PECB

Candidate Handbook

ISO/IEC 27002
LEAD MANAGER

Contents

SECTION I: INTRODUCTION 3
About PECB 3
Accreditations and Affiliations 3
PECB Code of Ethics 3
Introduction to ISO/IEC 27002 Lead Manager Certification 4
SECTION II: EXAM PROCESS, RULES AND POLICIES 5
Preparing For and Scheduling the Exam 5
Special Accommodations 5
Taking the Exam 5
Exam Results 6
Exam Retake Policy 6
Exam Security Policy 6
Exam Competency Domains 7
Sample Exam Questions 14
SECTION III: CERTIFICATION PROCESS, RULES AND POLICIES 16
PECB ISO/IEC 27002 Lead Manager Credentials 16
Applying for Certification 16
Professional Experience 17
Professional References 17
Project Experience 17
Evaluation of Certification Applications 17
SECTION IV: CERTIFICATION MAINTENANCE POLICY 18
Renewing the Certification 18
Upgrade Credentials 18
Suspension of Certification 18
Revocation of Certification 18
Other Statuses 18
SECTION V: OTHER POLICIES 19
Application Fees for Examination and Certification 19
Complaint and Appeal Policy 19
Exams from Other Accredited Certification Bodies 19
Refund Policy 19

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.

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 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

Accreditations and Affiliations

At PECB, we are driven and culturally powered by a systemic process of continual improvement and professional development. As a testament to our high standards and commitment to providing quality services to our clients, PECB is accredited by a number of bodies and is a member of many professional organizations.

For detailed information on our accreditations and affiliations, click here.

PECB Code of Ethics

The Code of Ethics is the set of values that PECB is committed to following, 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 PECB's Code of Ethics, click here.

[1] **Notes:**

- The legal name of PECB is "PECB Group Pte. Ltd."
- 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.
- "Certified" refers to ISO/IEC 17024 certifications' requirements and "Certificate holder" refers to ASTM E2659 certificate programs' requirements Certificate holders are not certified, licensed, accredited, or registered to engage in a specific occupation or profession.

Introduction to ISO/IEC 27002 Lead Manager Certification

This document specifies the PECB ISO/IEC 27002 Lead Manager certification scheme in compliance with ISO/IEC 17024. 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 certification application.

If you have questions or need further information after reading it, please contact support@pecb.com.

SECTION II: EXAM PROCESS, RULES AND POLICIES

For detailed and most up-to-date information, you are advised to refer to the online **Exam Rules and Policies** by clicking here.

Preparing For and Scheduling the Exam

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 location where the candidate is going to attend the exam.

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

Special Accommodations

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations for candidates, when appropriate. If candidates need special accommodations because of special needs (dyslexia, dyspraxia, ADHD, vision impairment, but not limited to) and temporary conditions (pregnancy, surgery, postoperative recovery, but not limited to), they can apply for such arrangements through the myPECB dashboard/ Enroll for an Exam. Any information that candidates provide regarding their special needs will be treated with confidentiality.

Taking the Exam

Candidates are required to arrive/be present at least 30 minutes before the exam starts. Candidates who arrive late will not receive additional time to make up for the delay and may not be allowed to sit for the exam.

Candidates are required to bring a valid identity card (national ID card, driver's license, or passport) and show it to the invigilator.

Online Exam Rules	Paper-Based Exam Rules
• Exams are provided electronically via the PECB Exams application. • The use of secondary electronic devices, such as tablets and phones, is 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. • If requested on the day of the exam, 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	• 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 Partner has organized the training course. • If requested on the day of the exam, 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

For specific information on exam types, languages available, and other details, please check the List of PECB Exams.

Exam Results

Exam results will be communicated via email.

- The time span for the communication of exam results 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 disagree with the evaluation, they may request a re-evaluation of their exam results within 30 days from the date they receive their exam results. If still not satisfied, they can file an appeal through the PECB Ticketing System within 30 days from the date they receive the re-evaluation decision. Appeals received after 30 days will not be processed. For more detailed information, please refer to the Complaint and Appeal Policy.

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. For more information, please visit this link: Exam Rules and Policies - PECB

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 who violate such rules and policies, including permanently banning individuals from pursuing PECB credentials and revoking/invalidating any previous ones. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

Exam Competency Domains

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts of information security, cybersecurity, and privacy

Main objective: Ensure that the candidate understands and is able to interpret the main concepts of information security, cybersecurity, and privacy.

Competencies	Knowledge statements
1. Ability to understand and explain the main standards of ISO/IEC 27000 family of standards 2. Ability to understand and explain the concepts of information security, cybersecurity, and privacy 3. Ability to understand and explain the three main principles of information security (confidentiality, integrity, and availability) 4. Ability to understand and explain the relationship between vulnerabilities and threats 5. Ability to understand and explain the purpose of different categories of information security controls 6. Ability to understand and explain the definition of information security risk 7. Ability to understand and explain privacy components and principles	1. Knowledge of ISO/IEC 27000 family of standards 2. Knowledge of the concepts of information security, cybersecurity, and privacy 3. Knowledge of the three main information security principles (confidentiality, integrity, and availability) 4. Knowledge of the relationship between vulnerabilities and threats 5. Knowledge of the categories of information security controls and their purpose 6. Knowledge of the definition of information security risk and its relationship with other information security components 7. Knowledge of the main terms and definitions related to privacy and privacy principles

Domain 2: Information security management system (ISMS) and initiation of ISO/IEC 27002 controls implementation

Main objective: Ensure that the candidate understands the definition of an information security management system (ISMS) and is able to plan the implementation of ISO/IEC 27002 controls.

Competencies	Knowledge statements
1. Ability to understand and explain the definition of a management system and the main components of an ISMS	1. Knowledge of the definition of a management system and the primary management system standards
2. Ability to identify and utilize the main approaches for implementing an ISMS	2. Knowledge of the “Plan-Do-Check-Act” (PDCA) cycle
3. Ability to understand and explain the structure of ISO/IEC 27002	3. Knowledge of the differences between ISO/IEC 27002:2013 and ISO/IEC 27002:2022 standards
4. Ability to distinguish and explain the categories of information security controls of ISO/IEC 27002	4. Knowledge of the structure of ISO/IEC 27002
5. Ability to select and utilize the approaches for analyzing the organization’s existing security architecture	5. Knowledge of organizational, people, physical, and technological controls of ISO/IEC 27002
6. Ability to perform a gap analysis and draft a gap analysis report	6. Knowledge of the main concepts and methods to analyze a security architecture
7. Ability to understand and explain the risk management process	7. Knowledge of techniques and approaches for gathering and interpreting information regarding a security architecture
8. Ability to select an appropriate risk assessment methodology	8. Knowledge of the main concepts related to risk
9. Ability to perform the different steps of the risk assessment process	9. Knowledge of the criteria that should be considered when selecting a risk assessment methodology
10. Ability to analyze and determine the level of risk	10. Knowledge of risk assessment process and its steps
11. Ability to identify risk treatment options and draft a risk treatment plan	11. Knowledge of the types of risk analysis including qualitative, semi-quantitative, and quantitative risk analysis
12. Ability to identify and select adequate controls to prevent and mitigate information security risk	12. Knowledge of risk treatment options (risk modification, risk retention, risk avoidance, and risk sharing)
13. Ability to understand the elements that should be considered when preparing for the implementation of information security controls	13. Knowledge of the main approaches for selecting adequate information security controls
	14. Knowledge of the steps that should be taken to implement the selected information security controls

Domain 3: Implementation and management of organizational and people controls based on ISO/IEC 27002

Main objective: Ensure that the candidate understands how organizational and people controls of ISO/IEC 27002 controls should be implemented and managed.

Competencies	Knowledge statements
1. Ability to understand and explain organizational and people controls based on ISO/IEC 27002	1. Knowledge of organizational and people controls of ISO/IEC 27002
2. Ability to understand and implement the guidelines of ISO/IEC 27002 regarding information security policies	2. Knowledge of the processes regarding the establishment of information security policies
3. Ability to assign and manage information security roles and responsibilities based on the guidelines ISO/IEC 27002	3. Knowledge of the ISO/IEC 27002 guidelines regarding the management of information security roles and responsibilities, segregation of duties, and responsibilities of the management
4. Ability to understand and explain legal, statutory, regulatory, and contractual requirements and other information security requirements	4. Knowledge of the legal, statutory, regulatory, and contractual requirements and compliance with policies, rules, and standards for information security
5. Ability to understand and implement the guidelines of ISO/IEC 27002 to ensure information security in project management and when using cloud services	5. Knowledge of information security practices for project management and cloud services
6. Ability to understand and implement the guidelines of ISO/IEC 27002 to protect records and documented operating procedures	6. Knowledge of the necessary information security controls that ensure the protection of records and personally identifiable information (PII)
7. Ability to understand and implement the guidelines of ISO/IEC 27002 to protect the management of information and other associated assets	7. Knowledge of the threat intelligence concept and its types
8. Ability to understand and implement the guidelines of ISO/IEC 27002 regarding access control, identity management, and access rights management	8. Knowledge of the ISO/IEC 27002 controls that address management of assets and classification and labelling of information
9. Ability to understand and implement the ISO/IEC 27002 controls related to the hiring process of employees, such as screening, termination or change of employment, and terms and conditions of employment	9. Knowledge of the ISO/IEC 27002 controls that address access control, identity management, and access rights management
10. Ability to understand and implement the guidelines of ISO/IEC 27002 regarding information security awareness and training programs	10. Knowledge of the ISO/IEC 27002 controls regarding the hiring process of employees
11. Ability to communicate, monitor, and manage roles and responsibilities regarding information security based on the guidelines of ISO/IEC 27002	11. Knowledge of the ISO/IEC 27002 guidelines regarding information security awareness and training programs
12. Ability to understand and implement the guidelines of ISO/IEC 27002 to ensure information security regarding supplier relationships	12. Knowledge of the ISO/IEC 27002 guidelines applicable to employees to ensure the protection of confidential information
13. Ability to review and monitor supplier services in terms of information security based on the guidelines of ISO/IEC 27002	13. Knowledge of ISO/IEC 27002 controls regarding supplier relationships and management of information security in the ICT supply chain
	14. Knowledge of the ISO/IEC 27002 guidelines for ensuring information security with regard to supplier agreements
	15. Knowledge of the ISO/IEC 27002 guidelines for ensuring the protection of ICT systems during disruptions
	16. Knowledge of the ISO/IEC 27002 guidelines for managing information security incidents including planning and preparation,

14. Ability to understand and explain the concept of business impact analysis and implement the guidelines of ISO/IEC 27002 regarding business continuity plans 15. Ability to understand and implement the guidelines of ISO/IEC 27002 regarding the information security incidents	assessment and decision, response, and learning from information security incidents

Domain 4: Implementation and management of physical and technological controls based on ISO/IEC 27002

Main objective: Ensure that the candidate is able to identify and understand the ISO/IEC 27002 guidelines regarding the management of physical and technological controls.

Competencies	Knowledge statements
1. Ability to understand the purpose of physical and technological controls of ISO/IEC 27002	1. Knowledge of physical and technological controls of ISO/IEC 27002
2. Ability to understand and implement the ISO/IEC 27002 guidelines regarding physical security perimeters	2. Knowledge of the ISO/IEC 27002 guidelines regarding physical security perimeter and physical entry controls
3. Ability to understand and implement the guidelines of ISO/IEC 27002 regarding the security of offices, rooms, and other facilities	3. Knowledge of the ISO/IEC 27002 guidelines regarding the security of offices, rooms, and facilities
4. Ability to utilize and implement the guidelines of ISO/IEC 27002 and other best practices for protecting an organization's premises against physical and environmental threats	4. Knowledge of the ISO/IEC 27002 controls that address secure areas
5. Ability to understand and implement the clear desk and clear screen policy based on the guidelines of ISO/IEC 27002	5. Knowledge of clear desk and clear screen policy of ISO/IEC 27002
6. Ability to understand and implement the guidelines of ISO/IEC 27002 to secure storage media and equipment	6. Knowledge of the ISO/IEC 27002 guidelines for managing storage media and protecting equipment
7. Ability to establish an equipment maintenance plan based on the guidelines of ISO/IEC 27002	7. Knowledge of the ISO/IEC 27002 guidelines regarding equipment maintenance plan
8. Ability to understand and implement the guidelines of ISO/IEC 27002 to ensure protection against malware	8. Knowledge of the ISO/IEC 27002 guidelines regarding the protection of information against malicious code
9. Ability to manage technical vulnerabilities based on the guidelines of ISO/IEC 27002	9. Knowledge of capacity management and configuration management based on the guidelines of ISO/IEC 27002
10. Ability to understand and implement the guidelines of ISO/IEC 27002 regarding data anonymization and pseudonymization	10. Knowledge of data masking process and data leakage prevention measures based on ISO/IEC 27002
11. Ability to understand and implement the guidelines of ISO/IEC 27002 regarding asymmetric and symmetric cryptography	11. Knowledge of the concept of cryptography and its management based on the guidelines of ISO/IEC 27002
12. Ability to understand and implement ISO/IEC 27002 controls to ensure the security of applications throughout their development life cycle	12. Knowledge of the ISO/IEC 27002 controls that address secure development life cycle, system architecture, and coding
13. Ability to understand and implement ISO/IEC 27002 controls that address endpoint devices, logging records, and clock synchronization	13. Knowledge of the ISO/IEC 27002 controls regarding the management of privileged access rights and the use of privileged utility programs
14. Ability to understand and implement ISO/IEC 27002 controls that ensure authorized access to information and other associated assets	14. Knowledge of the ISO/IEC 27002 guidelines regarding identity management and privileged access management
15. Ability to understand and implement ISO/IEC 27002 controls that address the protection of networks	15. Knowledge of the ISO/IEC 27002 guidelines that address risks related to unauthorized access of the source code
	16. Knowledge of the recording and reviewing processes of logs based on the guidelines of ISO/IEC 27002
	17. Knowledge of the guidelines of ISO/IEC 27002 to ensure the security of networks

Domain 5: Performance measurement, testing, and monitoring of ISO/IEC 27002 information security controls

Main objective: Ensure that the candidate is able to understand the ISO/IEC 27002 controls for testing information security and is able to conduct performance measurement and monitoring activities based on ISO/IEC 27002.

Competencies	Knowledge statements
1. Ability to understand and implement the guidelines of ISO/IEC 27002 for testing information security	1. Knowledge of the ISO/IEC 27002 guidelines regarding the stages of software testing life cycle and best security testing techniques and tools
2. Ability to understand and implement the guidelines of ISO/IEC 27002 for ensuring information security of outsourced services	2. Knowledge of the monitoring and review activities related to outsourced system development based on the guidelines of ISO/IEC 27002
3. Ability to understand and implement the guidelines of ISO/IEC 27002 for protecting the production environment	3. Knowledge of the ISO/IEC 27002 guidelines regarding software development environments including development, staging, and production
4. Ability to understand and implement the guidelines of ISO/IEC 27002 for protecting test information	4. Knowledge of the ISO/IEC 27002 guidelines that address the risks of unauthorized access to or use of test information
5. Ability to understand and implement the guidelines of ISO/IEC 27002 for protecting information systems during audit testing	5. Knowledge of the ISO/IEC 27002 guidelines that address the protection of information systems during audit testing
6. Ability to perform independent reviews of information security based on the guidelines of ISO/IEC 27002	6. Knowledge of the ISO/IEC 27002 guidelines for reviewing information security
7. Ability to understand and implement best practices for network monitoring	7. Knowledge of the network monitoring techniques
8. Ability to understand and implement continual improvement processes based on the guidelines of ISO/IEC 27002	8. Knowledge of the best approaches used to monitor the effectiveness of information security controls
9. Ability to select and implement the appropriate approaches for maintaining information security based on the guidelines of ISO/IEC 27002	9. Knowledge of the ISO/IEC 27002 guidelines regarding continual improvement activities

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 information security, cybersecurity, and privacy	10	12.5	X	
	Information security management system (ISMS) and initiation of ISO/IEC 27002 controls implementation	10	12.5	X	
	Implementation and management of organizational and people controls based on ISO/IEC 27002	20	25		X
	Implementation and management of physical and technological controls based on ISO/IEC 27002	20	25		X
	Performance measurement, testing, and monitoring of ISO/IEC 27002 information security controls	20	25	X	
	Total	**80**	**100%**		
	Number of questions per level of understanding			**40**	**40**
	% of the exam devoted to each level of understanding (cognitive/taxonomy)			**50%**	**50%**

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

This exam comprises multiple-choice questions: The multiple-choice exam can be used to evaluate candidates' understanding of 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-dependent, whereas scenario-based questions are context-dependent, i.e., they are developed based on a scenario that 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 copy of the ISO/IEC 27002 standard (accessed through the PECB Exams app and/or printed)
- 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

ChereX is an American manufacturer of electronic products. The company aims to provide advanced electronic products that meet customers' needs. As technology evolved, the electronics manufacturing industry became a target of cyberattacks. Therefore, *ChereX* has significantly invested to create secure systems and a sustainable security culture. As part of these initiatives, *ChereX* decided to implement an information security management system (ISMS) based on ISO/IEC 27001. In addition, they used ISO/IEC 27002 guidelines as part of the ISMS implementation.

Based on the guidelines of ISO/IEC 27002, *ChereX* established an information security awareness and training program which enabled the top management to ensure that all employees understand their roles and responsibilities regarding information security. The information security awareness and training sessions are performed each quarter and are customized to the roles and functions of different departments. *ChereX's* information security awareness and training program involves various discussions regarding the information security policies and the responsibilities of each employee to protect organization's assets.

ChereX also conducted a risk assessment process to identify and analyze the risks related to its information systems. Following the *ChereX*'s risk assessment methodology, the information security manager identified assets, threats, vulnerabilities, and risk sources. The list of assets included some damaged storage media that contained sensitive data. Since there was no procedure for managing storage media within the company, these devices were placed in *ChereX*'s offices without appropriate measures for protecting them against unauthorized access. Considering that the risk of unauthorized access to sensitive information through these devices was defined as "high," *ChereX* decided to immediately destroy the devices. The information security manager developed a topic-specific policy on the management of storage media. Then, the information security manager approved the policy and communicated it to the IT Department.

Based on the scenario above, answer the following questions:

1. ***ChereX* used ISO/IEC 27002 as a supporting standard for implementing the ISMS based on ISO/IEC 27001. Is this acceptable?**
   A. **Yes, the guidelines of ISO/IEC 27002 can be used within the context of an ISMS**
   B. No, only the guidelines of ISO/IEC 27002 should be used to implement an ISMS
   C. No, ISO/IEC 27002 can be used only by organizations that have already established an ISMS

2. ***ChereX* immediately implemented controls to treat the risk regarding the devices that contain sensitive data? Is this in accordance with the guidelines of ISO/IEC 27002?**
   A. Yes, *ChereX* should physically destroy all damaged devices that contain sensitive data
   B. **No, *ChereX* should conduct a risk assessment on damaged devices to determine whether they should be physically destroyed**
   C. No, *ChereX* should repair the damaged devices and ensure that the sensitive information is not deleted prior to disposal or re-use

3. *ChereX* has established an information security awareness program. Based on the guidelines of ISO/IEC 27002, what type of control has *ChereX* implemented?

A. Organizational
B. **People**
C. Technological

4. Has *ChereX* followed all the guidelines of ISO/IEC 27002 when developing the topic-specific policy regarding storage media management?

A. **No, topic-specific policies should be approved by top management**
B. No, topic-specific policies should be communicated and acknowledged by all personnel of the company
C. Yes, the topic-specific policy was developed and approved by the information security manager and communicated to relevant personnel

SECTION III: CERTIFICATION PROCESS, RULES AND POLICIES

PECB ISO/IEC 27002 Lead Manager Credentials

All PECB certifications have specific requirements regarding 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 27002 Lead Manager scheme have the following requirements:

Credential	Exam	Professional experience	Information security management experience	Other requirements
PECB Certified ISO/IEC 27002 Provisional Manager	PECB Certified **ISO/IEC 27002** Lead Manager exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27002 Manager		Two years: One year of work experience in information security management	Project activities: a total of 200 hours	
PECB Certified ISO/IEC 27002 Lead Manager		Five years: Two years of work experience in information security management	Project activities: a total of 300 hours	
PECB Certified ISO/IEC 27002 Senior Lead Manager		Ten years: Seven years of work experience in information security management	Project activities: a total of 1,000 hours	

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

1. Drafting an ISMS implementation plan
2. Managing an information security implementation project
3. Implementing information security processes
4. Selecting information security controls
5. Implementing and evaluating information security controls

For detailed and most up-to-date information, you are advised to refer to the online **Certification Process** by clicking here.

Applying for Certification

All participants who successfully pass their certification exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credentials they were examined for. Specific professional requirements will need to be fulfilled to be PECB certified.

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

- Create your account
- Check your email for the confirmation link
- Log in and click on Apply for Certificate

The approval of the application occurs when the Certification Department validates that you fulfil all the certification requirements regarding the credential you have applied for. An email will be sent to the address you provided during your application to update you on your application status. If

approved, you will then be able to download your certificate and digital badge from your member account.

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.

Project Experience

The candidate's project log will be checked to ensure that the candidate has the required number of information security management 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 can deny certification/certificate program if candidates:

- Falsify the application
- Violate the exam procedures
- Violate the PECB Code of Ethics
- Fail the exam

If applicants have any concerns regarding the denial of certification/certificate program, they may file an appeal by following the complaint and appeal process Complaint and Appeal Policy.

The application payment for the certification/certificate program is nonrefundable. This is due to the application verification process, the evidence submitted by the candidates, and the involvement of the relevant departments.

If candidates pass the exam, they can apply for the certificate within 12 months from the course completion date for instructor-led training, or within 12 months from the purchase date for self-study and eLearning formats. 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.

SECTION IV: CERTIFICATION MAINTENANCE POLICY

For detailed and most up-to-date information, you are advised to refer to the online **Certification Maintenance Policy** by clicking here.

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 continuing professional development (CPD) hours. In addition, they need to pay the annual maintenance fee.

Upgrade Credentials

PECB Certifications can be upgraded online through your dashboard by logging in here, clicking **View Certificate,** and then clicking the **Upgrade** button. For more information on the upgrade requirements and fees, go to the Certification Maintenance page on the PECB website.

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. In addition to these, the certification may be suspended for other reasons listed in the **Certification Maintenance Policy.** Individuals whose certification has been suspended are not authorized to further promote their certification while it is suspended.

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

Revocation of Certification

PECB can revoke (that is, withdraw) certification if the candidate fails to address the outstanding AMFs and CPDs during the 12-month suspension period. In addition to these, certification may be revoked for other reasons listed in the **Certification Maintenance Policy.** Individuals whose certification has been revoked are not authorized to use any references to a certified status.

If candidates disagree with any certification decision (certification level, suspension, or revocation) they may request a re-evaluation within 30 days from the date they receive their certification decision. If still not satisfied, they can file an appeal through the PECB Ticketing System within 30 days from the date they receive the re-evaluation decision. Appeals received after 30 days will not be processed. For more detailed information, please refer to Complaint and Appeal Policy.

Other Statuses

Besides being active, suspended, or revoked, a certification can be voluntary withdrawn, or designated as Emeritus. For more information, go to the Certification Maintenance page on the PECB website.

SECTION V: OTHER POLICIES

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 is as follows:

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

For candidates who complete a training, eLearning, or self-study course delivered by a PECB Partner, the training fee includes the first exam attempt, one free retake, the certification application fee, and the first year of the Annual Maintenance Fee (AMF). This cycle must be completed within 12 months from the course completion date for instructor-led training, or within 12 months from the purchase date for self-study and eLearning formats.

Complaint and Appeal Policy

A person wishing to file a complaint or an appeal can do so by submitting a service ticket and selecting the corresponding category in the topic dropdown menu: “file a complaint” or “file a certification/certificate program appeal”. Before filing a complaint or an appeal, make sure to follow the complaint and appeal policy.

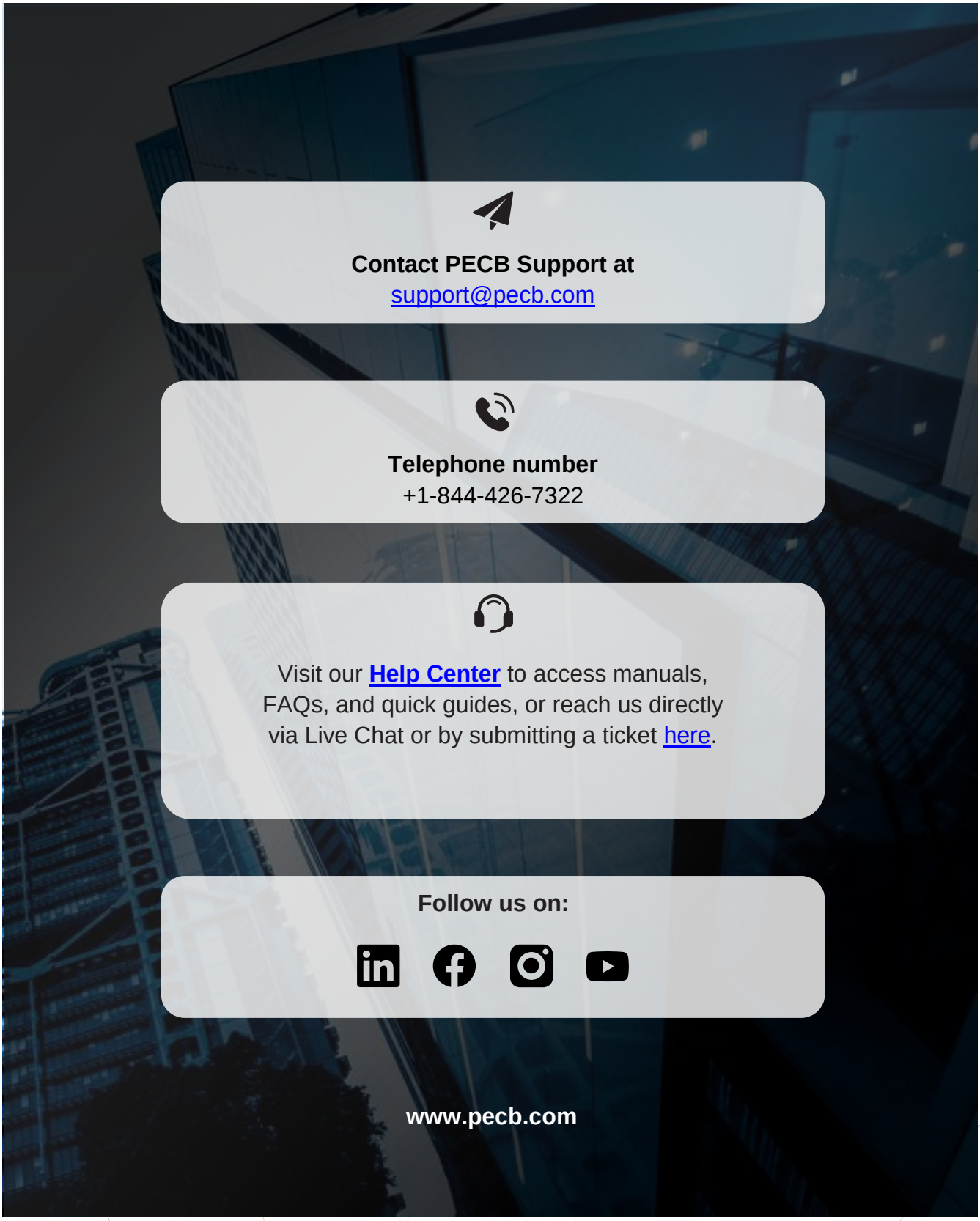
Exams from Other Accredited Certification Bodies

PECB accepts exams from other recognized accredited certification bodies. PECB will evaluate the requests through its equivalence process to decide whether the respective exam(s) can be accepted as equivalent to the respective PECB certification.

Refund Policy

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

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



Contact PECB Support at
support@pecb.com

Telephone number
+1-844-426-7322

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

Follow us on:

www.pecb.com

©2026 PECB