PECB

BEYOND RECOGNITION

ISO/IEC 27002 LEAD MANAGER

Candidate Handbook

Table of Contents

SECTION I: INTRODUCTION

About PECB

PECB is a certification body that provides education[1], certification, and certificate programs for individuals on a wide range of disciplines.

Through our presence in more than 150 countries, we help professionals demonstrate their competence in various areas of expertise by providing valuable evaluation, certification, and certificate programs against internationally recognized standards.

Our key objectives are:

1. Establishing the minimum requirements necessary to certify professionals and to grant designations
2. Reviewing and verifying the qualifications of individuals to ensure they are eligible for certification
3. Maintaining and continually improving the evaluation process for certifying individuals
4. Certifying qualified individuals, granting designations and maintaining respective directories
5. Establishing requirements for the periodic renewal of certifications and ensuring that the certified individuals are complying with those requirements
6. Ascertaining that PECB professionals meet ethical standards in their professional practice
7. Representing our stakeholders in matters of common interest
8. Promoting the benefits of certification and certificate programs to professionals, businesses, governments, and the public

Our mission

Provide our clients with comprehensive examination, certification, and certificate program services that inspire trust and benefit the society as a whole.

Our vision

Become the global benchmark for the provision of professional certification services and certificate programs.

Our values

Integrity, Professionalism, Fairness

[1] Education refers to training courses developed by PECB and offered globally through our partners.

The Value of PECB Certification

Global recognition
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.

The value of PECB certifications is validated by the accreditation from the International Accreditation Service (IAS-PCB-111), the United Kingdom Accreditation Service (UKAS-No. 21923) and the Korean Accreditation Board (KAB-PC-08) under ISO/IEC 17024 – General requirements for bodies operating certification of persons. The value of PECB certificate programs is 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 an associate member of The Independent Association of Accredited Registrars (IAAR), 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, CLUSIF, Credential Engine, and ITCC. In addition, PECB is an approved Licensed Partner Publisher (LPP) from the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) for the Cybersecurity Maturity Model Certification standard (CMMC), is approved by Club EBIOS to offer the EBIOS Risk Manager Skills certification, and is approved by CNIL (Commission Nationale de l'Informatique et des Libertés) to offer DPO 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. PECB has a team of experts who are responsible for addressing requests, questions, and needs. We do our best to maintain a 24-hour maximum response time without compromising the quality of the services.

Flexibility and convenience
Online learning opportunities make your professional journey more convenient as you can schedule your learning sessions according to your lifestyle. Such flexibility gives you more free time, offers more career advancement opportunities, and reduces costs.

PECB Code of Ethics

The Code of Ethics represents the highest values and ethics that PECB is fully committed to follow, as it recognizes the importance of them when providing services and attracting clients.

The Compliance Division makes sure that PECB employees, trainers, examiners, invigilators, partners, distributors, members of different advisory boards and committees, certified individuals, and certificate holders (hereinafter "PECB professionals") adhere to this Code of Ethics. In addition, the Compliance Division consistently emphasizes the need to behave professionally and with full responsibility, competence, and fairness in service provision with internal and external stakeholders, such as applicants, candidates, certified individuals, certificate holders, accreditation authorities, and government authorities.

It is PECB's belief that to achieve organizational success, it has to fully understand the clients and stakeholders' needs and expectations. To do this, PECB fosters a culture based on the highest levels of integrity, professionalism, and fairness, which are also its values. These values are integral to the organization, and have characterized the global presence and growth over the years and established the reputation that PECB enjoys today.

PECB believes that strong ethical values are essential in having healthy and strong relationships. Therefore, it is PECB's primary responsibility to ensure that PECB professionals are displaying behavior that is in full compliance with PECB principles and values.

PECB professionals are responsible for:

1. Displaying professional behavior in service provision with honesty, accuracy, fairness, and independence
2. Acting at all times in their service provision solely in the best interest of their employer, clients, the public, and the profession in accordance with this Code of Ethics and other professional standards
3. Demonstrating and developing competence in their respective fields and striving to continually improve their skills and knowledge
4. Providing services only for those that they are qualified and competent and adequately informing clients and customers about the nature of proposed services, including any relevant concerns or risks
5. Informing their employer or client of any business interests or affiliations which might influence or impair their judgment
6. Preserving the confidentiality of information of any present or former employer or client during service provision
7. Complying with all the applicable laws and regulations of the jurisdictions in the country where the service provisions were conducted
8. Respecting the intellectual property and contributions of others
9. Not communicating intentionally false or falsified information that may compromise the integrity of the evaluation process of a candidate for a PECB certification or a PECB certificate program
10. Not falsely or wrongly presenting themselves as PECB representatives without a proper license or misusing PECB logo, certifications or certificates
11. Not acting in ways that could damage PECB's reputation, certifications or certificate programs
12. Cooperating in a full manner on the inquiry following a claimed infringement of this Code of Ethics

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

Introduction to ISO/IEC 27002 Lead Manager

ISO/IEC 27002 provides guidelines for implementing information security controls to treat information security risks. The implementation of these information security controls will enable organizations to effectively establish and enforce policies and controls to ensure information security in accordance with industry best practices. ISO/IEC 27002 can be used within the context of an information security management system (ISMS) based on ISO/IEC 27001.

The "ISO/IEC 27002 Lead Manager" credential demonstrates that you possess the necessary competence to implement, monitor, and continually improve information security controls that help organizations protect their information. The training course provides a comprehensive overview of the main approaches and techniques to implement information security controls.

PECB certifications are not a license or simply a membership. They attest the candidates' knowledge and skills gained through our training courses and are issued to candidates that have the required experience and have passed the exam.

This document specifies the PECB ISO/IEC 27002 Lead Manager 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 the PECB international office at certification.team@pecb.com.

SECTION II: EXAMINATION PREPARATION, RULES, AND POLICIES

Preparing for and scheduling the exam

All candidates are responsible for their own study and preparation for certification exams. Although candidates are not required to attend the training course to be eligible for taking the exam, attending it can significantly increase their chances of successfully passing the exam.

To schedule the exam, candidates have two options:

1. Contact one of our authorized partners. To find an authorized partner in your region, please go to Active Partners. The training course schedule is also available online and can be accessed on Training Events.
2. Take a PECB exam remotely through the PECB Exams application. To schedule a remote exam, please go to the following link: Exam Events.

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 is $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 objective of the “PECB ISO/IEC 27002 Lead Manager” exam is to ensure that the candidate has acquired the adequate knowledge and skills to support an organization in selecting and implementing appropriate information security controls for treating information security risks.

The ISO/IEC 27002 Lead Manager certification is intended for:

- Managers or consultants seeking to increase their knowledge regarding the implementation of information security controls
- Managers or consultants involved in and concerned with the implementation of an ISMS
- Individuals responsible for maintaining conformity to the requirements of ISO/IEC 27001 in an organization
- IT professionals or consultants seeking to increase their knowledge in information security
- Members of an ISMS implementation team or information security team

The content of the exam is divided as follows:

- **Domain 1:** Fundamental principles and concepts of information security, cybersecurity, and privacy
- **Domain 2:** Information security management system (ISMS) and initiation of ISO/IEC 27002 controls implementation
- **Domain 3:** Implementation and management of organizational and people controls based on ISO/IEC 27002
- **Domain 4:** Implementation and management of physical and technological controls based on ISO/IEC 27002
- **Domain 5:** Performance measurement, testing, and monitoring of ISO/IEC 27002 information security controls

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 2. Ability to identify and utilize the main approaches for implementing an ISMS 3. Ability to understand and explain the structure of ISO/IEC 27002 4. Ability to distinguish and explain the categories of information security controls of ISO/IEC 27002 5. Ability to select and utilize the approaches for analyzing the organization's existing security architecture 6. Ability to perform a gap analysis and draft a gap analysis report 7. Ability to understand and explain the risk management process 8. Ability to select an appropriate risk assessment methodology 9. Ability to perform the different steps of the risk assessment process 10. Ability to analyze and determine the level of risk 11. Ability to identify risk treatment options and draft a risk treatment plan 12. Ability to identify and select adequate controls to prevent and mitigate information security risk 13. Ability to understand the elements that should be considered when preparing for the implementation of information security controls	1. Knowledge of the definition of a management system and the primary management system standards 2. Knowledge of the "Plan-Do-Check-Act" (PDCA) cycle 3. Knowledge of the differences between ISO/IEC 27002:2013 and ISO/IEC 27002:2022 standards 4. Knowledge of the structure of ISO/IEC 27002 5. Knowledge of organizational, people, physical, and technological controls of ISO/IEC 27002 6. Knowledge of the main concepts and methods to analyze a security architecture 7. Knowledge of techniques and approaches for gathering and interpreting information regarding a security architecture 8. Knowledge of the main concepts related to risk 9. Knowledge of the criteria that should be considered when selecting a risk assessment methodology 10. Knowledge of risk assessment process and its steps 11. Knowledge of the types of risk analysis including qualitative, semi-quantitative, and quantitative risk analysis 12. Knowledge of risk treatment options (risk modification, risk retention, risk avoidance, and risk sharing) 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 2. Ability to understand and implement the guidelines of ISO/IEC 27002 regarding information security policies 3. Ability to assign and manage information security roles and responsibilities based on the guidelines ISO/IEC 27002 4. Ability to understand and explain legal, statutory, regulatory, and contractual requirements and other information security requirements 5. Ability to understand and implement the guidelines of ISO/IEC 27002 to ensure information security in project management and when using cloud services 6. Ability to understand and implement the guidelines of ISO/IEC 27002 to protect records and documented operating procedures 7. Ability to understand and implement the guidelines of ISO/IEC 27002 to protect the management of information and other associated assets 8. Ability to understand and implement the guidelines of ISO/IEC 27002 regarding access control, identity management, and access rights management 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 10. Ability to understand and implement the guidelines of ISO/IEC 27002 regarding information security awareness and training programs	1. Knowledge of organizational and people controls of ISO/IEC 27002 2. Knowledge of the processes regarding the establishment of information security policies 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. Knowledge of the legal, statutory, regulatory, and contractual requirements and compliance with policies, rules, and standards for information security 5. Knowledge of information security practices for project management and cloud services 6. Knowledge of the necessary information security controls that ensure the protection of records and personally identifiable information (PII) 7. Knowledge of the threat intelligence concept and its types 8. Knowledge of the ISO/IEC 27002 controls that address management of assets and classification and labelling of information 9. Knowledge of the ISO/IEC 27002 controls that address access control, identity management, and access rights management 10. Knowledge of the ISO/IEC 27002 controls regarding the hiring process of employees 11. Knowledge of the ISO/IEC 27002 guidelines regarding information security awareness and training programs 12. Knowledge of the ISO/IEC 27002 guidelines applicable to employees to ensure the protection of confidential information 13. Knowledge of ISO/IEC 27002 controls regarding supplier relationships and

11. Ability to communicate, monitor, and manage roles and responsibilities regarding information security based on the guidelines of ISO/IEC 27002
12. Ability to understand and implement the guidelines of ISO/IEC 27002 to ensure information security regarding supplier relationships
13. Ability to review and monitor supplier services in terms of information security based on the guidelines of ISO/IEC 27002
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

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, 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 2. Ability to understand and implement the ISO/IEC 27002 guidelines regarding physical security perimeters 3. Ability to understand and implement the guidelines of ISO/IEC 27002 regarding the security of offices, rooms, and other 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 5. Ability to understand and implement the clear desk and clear screen policy based on the guidelines of ISO/IEC 27002 6. Ability to understand and implement the guidelines of ISO/IEC 27002 to secure storage media and equipment 7. Ability to establish an equipment maintenance plan based on the guidelines of ISO/IEC 27002 8. Ability to understand and implement the guidelines of ISO/IEC 27002 to ensure protection against malware 9. Ability to manage technical vulnerabilities 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 11. Ability to understand and implement the guidelines of ISO/IEC 27002 regarding asymmetric and symmetric cryptography 12. Ability to understand and implement ISO/IEC 27002 controls to ensure the security of applications throughout their development life cycle	1. Knowledge of physical and technological controls of ISO/IEC 27002 2. Knowledge of the ISO/IEC 27002 guidelines regarding physical security perimeter and physical entry controls 3. Knowledge of the ISO/IEC 27002 guidelines regarding the security of offices, rooms, and facilities 4. Knowledge of the ISO/IEC 27002 controls that address secure areas 5. Knowledge of clear desk and clear screen policy of ISO/IEC 27002 6. Knowledge of the ISO/IEC 27002 guidelines for managing storage media and protecting equipment 7. Knowledge of the ISO/IEC 27002 guidelines regarding equipment maintenance plan 8. Knowledge of the ISO/IEC 27002 guidelines regarding the protection of information against malicious code 9. Knowledge of capacity management and configuration management based on the guidelines of ISO/IEC 27002 10. Knowledge of data masking process and data leakage prevention measures based on ISO/IEC 27002 11. Knowledge of the concept of cryptography and its management based on the guidelines of ISO/IEC 27002 12. Knowledge of the ISO/IEC 27002 controls that address secure development life cycle, system architecture, and coding 13. Knowledge of the ISO/IEC 27002 controls regarding the management of privileged access rights and the use of privileged utility programs

13. Ability to understand and implement ISO/IEC 27002 controls that address endpoint devices, logging records, and clock synchronization 14. Ability to understand and implement ISO/IEC 27002 controls that ensure authorized access to information and other associated assets 15. Ability to understand and implement ISO/IEC 27002 controls that address the protection of networks	14. Knowledge of the ISO/IEC 27002 guidelines regarding identity management and privileged access management 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%**.

After successfully passing the exam, candidates will be able to apply for obtaining the “PECB Certified ISO/IEC 27002 Lead Manager” credential.

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. **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 Partner 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 information about online exams, go to the PECB Online Exam Guide.

PECB exams are available in two types:

1. Essay-type question exam
2. Multiple-choice question exam

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 27002 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

A sample of exam questions will be provided below.

Note: PECB will progressively transition to multiple-choice exams. They will also be open book and comprise scenario-based questions that will allow PECB to evaluate candidates' knowledge, abilities, and skills to use information in new situations (apply), draw connections among ideas (analyze), and justify a stand or decision (evaluate).

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

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. **_CherеX_ has established an information security awareness program. Based on the guidelines of ISO/IEC 27002, what type of control has _CherеX_ implemented?**
   A. Organizational
   B. **People**
   C. Technological

4. **Has _CherеX_ 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

Exam Security Policy

PECB is committed to protect the integrity of its exams and the overall examination process, and relies upon the ethical behavior of applicants, potential applicants, candidates and partners to maintain the confidentiality of PECB exams. This Policy aims to address unacceptable behavior and ensure fair treatment of all candidates.

Any disclosure of information about the content of PECB exams is a direct violation of this Policy and PECB's Code of Ethics. Consequently, candidates taking a PECB exam are required to sign an Exam Confidentiality and Non-Disclosure Agreement and must comply with the following:

1. The questions and answers of the exam materials are the exclusive and confidential property of PECB. Once candidates complete the submission of the exam to PECB, they will no longer have any access to the original exam or a copy of it.
2. Candidates are prohibited from revealing any information regarding the questions and answers of the exam or discuss such details with any other candidate or person.
3. Candidates are not allowed to take with themselves any materials related to the exam, out of the exam room.
4. Candidates are not allowed to copy or attempt to make copies (whether written, photocopied, or otherwise) of any exam materials, including, without limitation, any questions, answers, or screen images.
5. Candidates must not participate nor promote fraudulent exam-taking activities, such as:
   - Looking at another candidate's exam material or answer sheet
   - Giving or receiving any assistance from the invigilator, candidate, or anyone else
   - Using unauthorized reference guides, manuals, tools, etc., including using "brain dump" sites as they are not authorized by PECB

Once a candidate becomes aware or is already aware of the irregularities or violations of the points mentioned above, they are responsible for complying with those, otherwise if such irregularities were to happen, candidates will be reported directly to PECB or if they see such irregularities, they should immediately report to PECB.

Candidates are solely responsible for understanding and complying with PECB Exam Rules and Policies, Confidentiality and Non-Disclosure Agreement and Code of Ethics. Therefore, should a breach of one or more rules be identified, candidates will not receive any refunds. In addition, PECB has the right to deny the right to enter a PECB exam or to invite candidates for an exam retake if irregularities are identified during and after the grading process, depending on the severity of the case.

Any violation of the points mentioned above will cause PECB irreparable damage for which no monetary remedy can make up. Therefore, PECB can take the appropriate actions to remedy or prevent any unauthorized disclosure or misuse of exam materials, including obtaining an immediate injunction.
PECB will take action against individuals that violate the rules and policies, including permanently banning them 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.

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.

Candidates that disagree with the results may request a re-evaluation by writing to examination.team@pecb.com within 30 days of receiving the results. Re-evaluation requests received after 30 days will not be processed. If candidates do not agree with the results of the reevaluation, they have 30 days from the date they received the reevaluated exam results to file a complaint through the PECB Ticketing System. Any complaint 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 date the coupon code is received (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: when scheduling the exam retake, use initial coupon code to waive the fee
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.

SECTION III: CERTIFICATION PROCESS AND REQUIREMENTS

PECB ISO/IEC 27002 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 27002 scheme have the following requirements:

Credential	Education	Exam	Professional experience	Information security management experience	Other requirements
PECB Certified ISO/IEC 27002 Provisional Manager	At least secondary education	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

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 educational and professional requirements need to be fulfilled in order to obtain a PECB certification. Candidates are required to fill out the online certification application form (that can be accessed via their PECB account), including contact details of individuals who will be contacted to validate the candidates' professional experience. Candidates can submit their application in English, French, German, Spanish or Korean languages. 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. For more information about downloading the certificate, click here, and for more information about claiming the Digital Badge, click here.

PECB provides support both in English and French.

Professional experience

Candidates must provide complete and correct information regarding their professional experience, including job title(s), start and end date(s), job description(s), and more. Candidates are advised to summarize their previous or current assignments, providing sufficient details to describe the nature of the responsibilities for each job. More detailed information can be included in the résumé.

Professional references

For each application, two professional references are required. They must be from individuals who have worked with the candidate in a professional environment and can validate their information security management experience, as well as their current and previous work history. Professional references of persons who fall under the candidate's supervision or are their relatives are not valid.

Information security management 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.

SECTION IV: CERTIFICATION POLICIES

Denial of certification

PECB can deny certification/certificate program if candidates:

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

Candidates whose certification/certificate program has been denied can file a complaint through the complaints and appeals procedure. For more detailed information, refer to **Complaint and Appeal Policy** section.

The application payment for the certification/certificate program is nonrefundable.

Certification status options

Active

Means that your certification is in good standing and valid, and it is being maintained by fulfilling the PECB requirements regarding the CPD and AMF.

Suspended

PECB can temporarily suspend candidates' certification if they fail to meet the requirements. Other reasons for suspending certification include:

- 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.

Revoked

PECB can revoke (that is, to withdraw) the certification if the candidate fails to satisfy its requirements. In such cases, candidates are no longer allowed to represent themselves as PECB Certified Professionals. Additional reasons for revoking certification can be if the candidates:

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

Candidates whose certification has been revoked can file a complaint through the complaints and appeals procedure. For more detailed information, refer to **Complaint and Appeal Policy** section.

Other statuses

Besides being active, suspended, or revoked, a certification can be voluntarily withdrawn or designated as Emeritus. To learn more about these statuses and the permanent cessation status, go to Certification Status Options.

Upgrade and downgrade of credentials

Upgrade of credentials

Professionals can upgrade their credentials as soon as they can demonstrate that they fulfill the requirements.

To apply for an upgrade, candidates need to log into their PECB account, visit the “My Certifications” tab, and click on “Upgrade.” The upgrade application fee is $100.

Downgrade of credentials

A PECB Certification can be downgraded to a lower credential due to the following reasons:

- The AMF has not been paid.
- The CPD hours have not been submitted.
- Insufficient CPD hours have been submitted.
- Evidence on CPD hours has not been submitted upon request.

Note: *PECB certified professionals who hold Lead certifications and fail to provide evidence of certification maintenance requirements will have their credentials downgraded. The holders of Master Certifications who fail to submit CPDs and pay AMFs will have their certifications revoked.*

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 ($120). 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 complaints must be made no later than 30 days after receiving the certification decision. PECB will provide a written response to the candidate within 30 working days after receiving the complaint. If candidates do not find the response satisfactory, they have the right to file an appeal.

For more information about the Complaint and Appeal Policy, click here.

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 27002 Lead Manager 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.

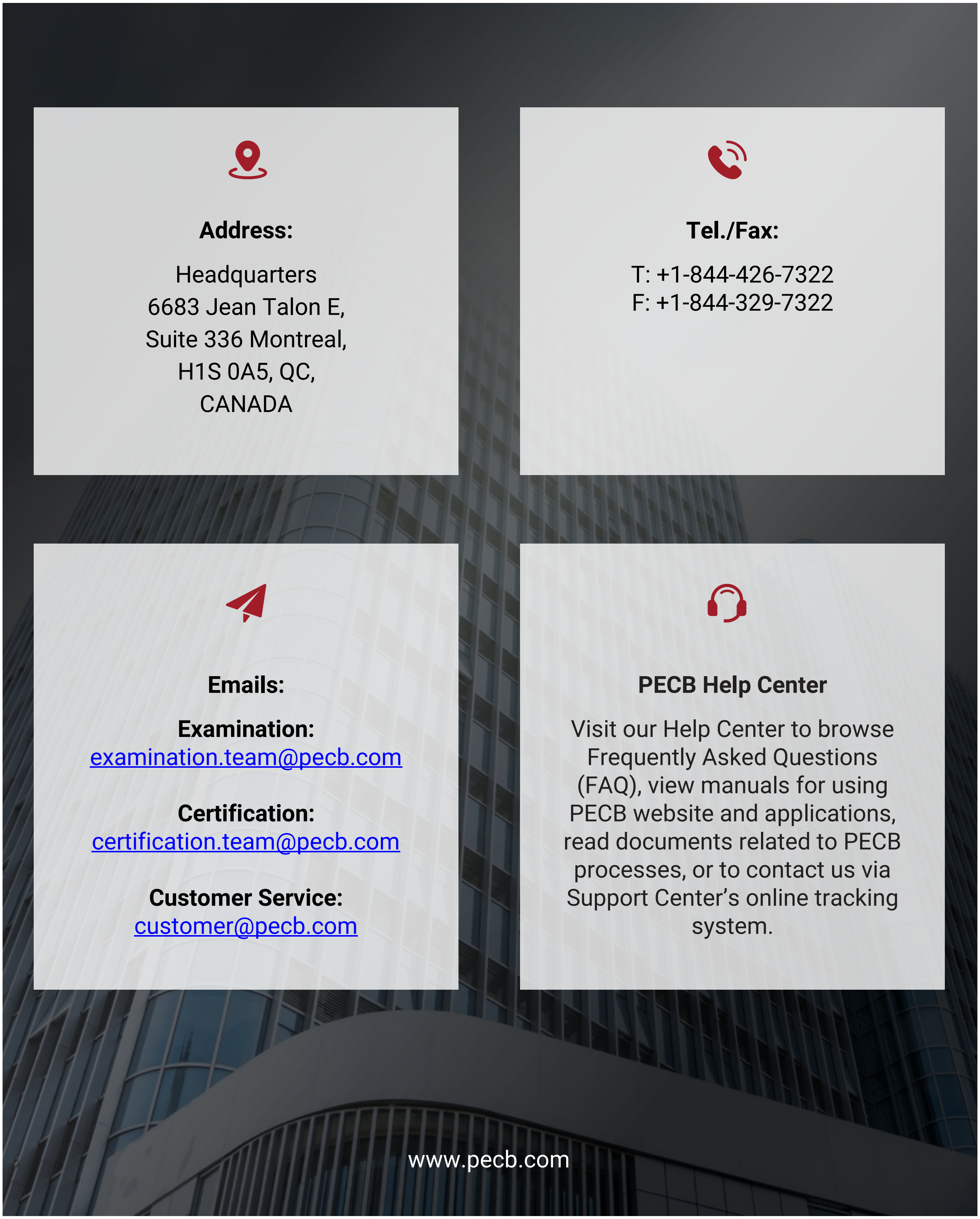
The purpose of this Policy is to ensure that PECB is managing unacceptable behavior of external stakeholders towards PECB staff in an impartial, confidential, fair, and timely manner. To read the Behavior Policy, click here.

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

Tel./Fax:

T: +1-844-426-7322
F: +1-844-329-7322

Emails:

Examination:
examination.team@pecb.com

Certification:
certification.team@pecb.com

Customer Service:
customer@pecb.com

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.

www.pecb.com