsel an organization to identify and select a certification body that meets their expectations 4. Ability to determine whether an organization is ready and prepared for the ISO/IEC 27001 certification audit 5. Ability to train and prepare an organization's personnel for the ISO/IEC 27001 certification audit 6. Ability to argue and challenge the audit findings and conclusions with external auditors	1. Knowledge of the evidence-based approach to an audit 2. Knowledge of the types of audit and their differences 3. Knowledge of the differences between Stage 1 and Stage 2 audits 4. Knowledge of the Stage 1 audit requirements, steps, and activities 5. Knowledge of the documented information review criteria 6. Knowledge of the Stage 2 audit requirements, steps, and activities 7. Knowledge of the audit follow-up requirements, steps, and activities 8. Knowledge of the surveillance audits and recertification audit requirements, steps, and activities 9. Knowledge of the requirements, guidelines, and best practices for developing action plans following an ISO/IEC 27001 certification audit

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 an information security management system (ISMS)	15	18.75	X	
	Information security management system (ISMS)	12	15	X	
	Planning an ISMS implementation based on ISO/IEC 27001	18	22.5		X
	Implementing an ISMS based on ISO/IEC 27001	14	17.5		X
	Monitoring and measurement of an ISMS based on ISO/IEC 27001	10	12.5	X	
	Continual improvement of an ISMS based on ISO/IEC 27001	6	7.5	X	
	Preparing for an ISMS certification audit	5	6.25		X
	Total	**80**	**100%**		
	Number of questions per level of understanding			**43**	**37**
	% of the exam devoted to each level of understanding (cognitive/taxonomy)			**53.75%**	**46.25%**

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 27001 Lead Implementer" 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.

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 the ISO/IEC 27001 standard
- Training course materials (accessed through PECB Exams app and/or printed)
- Any personal notes taken during the training course (accessed through 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 Questions

Scenario:

Company A is an insurance company headquartered in Chicago. It offers various range of services and products involving medical and car insurance. The company has recently become one of the most successful and largest insurance companies with more than 70 offices nationwide.

The company's objectives are to properly maintain their assets and protect the confidentiality of information of their clients. The company decided to get certified against ISO/IEC 27001 since it would help them not only achieve their organizational objectives and comply with international laws and regulations but also increase their reputation. The company initiated the implementation of the ISMS by defining an implementation strategy based on a detailed analysis of their existing processes and the ISMS requirements. The company paid special attention to the information security risk assessment, which was crucial in understanding the threats and vulnerabilities that they faced. They also defined the risk criteria with the aim of evaluating the identified risks.

Company A experienced rapid growth which resulted in complex and intensive data processing, and based on the risk assessment results they decided to initially update their existing information classification scheme and then implement the necessary security controls based on the level of protection required by each classification of information.

The medical claims of their clients, classified as sensitive information, were encrypted using the AES encryption and then moved to the private cloud. *Company A* used cloud storage for its ease of access. Due to the frequent access of its employees to this service, the company also decided to utilize the logging process. The service was configured to automatically grant access to cloud storage for all employees responsible for handling medical claims.

Because the cloud storage services experienced security breaches either from human error or deliberate attacks, the company's IT department decided to restrict the access to sensitive information stored in the cloud if professional business emails were not used. In addition, they used a password manager software to manage the passwords of these email addresses and generate stronger passwords.

Based on this scenario, answer the following questions:

1. **The IT Department did not restrict access to cloud storage. Which of the threats below can exploit such vulnerability?**
   A. Tampering with hardware
   B. **Unauthorized use of sensitive information**
   C. Insufficient cloud storage training

2. ***Company A* encrypts sensitive information prior to moving them to the cloud. Which information security principle is followed in this case?**
   A. **Confidentiality, because encryption ensures that only authorized users can access the encrypted information**
   B. Availability, because encryption ensures that information is secured either at rest or in transit, therefore accessible when needed
   C. Integrity, because encryption ensures that only authorized modifications are made to the encrypted information

3. ***Company A* decided to restrict the access to sensitive information stored in the cloud if professional business emails were not used. Which security control was implemented in this case?**
   A. Detective control
   B. **Preventive control**
   C. Corrective control

4. ***Company A* defined the risk criteria when assessing its risks. Is this necessary?**
   A. **Yes, because the company should establish and maintain the risk criteria when assessing the information security risks**
   B. No, because the risk criteria should be established only when risk treatment options are defined
   C. No, because the risk criteria is established when the information security residual risks are accepted

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 27001 Lead Implementer

The requirements for PECB ISO/IEC 27001 Implementer certifications are:

Credential	Exam	Professional experience	ISMS project experience	Other requirements
PECB Certified ISO/IEC 27001 Provisional Implementer	PECB Certified ISO/IEC 27001 Lead Implementer exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27001 Implementer	PECB Certified ISO/IEC 27001 Lead Implementer exam or equivalent	Two years (One in information security management)	200 hours	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27001 Lead Implementer	PECB Certified ISO/IEC 27001 Lead Implementer exam or equivalent	Five years (Two in information security management)	300 hours	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27001 Senior Lead Implementer	PECB Certified ISO/IEC 27001 Lead Implementer exam or equivalent	Ten years (Seven in information security management)	1,000 hours	Signing the PECB Code of Ethics

The ISMS project experience should follow best implementation practices and include the following activities:

1. Drafting an ISMS implementation business case
2. Managing an ISMS implementation project
3. Implementing the ISMS
4. Managing documented information
5. Implementing metrics
6. Implementing corrective actions
7. Performing a management review
8. Managing the ISMS performance
9. Managing an ISMS team

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 project 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.

ISMS Project Experience

The candidate's ISMS project log will be checked to ensure that the candidate has the required number of implementation 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 fulfil 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.

PECB

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 (including examination 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