PECB BEYOND RECOGNITION

Candidate Handbook

ISO/IEC 27002 LEAD MANAGER

PECB

Table of Contents

SECTION I: INTRODUCTION

About PECB

PECB is a certification body which provides education[1] and certification in accordance with ISO/IEC 17024 for individuals on a wide range of disciplines.

We help professionals show commitment and competence by providing them with valuable evaluation and certification services against internationally recognized standards. Our mission is to provide services that inspire trust and continual improvement, demonstrate recognition, and benefit the society as a whole.

The key objectives of PECB are:

1. Establishing the minimum requirements necessary to certify professionals
2. Reviewing and verifying the qualifications of applicants to ensure they are eligible to apply for certification
3. Developing and maintaining reliable certification evaluations
4. Granting certifications to qualified candidates, maintaining records, and publishing a directory of the holders of a valid certification
5. Establishing requirements for the periodic renewal of certification and ensuring compliance with those requirements
6. Ensuring that candidates meet ethical standards in their professional practice
7. Representing its members, where appropriate, in matters of common interest
8. Promoting the benefits of certification to organizations, employers, public officials, practitioners in related fields, and the public

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

The Value of PECB Certification

Why Choose PECB as Your Certification Body?

Global Recognition
Our certifications are internationally recognized and accredited by the International Accreditation Service (IAS); signatory of IAF Multilateral Recognition Arrangement (MLA) which ensures mutual recognition of accredited certification between signatories to the MLA and acceptance of accredited certification in many markets. Therefore, professionals who pursue a PECB certification credential will benefit from PECB's recognition in domestic and international markets.

Competent Personnel
The core team of PECB consists of competent individuals who have relevant sector-specific experience. All of our employees hold professional credentials and are constantly trained to provide more than satisfactory services to our clients.

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

Customer Service
We are a customer-centered company and treat all our customers with value, importance, professionalism, and honesty. PECB has a team of experts dedicated to support customer requests, problems, concerns, needs, and opinions. We do our best to maintain a 24-hours maximum response time without compromising the quality of the service.

PECB Code of Ethics

PECB professionals will:

1. Conduct themselves professionally, with honesty, accuracy, fairness, responsibility, and independence
2. Act at all times solely in the best interest of their employer, their clients, the public, and the profession, by adhering to the professional standards and applicable techniques while offering professional services
3. Maintain competency in their respective fields and strive to constantly improve their professional capabilities
4. Offer only professional services for which they are qualified to perform, and adequately inform clients about the nature of the proposed services, including any relevant concerns or risks
5. Inform each employer or client of any business interests or affiliations that might influence their judgment or impair their fairness
6. Treat in a confidential and private manner the information acquired during professional and business dealings of any present or former employer or client
7. Comply with all laws and regulations of the jurisdictions where professional activities are conducted
8. Respect the intellectual property and contributions of others
9. Not, intentionally or otherwise, communicate false or falsified information that may compromise the integrity of the evaluation process of a candidate for a professional designation
10. Not act in any manner that could compromise the reputation of PECB or its certification programs
11. Fully cooperate on the inquiry following a claimed infringement of this Code of Ethics

The full version of the PECB Code of Ethics can be downloaded here.

Introduction to ISO/IEC 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.

It is important to understand that PECB certifications are not a license or simply a membership. They represent peer recognition that an individual has demonstrated proficiency in, and comprehension of, a set of competences. PECB certifications are awarded to candidates that can demonstrate experience and have passed a standardized exam in the certification area.

This document specifies the PECB ISO/IEC 27002 Lead Manager certification scheme in compliance with ISO/IEC 17024:2012. This candidate handbook also contains information about the process by which candidates may earn and maintain their credentials. It is very important that you read all the information included in this candidate handbook before completing and submitting your application. If you have questions after reading it, please contact the PECB international office at certification@pecb.com.

SECTION II: PECB CERTIFICATION PROCESS AND EXAMINATION PREPARATION, RULES, AND POLICIES

Decide Which Certification Is Right for You

All PECB certifications have specific education and professional experience requirements. To determine the right credential for you, verify the eligibility criteria for various certifications and your professional needs.

Prepare and Schedule the Exam

All candidates are responsible for their own study and preparation for certification exams. No specific set of training courses or curriculum of study is required as part of the certification process. Nevertheless, attending a training course can significantly increase candidates' chances of successfully passing a PECB exam.

To schedule an exam, candidates have two options:

1. Contact one of our partners who provide training courses and exam sessions. To find a training course provider in a particular region, candidates should go to Active Partners. The PECB training course schedule is also available on Training Events.
2. Take a PECB exam remotely from their home or any location they desire through the PECB Exam application, which can be accessed here: Exam Events.

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

Application Fees for Examination and Certification

PECB offers direct exams, where a candidate can sit for the exam without attending the training course. The applicable prices are as follows:

- Lead Exam: $1000
- Manager Exam: $700
- Foundation and Transition Exam: $500

The application fee for certification is $500.

For all candidates that have followed the training course and taken the exam with one of PECB's partners, the application fee includes the costs associated with examination, application for certification, and the first year of Annual Maintenance Fee (AMF) only.

Competency Domains

The objective of the "PECB Certified 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.

This training course 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 exam covers the following competency domains:

- **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

PECB

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

PECB

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

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

Knowledge statements

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 management of information security in the ICT supply chain

information security awareness and training programs 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	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

PECB

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

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

Knowledge statements

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

applications throughout their development life cycle 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

PECB

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

1. Ability to understand and implement the guidelines of ISO/IEC 27002 for testing information security
2. Ability to understand and implement the guidelines of ISO/IEC 27002 for ensuring information security of outsourced services
3. Ability to understand and implement the guidelines of ISO/IEC 27002 for protecting the production environment
4. Ability to understand and implement the guidelines of ISO/IEC 27002 for protecting test information
5. Ability to understand and implement the guidelines of ISO/IEC 27002 for protecting information systems during audit testing
6. Ability to perform independent reviews of information security based on the guidelines of ISO/IEC 27002
7. Ability to understand and implement best practices for network monitoring
8. Ability to understand and implement continual improvement processes based on the guidelines of ISO/IEC 27002
9. Ability to select and implement the appropriate approaches for maintaining information security based on the guidelines of ISO/IEC 27002

Knowledge statements

1. Knowledge of the ISO/IEC 27002 guidelines regarding the stages of software testing life cycle and best security testing techniques and tools
2. Knowledge of the monitoring and review activities related to outsourced system development based on the guidelines of ISO/IEC 27002
3. Knowledge of the ISO/IEC 27002 guidelines regarding software development environments including development, staging, and production
4. Knowledge of the ISO/IEC 27002 guidelines that address the risks of unauthorized access to or use of test information
5. Knowledge of the ISO/IEC 27002 guidelines that address the protection of information systems during audit testing
6. Knowledge of the ISO/IEC 27002 guidelines for reviewing information security
7. Knowledge of the network monitoring techniques
8. Knowledge of the best approaches used to monitor the effectiveness of information security controls
9. Knowledge of the ISO/IEC 27002 guidelines regarding continual improvement activities

Based on the abovementioned domains and their relevance, 80 questions are included in the exam, as summarized in the table below:

				Level of understanding (Cognitive/Taxonomy) required	
		Number of questions/points per competency domain	% of the exam devoted/points to/for each competency domain	Questions that measure comprehension, application, and analysis	Questions that measure synthesis and evaluation
Competency domains	Fundamental principles and concepts of 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 the "PECB Certified ISO/IEC 27002 Lead Manager" credential depending on their level of experience.

PECB

Taking the Exam

General Information on the Exam

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

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

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 detailed information about the online format, please refer 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 contains multiple choice questions: This format has been chosen because it has proven to be effective and efficient for measuring and assessing learning outcomes related to the defined competency domains. The multiple-choice exam can be used to evaluate a candidate's understanding on many subjects, including both simple and complex concepts. When answering these questions, candidates will have to apply various principles, analyze problems, evaluate alternatives, combine several concepts or ideas, etc. The multiple-choice questions are scenario based, which means they are developed based on a scenario that candidates are asked to read and are expected to provide answers to one or more questions related to that scenario. This multiple-choice exam is "open book", due to the context-dependent characteristic of the questions. You will find a sample of exam questions provided below.

Since the exam is "open book," candidates are authorized to use the following reference materials:
- A hard copy of the ISO/IEC 27002 standard
- Training course materials (accessed through 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

Any attempt to copy, collude, or otherwise cheat during the exam session will lead to automatic failure.

PECB exams are available in English and other languages. To learn if the exam is available in a particular language, please contact examination@pecb.com.

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

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

Sample Exam Questions

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

Receiving the Exam Results

Exam results will be communicated via email. The only possible results are *pass* and *fail*; no specific grade will be included.

- The time span for the communication starts from the exam date and lasts two to four weeks for multiple-choice paper-based exams.
- For online multiple-choice exams, candidates receive their results instantly.

Candidates who successfully complete the exam will be able to apply for one of the credentials of the respective certification scheme.

For candidates who fail the exam, a list of the domains where they have performed poorly will be added to the email to help them prepare better for a retake.

Candidates that disagree with the results may request a re-evaluation by writing to results@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 allowed time span between exam retakes.

- If a candidate does not pass the exam on the 1st attempt, they must wait 15 days from the initial date of the exam for the next attempt (1st retake). Retake fees apply.
  Note: *Candidates who have completed the training course but failed the exam are eligible to retake the exam once for free within a 12-month period from the initial date of the exam*.
- If a candidate does not pass the exam on the 2nd attempt, they must wait three months after the initial date of the exam for the next attempt (2nd retake). Retake fees apply.
  Note: For candidates that fail the exam in the 2nd retake, PECB recommends them to attend a training course in order to be better prepared for the exam.
- If a candidate does not pass the exam on the 3rd attempt, they must wait six months after the initial date of the exam for the next attempt (3rd retake). Retake fees apply.
- After the 4th attempt, the waiting period for further retake exams is 12 months from the date of the last attempt. Retake fees apply.

To arrange exam retakes (date, time, place, costs), candidates need to contact the PECB Partner/Distributor who has initially organized the session.

Exam Security

A significant component of a professional certification credential is maintaining the security and confidentiality of the exam. PECB relies upon the ethical behavior of certification holders and applicants to maintain the security and confidentiality of PECB exams. Any disclosure of information about the content of PECB exams is a direct violation of PECB's Code of Ethics. PECB will take action against any individuals that violate such rules and policies, including permanently banning individuals from pursuing PECB credentials

and revoking any previous ones. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

Reschedule the Exam

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

Apply for Certification

All candidates who successfully pass the exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credentials they were examined for. Specific educational and professional requirements need to be fulfilled in order to obtain a PECB certification. Candidates are required to fill out the online certification application form (that can be accessed via their PECB online profile), including contact details of references who will be contacted to validate the candidate's professional experience. Candidates can submit their application in various languages. Candidates can choose to either pay online or be billed. For additional information, contact certification@pecb.com.

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

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

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

The application is approved as soon as the Certification Department validates that the candidate fulfills all the certification requirements regarding the respective credential. An email will be sent to the email address provided during the application process to communicate the application status. If approved, candidates will then be able to download the certification from their PECB Account.

PECB provides support in both English and French.

Renew your Certification

PECB certifications are valid for three years. To maintain them, candidates must demonstrate every year that they are still performing tasks that are related to the certification. PECB certified professionals must annually provide Continual Professional Development (CPD) credits and pay $100 as the Annual Maintenance Fee (AMF) to maintain the certification. For more information, please visit the Certification Maintenance page on the PECB website.

Closing a Case

If candidates do not apply for certification within three years, their case will be closed. Even though the certification period expires, candidates have the right to reopen their case. However, PECB will no longer be responsible for any changes regarding the conditions, standards, policies, and candidate handbook that were applicable before the case was closed. A candidate requesting their case to reopen must do so in writing and pay the required fee.

PECB

SECTION III: CERTIFICATION REQUIREMENTS

ISO/IEC 27002 Lead Manager

The requirements for PECB ISO/IEC 27002 Manager certifications are:

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	PECB Certified ISO/IEC 27002 Lead Manager exam or equivalent	Two years: One year of work experience in information security management	Project activities: a total of 200 hours	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27002 Lead Manager	PECB Certified ISO/IEC 27002 Lead Manager exam or equivalent	Five years: Two years of work experience in information security management	Project activities: a total of 300 hours	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27002 Senior Lead Manager	PECB Certified ISO/IEC 27002 Lead Manager exam or equivalent	Ten years: Seven years of work experience in information security management	Project activities: a total of 1,000 hours	Signing the PECB Code of Ethics

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

PECB

SECTION IV: CERTIFICATION RULES AND POLICIES

Professional References

For each application, two professional references are required. They must be from individuals who have worked with the candidate in a professional environment and can validate their information security 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.

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.

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 candidate's eligibility for certification. A candidate whose application is being reviewed will be notified in writing and, if necessary, given a reasonable time frame to provide any additional documentation. If a candidate does not respond by the deadline or does not provide the required documentation within the given time frame, the Certification Department will validate the application based on the initial information provided, which can eventually lead to its downgrade to a lower credential.

Denial of Certification

PECB can deny certification if candidates:

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

For more detailed information, refer to "Complaint and Appeal" section.

The application payment for the certification is non-refundable.

Suspension of Certification

PECB can temporarily suspend certification if the candidate fails to satisfy the requirements. Other reasons for suspending certification include:

- PECB receives large amounts of or serious complaints by interested parties (Suspension will be applied until the investigation has been completed.).
- The logos of PECB or accreditation bodies are intentionally misused.
- The candidate fails to correct the misuse of a certification mark within the time frame determined by PECB.
- The certified individual has voluntarily requested a suspension.
- PECB deems appropriate other conditions for suspension of certification.

Revocation of Certification

PECB can revoke certification if the candidate fails to fulfill the PECB requirements. Candidates are then no longer allowed to represent themselves as PECB certified professionals. Other reasons for revoking certification can be if candidates:

- Violate the PECB Code of Ethics
- Misrepresent and provide false information of the scope of the certification
- Break any other PECB rules

Upgrade of Credentials

Professionals can apply to upgrade to a higher credential as soon as they can demonstrate that they fulfil the requirements.

In order to apply for an upgrade, candidates need to login in to their PECB Account, visit the "My Certifications" tab, and click on the "Upgrade" link. The upgrade application fee is $100.

Downgrade of Credentials

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

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

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

Other Statuses

Besides being active, suspended, or revoked, a certification can be voluntarily withdrawn or designated as Emeritus. More information about these statuses and the permanent cessation status, and how to apply, please visit Certification Status Options.

SECTION V: PECB GENERAL POLICIES

PECB Code of Ethics

Adherence to the PECB Code of Ethics is a voluntary engagement. It is important that PECB certified professionals not only adhere to the principles of this Code, but also encourage and support the same from others. More information can be found here.

Other Exams and Certifications

PECB accepts certifications and exams from other recognized accredited certification bodies. PECB will evaluate the requests through its equivalence process to decide whether the respective certification(s) or exam(s) can be accepted as equivalent to the respective PECB certification (e.g., ISO/IEC 27001 Lead Auditor certification).

Non-discrimination and Special Accommodations

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

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations for candidates, when appropriate. If candidates need special accommodations because of a disability or a specific physical condition, they should inform the Partner/Distributor in order for them to make proper arrangements. Any information candidates provide regarding their disability/need will be treated with strict confidentiality.

Click here to download the Candidates with Disabilities Form.

Complaints and Appeals

Any complaints must be made no later than 30 days after receiving the certification decision. PECB will provide a written response to the candidate within 30 working days after receiving the complaint. If they do not find the response satisfactory, the candidate has the right to file an appeal. For more information about the complaints and appeal procedures, click here.

(1) According to ADA, the term "reasonable accommodation" may include: (A) making existing facilities used by employees readily accessible to and usable by individuals with disabilities; and (B) job restructuring, part-time or modified work schedules, reassignment to a vacant position, acquisition or modification of equipment or devices, appropriate adjustment or modifications of examinations, training materials or policies, the provision of qualified readers or interpreters, and other similar accommodations for individuals with disabilities.

(2) ADA Amendments Act of 2008 (P.L. 110-325) Sec. 12189. Examinations and courses. [Section 309]: Any person that offers examinations or courses related to applications, licensing, certification, or credentialing for secondary or post-secondary education, professional, or trade purposes shall offer such examinations or courses in a place and manner accessible to persons with disabilities or offer alternative accessible arrangements for such individuals.

Address:
Headquarters
6683 Jean Talon E,
Suite 336 Montreal,
H1S 0A5, QC,
CANADA

Tel./Fax.
T: +1-844-426-7322
F: +1-844-329-7322

PECB Help Center
Visit our Help Center to browse Frequently Asked Questions (FAQ), view manuals for using PECB website and applications, read documents related to PECB processes, or to contact us via Support Center's online tracking system.

Emails:
Examination: examination@pecb.com
Certification: certification@pecb.com
Customer Service: customer@pecb.com