PECB

BEYOND RECOGNITION

ISO/IEC 27001
LEAD IMPLEMENTER

Candidate Handbook

PECB

Table of Contents

SECTION I: INTRODUCTION

About PECB[1]

PECB is a leading certification body dedicated to fostering digital trust through comprehensive education, certification, and certificate programs across various disciplines. We empower professionals to develop and demonstrate their competence in digital security and other areas of expertise by providing world-class certification programs that adhere to internationally recognized standards.

Slogan:
Beyond Recognition

Vision:
As the global leader in digital trust education and certification, our vision is to empower and inspire professionals by enhancing their skills and fostering their professional success.

Mission:
Our mission is to empower professionals with the knowledge and skills to protect their digital assets and ensure business continuity. Through our comprehensive training programs, we aim to foster a secure digital ecosystem where innovation thrives and risks are managed effectively.

Values
Growth, Change, Harmony, Simplicity, Reliability and Quality

[1] **Notes:**

- The legal name of PECB is "PECB Group Inc."
- PECB is an acronym that stands for "Professional Evaluation and Certification Board."
- Education (used in the first sentence of this page) refers to training courses developed by PECB, and offered globally through its network of partners.
- Certification refers to certification services provided according to ISO/IEC 17024.
- Certificate Program refers to certificate program services provided according to ANSI/ASTM E2659.
- The term "certified" shall only be used for personnel certifications, based on ISO/IEC 17024 requirements. The term "certificate holder" shall only be used for certificate programs, based on ANSI/ASTM E2659 requirements. Certificate holders are not certified, licensed, accredited, or registered to engage in a specific occupation or profession.

The Value of PECB Certification/Certificate Program

Accreditation

PECB credentials are internationally recognized and endorsed by many accreditation bodies, so professionals who pursue them will benefit from our recognition in domestic and international markets.

Our certifications are distinguished by prestigious global accreditations, affirming both their value and your expertise. PECB certifications are validated by top-tier bodies including the International Accreditation Service (IAS-PCB-111), the United Kingdom Accreditation Service (UKAS-No. 21923), the Korean Accreditation Board (KAB-PC-08), and Comité français d'accréditation (COFRAC N° 4-0637) under ISO/IEC 17024 – General requirements for bodies operating certification of persons. Additionally, our certificate programs are validated by the accreditation from the ANSI National Accreditation Board (ANAB-Accreditation ID 1003) under ANSI/ASTM E2659-18, Standard Practice for Certificate Programs.

PECB is also an esteemed associate member of The Independent Association of Accredited Registrars (IAAR), and a full member of the International Personnel Certification Association (IPC), a signatory member of IPC MLA, and a member of Club EBIOS, CPD Certification Service, and CLUSIF. Furthermore, we hold an approved status as an Approved Publishing Partner (APP) by the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) for the Cybersecurity Maturity Model Certification standard (CMMC), and are authorized by Club EBIOS to offer the EBIOS Risk Manager Skills certification and by CNIL (Commission Nationale de l'Informatique et des Libertés) to offer the DPO's skills and knowledge certification.For more detailed information, click here.

High-quality products and services

We are proud to provide our clients with high-quality products and services that match their needs and demands. All of our products are carefully prepared by a team of experts and professionals based on the best practices and methodologies.

Compliance with standards

Our certifications and certificate programs are a demonstration of compliance with ISO/IEC 17024 and ASTM E2659. They ensure that the standard requirements have been fulfilled and validated with adequate consistency, professionalism, and impartiality.

Customer-oriented service

We are a customer-oriented company and treat all our clients with value, importance, professionalism, and honesty. Our Customer Support team is available 24 hours a day, 7 days a week to address questions, requests and needs.

PECB Code of Ethics

The Code of Ethics are the values and ethics that PECB is committed to follow, and defines the responsibilities of PECB professionals including employees, trainers, examiners, invigilators, members of different committees, partners, distributors, certified individuals and certificate holders.

To read the complete version of PECB's Code of Ethics, go to Code of Ethics - PECB.

Introduction to PECB ISO/IEC 27001 Lead Implementer Certification

This document specifies the PECB ISO/IEC 27001 Lead Implementer certification scheme in compliance with ISO/IEC 17024:2012. It also outlines the steps that candidates should take to obtain and maintain their credentials. As such, it is very important to carefully read all the information included in this document before completing and submitting your application. If you have questions or need further information after reading it, please contact certification.team@pecb.com.

PECB

SECTION II: EXAMINATION PREPARATION, RULES, AND POLICIES

Preparing for and scheduling the exam

Candidates are responsible for their own studying and preparation for certification exams. No specific set of training courses or curriculum of study is required as part of the certification process.

To schedule the exam, candidates have two options:

1. **Online:** Through the PECB Exams application. To schedule a remote exam, please go to the following link: Exam Events.
2. **Paper-based:** By contacting the PECB authorized partner that provided the training course. The partner arranges the date, time, and the location where the candidate is going to attend the exam.

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

Rescheduling the exam

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

Application fees for examination and certification

Candidates may take the exam without attending the training course. The applicable prices are as follows:

- Lead Exam: $1000[2]
- Manager Exam: $700
- Foundation Exam: $500
- Transition Exam: $500

The application fee for certification are as follows:

- Master Certification: $100
- Foundation Certification: $200
- Transition Certification: $200
- All other Certifications: $500

For the candidates that have attended the training course via one of PECB's partners, the application fee covers the costs of the exam (first attempt and first retake), the application for certification, and the first year of Annual Maintenance Fee (AMF).

[2] All prices listed in this document are in US dollars.

Competency domains

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
- Project managers, consultants, or expert advisers seeking to master the implementation of an information security management system
- Individuals responsible for maintaining conformity with the ISO/IEC 27001 requirements in an organization
- Members of an ISMS implementation team

The content of the exam is divided as follows:

- **Domain 1:** Fundamental principles and concepts of an information security management system
- **Domain 2:** Information security management system requirements
- **Domain 3:** Planning of an ISMS implementation based on ISO/IEC 27001
- **Domain 4:** Implementation of 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:** Preparation for an ISMS certification audit

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

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

Competencies	Knowledge statements
1. Ability to explain the main concepts of information security 2. Ability to explain the difference and relationship between information and asset 3. Ability to interpret the difference between documents, specifications, and records 4. Ability to explain the relationship between the concepts of vulnerability, threat, risk, and their impact 5. Ability to explain the concepts of confidentiality, integrity, and availability of information 6. Ability to interpret the classification of security controls and their objectives 7. Ability to interpret the relationship between information security elements 8. Ability to explain the information security risk management process, including risk assessment and treatment	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 potential impacts that can affect confidentiality, integrity, or availability of information 7. Knowledge of the difference between security control types such as technical, legal, administrative, and managerial controls 8. Knowledge of the difference between security controls classified by their function such as preventive, corrective, and detective controls

Domain 2: Information security management system requirements

Main objective: Ensure that the candidate is able to identify and explain the requirements for an information security management system based on 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 document the implementation of selected information security controls 5. Ability to interpret and analyze Annex A controls of ISO/IEC 27001 6. 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, boundary control services, integrity services, cryptographic services, and audit and monitoring services 2. Knowledge of the most common architecture frameworks 3. Knowledge of the 93 Annex A controls of ISO/IEC 27001 and their guidance specified in ISO/IEC 27002 4. Knowledge of the four groups of Annex A controls such as organizational controls, people controls, physical controls, technological controls 5. Knowledge of the selection and implementation of ISO/IEC 27001 Annex A controls 6. Knowledge of the documentation of the selected information security

Domain 3: Planning of 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	1. Knowledge of the main project management concepts, terminology, process and best practices
2. Ability to interpret and set information security and ISMS objectives	2. Knowledge of the principal approaches and methodology frameworks to implement an ISMS
3. Ability to identify and interpret ISMS risks and their impacts	3. Knowledge of typical information security and ISMS objectives and how to achieve specific results
4. Ability to analyze and consider the internal and external context of an organization	4. Knowledge of what typically constitutes an organization's internal and external context
5. Ability to identify the resources required for the ISMS implementation	5. Knowledge of the approaches used to understand the context of an organization
6. Ability to manage, estimate, and monitor the required resources for the ISMS implementation	6. Knowledge of the techniques used to gather information on an organization and to perform a gap analysis of a management system
7. Ability to identify the roles and responsibilities of key interested parties during and after the implementation and operation of an ISMS	7. Knowledge of an ISMS project plan and an ISMS project team
8. Ability to draft, file, and review an ISMS project plan	8. Knowledge of the resources required for an ISMS implementation
9. Ability to perform a gap analysis and clarify the information security management objectives	9. Knowledge of the main organizational structures applicable for an organization to manage an ISMS
10. Ability to define and justify an ISMS scope adapted to the organization's specific information security objectives	10. Knowledge of the characteristics of an ISMS scope in terms of organizational, technological, and physical boundaries
11. Ability to develop and establish an ISMS policy	11. Knowledge of the best practices and techniques used to draft and establish information security policies and procedures
12. Ability to perform the steps of the risk assessment process such as risk identification, risk analysis, and risk evaluation	12. Knowledge of the different approaches and methodologies used to perform the risk assessment process
13. Ability to perform risk treatment, risk communication and consultation, recording and reporting, and monitoring and review	13. Knowledge of the selection and implementation of risk treatment options
14. Ability to understand and draft the Statement of Applicability document	14. Knowledge of the characteristics of the Statement of Applicability document

Domain 4: Implementation of an ISMS based on ISO/IEC 27001

Main objective: Ensure that the candidate is able to implement the processes of an ISMS required for an ISO/IEC 27001 certification.

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 and create documents that are understandable and available to all stakeholders 3. Ability to develop a documented information management process to properly manage the document lifecycle 4. Ability to identify the documented information required to demonstrate conformity of the ISMS to the ISO/IEC 27001 requirements 5. Ability to define, design and implement processes necessary for the operation of an ISMS and properly document them 6. Ability to understand, manage, and evaluate organizational knowledge 7. Ability to understand today's world trends and technologies such as big data, artificial intelligence, machine learning, cloud computing, and outsourced operations 8. Ability to define and implement appropriate information security training and awareness programs, and communication plans 9. 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 10. Ability to establish an incident management policy and incident response team 11. Ability to explain the difference between business continuity and disaster recovery 12. Ability to define and implement an incident management process based on information security best practices	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 documents that ensure compliance with ISO/IEC 27001 requirements 4. Knowledge of the three V's of big data: volume, variety, and velocity 5. Knowledge of weak and strong artificial intelligence, machine learning 6. Knowledge of cloud computing services: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) 7. Knowledge of the impact of new technologies in information security 8. Knowledge of the characteristics and the best practices of implementing information security training and awareness programs and communication plans 9. Knowledge of the communication objectives, activities, and interested parties to enhance their support and confidence 10. Knowledge of the incident management process based on information security best practices 11. 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 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	1. Knowledge of the main processes, tools, and techniques used to identify the root causes of nonconformities
2. Ability to identify and analyze the root causes of nonconformities, and propose action plans to treat them	2. Knowledge of the treatment of nonconformities process
3. Ability to counsel an organization on how to continually improve the effectiveness and efficiency of an ISMS	3. Knowledge of the main processes, tools, and techniques used to develop corrective action plans
4. Ability to implement continual improvement processes in an organization	4. Knowledge of the main concepts related to continual improvement
5. Ability to determine the appropriate tools to support the continual improvement processes of an organization	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 candidate is able to prepare an organization for the certification against ISO/IEC 27001.

Competencies	Knowledge statements
1. Ability to interpret the main steps, processes, and activities related to the ISO/IEC 27001 certification audit 2. Ability to explain and illustrate the audit evidence approach of 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 an 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 above-mentioned domains and their relevance, the exam contains 80 multiple-choice questions, 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 evaluation
Competency domains	Fundamental principles and concepts of an information security management system	15	18.75	X	
	Information security management system requirements	12	15	X	
	Planning of an ISMS implementation based on ISO/IEC 27001	18	22.5		X
	Implementation of 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	
	Preparation 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%**.

Taking the exam

General information about 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) Online Exam: Exams are provided electronically via the PECB Exams application. The use of secondary electronic devices, such as tablets and phones, are not allowed during the exam. The exam session is supervised remotely by a PECB Invigilator via the PECB Exams application and an external/integrated camera.

PECB Exam Types:

a. Multiple-choice, closed-book, where the candidates are not allowed to use any reference materials. Usually, Foundation and Transition exams are of this type.

b. Essay-type, open-book, where candidates are allowed to use the following reference materials:

   - A hard copy of main standard
   - Training course materials (accessed through the PECB Exams app and/or printed)
   - Any personal notes taken during the training course (accessed through the PECB Exams app and/or printed)
   - A hard copy dictionary

c. Multiple-choice, open-book, where candidates are allowed to use the following reference materials:

   - A hard copy of main standard
   - Training course materials (accessed through the PECB Exams app and/or printed)
   - Any personal notes taken during the training course (accessed through the PECB Exams app and/or printed)
   - A hard copy dictionary

2) Paper Based: Exams are also available in a paper format. 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 Partner has organized the training course.

PECB Exam Types:

1. Multiple-choice, closed-book, where the candidates are not allowed to use any reference materials. Usually, Foundation and Transition exams are of this type.

2. Essay-type, open-book, where candidates are allowed to use the following reference materials:

    - A hard copy of main standard
    - Training course materials (printed)
    - Any personal notes taken during the training course (printed)
    - A hard copy dictionary

3. Multiple-choice, open-book, where candidates are allowed to use the following reference materials:

    - A hard copy of main standard
    - Training course materials (printed)
    - Any personal notes taken during the training course (printed)
    - A hard copy dictionary

For specific information about exam types, languages available, and other details, please contact support@pecb.com or go to the List of PECB Exams.

This exam comprises multiple-choice questions: The multiple-choice exam can be used to evaluate candidates' understanding on both simple and complex concepts. It comprises both stand-alone and scenario-based questions. Stand-alone questions stand independently within the exam and are not context-depended, whereas scenario-based questions are context-dependent, i.e., they are developed based on a scenario which a candidate is asked to read and is expected to provide answers to five questions related to that scenario. When answering stand-alone and scenario-based questions, candidates will have to apply various concepts and principles explained during the training course, analyze problems, identify and evaluate alternatives, combine several concepts or ideas, etc.

Each multiple-choice question has three options, of which one is the correct response option (keyed response) and two incorrect response options (distractors).

This is an open-book exam. The candidate is allowed to use the following reference materials:

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

A sample of exam questions will be provided below.

Sample exam questions

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 its assets and protect the confidentiality of information of its 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 its 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 advanced encryption standard (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 access to sensitive information stored in the cloud if professional business emails were not used. In addition, they used 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 it 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

Exam results

Exam results will be communicated via email.

- The time span for the communication starts from the exam date and lasts three to eight weeks for essay type exams and 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.

If candidates do not agree with the results, they have 30 days from the date of receiving the results to file a complaint through the PECB Ticketing System. Complaints received after 30 days will not be processed.

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 time span between exam retakes.

If a candidate does not pass the exam on the 1st attempt, they must wait 15 days after the initial date of the exam for the next attempt (1st retake).

Note: Candidates who have completed the training course with one of our partners, and failed the first exam attempt, are eligible to retake for free the exam within a 12-month period from the course completion date (the fee paid for the training course, includes a first exam attempt and one retake). Otherwise, retake fees apply.

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

To arrange exam retakes, based on exam format, candidates that have completed a training course, must follow the steps below:

1. **Online Exam:** Schedule directly through MyPECB Dashboard.
2. **Paper-Based Exam**: candidates need to contact the PECB Partner/Distributor who has initially organized the session for exam retake arrangement (date, time, place, costs).

Candidates that have not completed a training course with a partner, but sat for the online exam directly with PECB, do not fall under this Policy. The process to schedule the exam retake is the same as for the initial exam.

Exam Security Policy

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.

PECB

SECTION III: CERTIFICATION PROCESS AND REQUIREMENTS

PECB ISO/IEC 27001 Lead Implementer credentials

All PECB certifications have specific requirements regarding education and professional experience. To determine which credential is right for you, take into account your professional needs and analyze the criteria for the certifications.

The credentials in the PECB ISO/IEC 27001 Lead Implementer scheme have the following requirements:

Credential	Exam	Professional experience	MS 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		Two years: One year of work experience in information security management	Project activities: a total of 200 hours	
PECB Certified ISO/IEC 27001 Lead Implementer		Five years: Two years of work experience in information security management	Project activities: a total of 300 hours	
PECB Certified ISO/IEC 27001 Senior Lead Implementer		Ten years: Seven years of work experience in information security management	Project activities: a total of 1,000 hours	

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

1. Drafting ISMS implementation plans
2. Initiating ISMS implementation projects
3. Establishing policies, processes, and procedures
4. Setting objectives at relevant levels
5. Implementing the ISMS
6. Managing, monitoring, and maintaining the ISMS
7. Identifying and acting upon continual improvement opportunities

Applying for certification

All candidates who successfully pass the exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credential they were assessed for. Specific professional experience 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 account), including contact details of individuals who will be contacted to validate the candidates' professional experience. They can choose to either pay online or be billed. For additional information, please contact certification.team@pecb.com.

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

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

For more information on how to apply for certification, click here.

The Certification Department validates that the candidate fulfills all the certification requirements regarding the respective credential. The candidate will receive an email about the application status, including the certification decision.

Following the approval of the application by the Certification Department, the candidate will be able to download the certificate and claim the corresponding Digital Badge by going to their Dashboard and clicking view Certificate. For more information about downloading the certificate and the digital badge, click here.

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 CV.

Professional references

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

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 candidates' eligibility for certification or certificate program. 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 may lead to the candidates' credential downgrade.

PECB

SECTION IV: CERTIFICATION POLICIES

Denial of Certification/Certificate Program

PECB can deny certification/certificate program 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/certificate program may file a complaint or appeal by following the complaint and appeal process Complaint and Appeal Policy - PECB).

The application payment for the certification/certificate program is nonrefundable. This is because of the process of verifying the application, the evidence submitted by the candidates, and the engagement of the relevant departments in this process.

Suspension of Certification

Failure to submit the CPD and AMF payment during the certification cycle will result in a 12-month suspension period, during which you can address any outstanding AMFs and CPDs.

Additional reasons for suspension 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 willfully misused.
- The candidate fails to correct the misuse of a certification mark within the determined time by PECB.
- The certified individual has voluntarily requested a suspension.
- PECB deems appropriate other conditions for suspension of certification/certificate program.

Individuals whose certification has been suspended, are not authorized to further promote their certification while it is suspended.

A suspended certification can either be:

- Reinstated – if reasons for suspension are corrected within the given time frame by PECB
- Revoked – if reasons for suspension are not corrected within the given time frame by PECB

Suspended members must remediate their suspension within a maximum period of 12 months.

Revocation of Certification

PECB can revoke (that is, to withdraw) certification if the candidate fails to address the outstanding AMFs and CPDs during the 12-month suspension period. Candidates are then no longer allowed to represent themselves as PECB certified professionals. Additional reasons can be if candidates:

- Violate the PECB Code of Ethics
- Misrepresent and provide false information of the scope of the certification/certificate program
- Break any other PECB rules
- Any other reasons that PECB deems appropriate

Individuals whose certification has been revoked, are not authorized to use any references to a certified status.

Individuals whose certification has been revoked may appeal by following the complaint and appeal process Complaint and Appeal Policy - PECB).

Other Statuses

Besides being active, suspended, or revoked, a certification can be voluntary withdrawn, or designated as Emeritus.

Emeritus Status

Means that your certification is in good standing, but does not need to be maintained by fulfilling CPD nor AMF requirements.

To qualify and be eligible to apply for the Emeritus status, you must be over 60 years of age, have held a PECB certification for at least five years, and you must no longer practice job functions that are specific to the certification.

Optionally, Emeritus who would like to continue practicing job functions, such as audits and/or implementation projects, must report their CPDs on an annual basis, and fulfill a minimum annual requirement of 20 hours of work experience, implementation/auditing or consulting-related experience, training, private study, coaching, attendance at seminars and conferences, or other relevant activities. AMF is not required.

To apply for this status, please complete the form and send it to certification@pecb.com.

Important note: *In order to return to active certification status, you are required to retake the exam and apply for certification.*

Check the brochure for more information about the benefits of the Emeritus Certification Status.

Voluntary Withdrawal Status

Means that your certification is in good standing, but you decide you do not want to maintain your certification(s) anymore.

To apply for this status, please complete the form and send it to certification@pecb.com.
Individuals whose certification has been voluntarily withdrawn will no longer be allowed to present themselves as PECB Certified Professionals.

Important note: *In order to return to active certification status, you are required to retake the exam and apply for certification.*

Permanent Cessation Status

In the event that the certified individual passes away or becomes incapacitated (e.g., because of an accident), the legal representative is responsible for sending the required information to PECB (i.e., death certificate or medical certificate). Consequently, the name of the person will be removed from the contact list and the PECB account will be deleted.

Upgrade credentials

Upgrade of credentials
PECB Professionals can apply for a higher credential once they provide evidence that proves that they fulfill the requirements of the higher credential.

PECB Certifications can be upgraded online through your dashboard by logging here, clicking **View Certificate** and then the **Upgrade** button.

For more information about the upgrade fee, go to the Certification Maintenance page on the PECB website.

Renewing the certification

PECB certifications are valid for three years. To maintain them, PECB certified professionals must meet the requirements related to the designated credential, e.g., they must fulfill the required number of continual professional development (CPD) hours. In addition, they need to pay the annual maintenance fee. For more information, go to the Certification Maintenance page on the PECB website.

Closing a case

If candidates do not apply for certification within one year, 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 to certification.team@pecb.com and pay the required fee.

Complaint and Appeal Policy

Any complaint that a candidate has must be submitted in writing no later than 30 days after PECB's initial decision. Within 30 working days of receiving the complaint, PECB will provide a written response to the candidate, outlining the results of the review and any actions taken.

Candidates may request a re-evaluation of their exam results or certification decision within 30 days. If not satisfied, they can file an appeal through the PECB Ticketing System. For more detailed information, please refer to the Complaint and Appeal Policy | PECB

PECB

SECTION V: GENERAL POLICIES

Exams and certifications from other accredited certification bodies

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 Implementer certification).

Non-discrimination and special accommodations

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

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations[3] for candidates, when appropriate. If candidates need special accommodations because of a disability or a specific physical condition, they should inform the partner/distributor in order for them to make proper arrangements[4]. Any information that candidates provide regarding their disability/special needs will be treated with confidentiality. To download the Candidates with Disabilities Form, click here.

Behavior Policy

PECB aims to provide top-quality, consistent, and accessible services for the benefit of its external stakeholders: distributors, partners, trainers, invigilators, examiners, members of different committees and advisory boards, and clients (trainees, examinees, certified individuals, and certificate holders), as well as creating and maintaining a positive work environment which ensures safety and well-being of its staff, and holds the dignity, respect and human rights of its staff in high regard.

The purpose of this Policy is to ensure that PECB is managing unacceptable behavior of external stakeholders towards PECB staff in an impartial, confidential, fair, and timely manner. To read the Behavior Policy, click here.

Refund Policy

PECB will refund your payment, if the requirements of the Refund Policy are met. To read the Refund Policy, click here.

[3] 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.

[4] 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

Telephone number:

+1-844-426-7322

Emails:

Examination:
examination.team@pecb.com

Certification:
certification.team@pecb.com

Customer Service:
support@pecb.com

PECB Help Center

Visit our Help Center to access manuals, FAQs, and quick guides or reach us directly via Live Chat or by submitting a ticket.

www.pecb.com