PECB BEYOND RECOGNITION

Candidate Handbook

ISO/IEC 27001 Foundation

PECB

Table of Contents

SECTION I: INTRODUCTION

About PECB

PECB is a certificate issuer which provides certificate programs in accordance with ASTM E2659-18 for individuals on a wide range of disciplines.

We help professionals show commitment and competence by providing them with valuable certificate programs 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 for the certificate programs
2. Reviewing and verifying the qualifications of applicant to ensure they are eligible to apply for the certificate programs
3. Developing and maintaining reliable exams
4. Granting certificates to qualified candidates, maintaining records, and publishing a directory of the holders of a valid certificates
5. Representing its members, where appropriate, in matters of common interest
6. Promoting the benefits of certificate programs to organizations, employers, public officials, practitioners in related fields, and the public

The Value of PECB Certificate Program

Why Choose PECB as Your Certificate Issuer?

Global Recognition
Professionals who pursue a PECB certificate program 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 certificate programs are a demonstration of compliance with ASTM E2659. 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 Foundation Certificate Program

ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). The purpose of the PECB ISO/IEC 27001 Foundation certificate program is to help participants understand the basic information security concepts and gain fundamental knowledge on ISMS processes and operations.

The "ISO/IEC 27001 Foundation" certificate demonstrates that individuals have fundamental knowledge of ISO/IEC 27001 requirements for implementing and managing an ISMS. The ISO/IEC 27001 Foundation certificate is intended for:

- Individuals involved in information security management
- Individuals seeking to gain knowledge about the main processes of an ISMS
- Individuals interested to pursue a career in information security management

It is important to understand that PECB certificates 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 Foundation certificates are awarded to candidates that have passed a standardized exam in the certificate program area.

This candidate handbook contains information about the process by which candidates may earn 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 CERTIFICATE PROGRAM PROCESS AND EXAMINATION PREPARATION, RULES, AND POLICIES

Decide Which Certificate Is Right for You

To determine the right credential for you, verify the eligibility criteria for various certificates and your professional needs.

Schedule the Training Course

The first step is to take the training course. Candidates can access the list of the PECB Training Courses here.

Prepare and Schedule the Exam

After completing the training course, candidates need to schedule the exam:

- Contact one of our resellers who provide certificate programs and exam sessions. To find a training course program provider in a particular region, candidates should go to Active Resellers. The PECB training course schedule is also available on Training Events.

ISO/IEC 27001 Foundation Summative Assessment

The summative assessment of the "PECB ISO/IEC 27001 Foundation" certificate program is in the form of a written exam. The objective of the "PECB ISO/IEC 27001 Foundation" exam is to ensure that the candidate has acquired fundamental knowledge of the main concepts and processes related to the implementation and management of an information security management system (ISMS). The exam aims to measure the knowledge and understanding of the learner compared to the intended learning outcomes of the certificate program.

Competency Domains

The exam covers the following competency domains:

- **Domain 1:** Fundamental principles and concepts of an information security management system (ISMS)
- **Domain 2:** Information security management system (ISMS)

The tables below provide the intended learning outcomes of the ISO/IEC 27001 Foundation certificate program in terms of competence and knowledge.

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 main 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 relationship between information and assets 3. Ability to understand and explain the difference between documents, specifications, and records 4. Ability to understand the concept of confidentiality, integrity, and availability of information 5. Ability to understand and interpret the relationship between information security concepts, such as vulnerability, threat, risk, and their impact 6. Ability to understand the main characteristics of artificial intelligence and cloud computing 7. Ability to understand the relationship between assets, risks, threats, vulnerabilities, and controls 8. Ability to understand the definition and benefits of an ISMS 9. Ability to understand the structure and requirements of ISO/IEC 27001 10. Ability to understand, explain, and illustrate the main steps to establish, implement, operate, monitor, review, maintain, and improve an organization's ISMS 11. Ability to understand the "Plan-Do-Check-Act" (PDCA) cycle	1. Knowledge of the information security regulations, international and industry standards, and best practices an organization must comply with 2. Knowledge of the main concepts and terminology of ISO/IEC 27001 3. Knowledge of information security vulnerabilities, threats, and risks 4. Knowledge of the concept of information confidentiality, integrity, and availability 5. Knowledge of the relationship of information security elements 6. Knowledge of the main characteristics of artificial intelligence and cloud computing 7. Knowledge of the definition of management system and management system standards 8. Knowledge of the supporting standards of ISO/IEC 27001 9. Knowledge of ISO/IEC 27001 structure 10. Knowledge of the ISO/IEC 27001 requirements, clauses 4 to 10 11. Knowledge of the main steps for establishing ISMS policies, objectives, processes, and procedures relevant to managing risks and improving information security management system 12. Knowledge of the "Plan-Do-Check-Act" (PDCA) cycle

PECB

Domain 2: Information security management system (ISMS)

Main objective: Ensure that the candidate understands and is able to interpret and identify the requirements for an ISMS based on ISO/IEC 27001

Competencies

1. Ability to understand and set ISMS objectives
2. Ability to analyze and consider the internal and external context of an organization
3. Ability to understand the key roles and responsibilities of interested parties regarding the ISMS
4. Ability to understand and explain different types of policies
5. Ability to understand and interpret the development life cycle of an information security policy
6. Ability to understand the different steps of the risk assessment process
7. Ability to understand how risks are identified, analyzed, and evaluated
8. Ability to understand the ISO/IEC 27001 requirements regarding information security risk treatment
9. Ability to understand the resources required for the ISMS implementation
10. Ability to understand ISO/IEC 27001 requirements regarding competence and people development
11. Ability to understand and interpret the concepts of training, awareness, and communication
12. Ability to understand and explain ISO/IEC 27001 requirements regarding documented information
13. Ability to identify the main processes necessary for the operation of an ISMS
14. Ability to understand and interpret the concepts of monitoring, measurement, analysis, and performance evaluation and their differences
15. Ability to understand the types of audits and their differences

Knowledge statements

1. Knowledge of typical ISMS objectives
2. Knowledge of what typically constitutes an organization's internal and external context
3. Knowledge of ISO/IEC 27001 requirements for roles and responsibilities of interested parties relevant to ISMS
4. Knowledge of different policies, such as high-level general, high-level specific, and topic-specific
5. Knowledge of information security policy and its development life cycle
6. Knowledge of the approaches used to perform the risk assessment process
7. Knowledge of the processes required to identify, analyze, and evaluate risks
8. Knowledge of the basic processes required to treat risks
9. Knowledge of resource management during the ISMS implementation process
10. Knowledge of main competence management and people development activities
11. Knowledge of training and awareness activities and communication principles
12. Knowledge of the types of documented information relevant to the ISMS
13. Knowledge of operational planning
14. Knowledge of the best practices used to monitor and evaluate the effectiveness of an ISMS
15. Knowledge of internal and external audits
16. Knowledge of nonconformities, action plans, and corrective actions
17. Knowledge of the definition and benefits of continual improvement
18. Knowledge of the type and function of security controls
19. Knowledge of Annex A controls and their objectives

16. Ability to understand the concept of nonconformity and the corrective action process 17. Ability to understand and interpret the classification of security controls and their objectives 18. Ability to identify Annex A controls of ISO/IEC 27001 and their objectives	

Based on the abovementioned domains and their relevance, 40 questions are included in the multiple-choice 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	Sections related to each competency domain
Competency domains	Fundamental principles and concepts of an information security management system (ISMS)	20	50	X		Sections 2, 3, and 4
	Information security management system (ISMS)	20	50		X	Sections 5, 6, 7, 8, 9, 10, 11, and 12
	Total	**40**	**100%**			
	Number of questions per level of understanding			**20**	**20**	
	% of the exam devoted to each level of understanding (cognitive/taxonomy)			**50%**	**50%**	

The passing score of the exam is **70%**.

PECB

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.

The exam duration is one hour. If requested on the day of the exam (paper-based exams), 10 additional minutes can be provided to candidates taking the Foundation exam in a non-native language.

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 learner's understanding on many subjects, including both simple and complex concepts. You will find a sample of exam questions provided below.

Since the PECB ISO/IEC 27001 Foundation exam is "closed book", candidates are not authorized to use reference materials.

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.

For specific information about exam types, languages available, and other details, visit the List of PECB Exams.

Sample Exam Questions

1. **What does ISO/IEC 27001 provide?**
   A. **Requirements for an ISMS**
   B. Guidance for codes of practices for information security controls
   C. Guidelines for implementing an ISMS

2. **Which information principle ensures that information is easily reachable when required?**
   A. Confidentiality
   B. Integrity
   C. **Availability**

3. **What type of policy is the information security policy?**
   A. High-level general policies
   B. **High-level specific policies**
   C. Topic-specific policies

4. **During which phase of risk management is residual risk evaluated?**
   A. Risk evaluation
   B. **Risk treatment**
   C. Risk analysis

5. **According to ISO 9000, what is a nonconformity?**
   A. **Non-fulfilment of a requirement**
   B. Fulfilment of a requirement
   C. Fulfilment of information security objectives

Receiving the Exam Results

Exam results will be communicated via email. The only possible results are *pass* and *fail*.

- 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 certificate program.

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 the certificate program is maintaining the security and confidentiality of the exam. PECB relies upon the ethical behavior of certificate 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 invalidating 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 the Certificate

All candidates who successfully pass the ISO ISO/IEC 27001 Foundation exam are entitled to apply for the PECB Certificate Holder in ISO/IEC 27001 Foundation certificate. Candidates are required to fill out the online certificate application form (that can be accessed via their PECB online profile). 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 certificate 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 the certificate

For more information about the application process, follow the instructions on this manual.

The application is approved as soon as the Certification Department validates that the candidate fulfills all the certificate 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 certificate from their PECB Account.

PECB provides support in both English and French.

Closing a Case

If candidates do not apply for the certificate within three years, their case will be closed. Even though the certificate 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: CERTIFICATE PROGRAM REQUISITES

ISO/IEC 27001 Foundation

First, a candidate needs to complete the PECB ISO/IEC 27001 Foundation training course. Then, they need to take the exam and after successfully passing the exam, candidates will be able to apply for the "PECB Certificate Holder in ISO/IEC 27001 Foundation" certificate. This is an entry-level credential.

There are no prerequisites on professional or management system project experience required. Thus, following the training course, passing the exam and applying for the certificate are the only certificate program requisites that certificate holders shall meet before obtaining the certificate.

Designation	Training course	Exam	Professional experience	MS project experience	Other requirements
PECB Certificate Holder in ISO/IEC 27001 Foundation	Complete the PECB ISO/IEC 27001 Foundation Training Course	Pass the PECB ISO/IEC 27001 Foundation exam	None	None	Signing the PECB Code of Ethics

SECTION IV: CERTIFICATE PROGRAM PROCESS RULES AND POLICIES

Evaluation of the Certificate Applications

The Certification Department will evaluate each application to validate the candidate's eligibility for the certificate. 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 rejecting the application.

Denial of the Certificate

PECB can deny the certificate 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 certificate is non-refundable.

Invalidation of the PECB Foundation Certificates

PECB Foundation certificates are invalidated only if the person it was issued to is found to have not fulfilled the certificate program requisites in the first place. Examples of circumstances that might lead to the certificate issuer's invalidation of a certificate include:

- a learner's falsification or misrepresentation of identity or information to the certificate issuer or
- participation in activities that provided an unfair advantage in meeting the certificate program's requirements

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.

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 certificate 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