PECB BEYOND RECOGNITION

Candidate Handbook

ISO/IEC 27001 LEAD AUDITOR

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 applicant 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 27001 Lead Auditor

ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). The most important skills required in the market are the ability to effectively plan and perform audits in conformance with the certification process of ISO/IEC 27001, master audit techniques, and manage (or be part of) ISMS audit teams and programs.

In addition to the implementation of the ISMS, organizations need assurance that the controls or processes they have implemented produce effective results. Auditing enables organizations to evaluate the effectiveness of the ISMS in place and further improve it.

The "ISO/IEC 27001 Lead Auditor" credential is a professional certification for individuals aiming to demonstrate the competence to audit an information security management system and lead an ISMS audit team.

Considering that auditing is one of the most in-demand professions, an internationally recognized certification can help you exploit your career potential and reach your professional objectives.

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 27001 Lead Auditor 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.

PECB

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 27001 Lead Auditor" exam is to ensure that the candidate has the necessary competence to perform an information security management system (ISMS) audit in compliance with the ISO/IEC 27001 standard requirements, manage an audit team by applying widely recognized audit principles, procedures, and techniques, and, lastly, plan and carry out internal and external audits as per the guidelines of ISO 19011 and in compliance with the ISO/IEC 17021-1 certification processes.

The ISO/IEC 27001 Lead Auditor certification is intended for:

- Auditors seeking to perform and lead information security management system (ISMS) audits

- Managers or consultants seeking to master the information security management system audit process
- Individuals responsible for maintaining conformity with the ISMS requirements in an organization
- Technical experts seeking to prepare for an information security management system audit
- Expert advisors in information security management

The content of the exam is divided as follows:

- **Domain 1:** Fundamental principles and concepts of an information security management system (ISMS)
- **Domain 2:** Information security management system (ISMS)
- **Domain 3:** Fundamental audit concepts and principles
- **Domain 4:** Preparing an ISO/IEC 27001 audit
- **Domain 5:** Conducting an ISO/IEC 27001 audit
- **Domain 6:** Closing an ISO/IEC 27001 audit
- **Domain 7:** Managing an ISO/IEC 27001 audit program

Domain 1: Fundamental principles and concepts of an information security management system (ISMS) **Main objective:** Ensure that the candidate understands and is able to interpret ISO/IEC 27001 principles and concepts	
Competencies	**Knowledge statements**
1. Ability to understand and explain the main concepts of the information security management system 2. Ability to understand and explain the organization's operations and the development of information security standards 3. Ability to identify, analyze, and evaluate the information security compliance requirements for an organization 4. Ability to explain and illustrate the main concepts in information security and information security risk management 5. Ability to distinguish and explain the difference between information asset, data and record 6. Ability to understand, interpret, and illustrate the relationship between information security aspects such as controls, vulnerabilities, threats, risks, and assets 7. Ability to identify and illustrate big data, artificial intelligence, machine learning, cloud computing, and outsourcing operations	1. Knowledge of the information security laws, regulations, international and industry standards, contracts, market practices, internal policies, etc., an organization must comply with 2. Knowledge of the main standards related to information security 3. Knowledge the main concepts and terminology of ISO/IEC 27001 4. Knowledge of the concept of risk and its application in information security 5. Knowledge of the relationship between information security aspects 6. Knowledge of the difference and characteristics of security objectives and controls 7. Knowledge of the difference between preventive, detective, and corrective controls 8. Knowledge of the main characteristics of big data, artificial intelligence, machine learning, cloud computing, and outsourcing operations

Domain 2: Information security management system (ISMS) and ISO/IEC 27001 requirements

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

Competencies	Knowledge statements
1. Ability to understand the structure of the ISO/IEC 27001:2022 standard	1. Knowledge of the ISO/IEC 27001:20022 standard and its supporting standards
2. Ability to understand the components of an information security management system based on ISO/IEC 27001 and its principal processes	2. Knowledge of the concepts, principles and terminology related to management systems
3. Ability to understand, interpret, and analyze the requirements of ISO/IEC 27001	3. Knowledge of the principal characteristics of an integrated management system
4. Ability to understand, explain, and illustrate the main steps to establish, implement, operate, monitor, review, maintain, and improve an organization's ISMS	4. Knowledge of the ISO/IEC 27001 requirements presented in the clauses 4 to 10
5. Ability to establish the external and internal factors related to the ISMS and determine the interested parties and their needs	5. Knowledge of the 93 controls listed in ISO/IEC 27001 Annex A
6. Ability to determine the scope of the ISMS	6. Knowledge of the ISMS internal and external factors and interested parties
7. Ability to ensure management commitment, establish an information security policy, and assign the ISMS roles and responsibilities	7. Knowledge of the main steps to establish the ISMS scope and information security policy
8. Ability to plan changes and the actions to address risks	8. Knowledge of the top management's leadership and commitment and the organizational roles and responsibilities related to the ISMS
9. Ability to understand the risk assessment and risk treatment processes	9. Knowledge of security objectives, processes and procedures relevant to managing risks, and improving information security to deliver results in accordance with an organization's overall policies and objectives
10. Ability to understand the selection of appropriate controls based upon Annex A of ISO/IEC 27001	10. Knowledge of risk assessment and treatment approaches and methodologies
11. Ability to ensure that employees are aware and competent to perform their ISMS related tasks	11. Knowledge of the selection of Annex A controls and their inclusion in the Statement of Applicability
12. Ability to monitor and evaluate the performance of the ISMS and conduct internal audits and management reviews	12. Knowledge of the performance evaluation process including monitoring, measurement, analysis and evaluation, internal audit, and management review
13. Ability to ensure continual improvement and implement appropriate actions to treat nonconformities	13. Knowledge of the concept of continual improvement and its application to an ISMS

PECB

Domain 3: Fundamental audit concepts and principles **Main objective:** Ensure that the candidate understands and is able to interpret and apply the main concepts and principles related to a ISMS audit	
Competencies	**Knowledge statements**
1. Ability to understand, explain, and illustrate the application of the audit principles in an ISMS audit 2. Ability to differentiate first, second, and third party audits 3. Ability to identify and judge situations that would discredit the professionalism of the auditor and violate the PECB Code of Ethics 4. Ability to identify and judge ethical issues considering the obligations related to the audit client, auditee, law enforcement, and regulatory authorities 5. Ability to understand the legal implications related to any irregularities committed by the auditee 6. Ability to explain, illustrate, and apply the audit evidence approach in the context of an ISMS audit 7. Ability to explain and compare evidence types and their characteristics 8. Ability to determine and justify the type and amount of evidence required in an ISMS audit 9. Ability to understand the impact of trends and technology in auditing	1. Knowledge of the main audit concepts and principles as described in ISO 19011 2. Knowledge of the differences between first, second, and third party audits 3. Knowledge of the principles of auditing such as integrity, fair presentation, due professional care, confidentiality, independence, evidence-based approach, and risk-based approach 4. Knowledge of an auditor's professional responsibility and the PECB Code of Ethics 5. Knowledge of evidence-based approach in an audit 6. Knowledge of the different types of audit evidence such as physical, mathematical, confirmative, technical, analytical, documentary, and verbal 7. Knowledge of the laws and regulations applicable to the auditee and the country it operates in 8. Knowledge of the use of big data in audits 9. Knowledge of the auditing of outsourced operations

PECB

Domain 4: Preparing an ISO/IEC 27001 audit

Main objective: Ensure that the candidate is able to prepare an information security management system audit

Competencies	Knowledge statements
1. Ability to understand and illustrate the steps and activities to prepare an ISMS audit considering the specific context of the audit 2. Ability to determine and evaluate the level of materiality and apply the risk-based approach during the different stages of an ISMS audit 3. Ability to judge the appropriate level of reasonable assurance needed for an ISMS audit 4. Ability to understand and explain the roles and responsibilities of the audit team leader, audit team members, and technical experts 5. Ability to determine the audit feasibility 6. Ability to determine, evaluate, and confirm the audit objectives, the audit criteria, and the audit scope for an ISMS audit 7. Ability to explain, illustrate, and define the characteristics of the terms of the audit engagement and apply the best practices to establish the initial contact with an auditee	1. Knowledge of the audit plan preparation procedure 2. Knowledge of the risk-based approach to an audit and the different types of risks related to audit activities such as inherent risk, control risk, and detection risk 3. Knowledge of the concept of materiality and its application to an audit 4. Knowledge of the concept of reasonable assurance and its application to an audit 5. Knowledge of the main responsibilities of the audit team leader, audit team members, and technical experts 6. Knowledge of the audit objectives, audit scope, and audit criteria 7. Knowledge of the difference between an ISMS scope and the audit scope 8. Knowledge of the factors to take into account during the audit feasibility 9. Knowledge of the cultural aspects to consider in an audit 10. Knowledge of the characteristics of terms of the audit engagement and the best practices to establish the initial contact with an auditee

Domain 5: Conducting an ISO/IEC 27001 audit

Main objective: Ensure that the candidate can efficiently conduct an ISMS audit

Competencies	Knowledge statements
1. Ability to conduct the stage 1 audit, taking into account the documented information evaluation criteria	1. Knowledge of the objectives and the content of the opening meeting in an audit
2. Ability to organize and conduct an opening meeting	2. Knowledge of the difference between stage 1 audit and stage 2 audit
3. Ability to conduct the stage 2 audit by appropriately following the procedures that this stage entails	3. Knowledge of stage 1 audit requirements, steps, and activities
4. Ability to apply the best practices of communication to collect the appropriate audit evidence	4. Knowledge of the documented information evaluation criteria and ISO/IEC 27001 requirements
5. Ability to consider the roles and responsibilities of all the interested parties involved	5. Knowledge of stage 2 audit requirements, steps, and activities
6. Ability to explain, illustrate, and apply evidence collection procedures and tools	6. Knowledge of the best communication practices during an audit
7. Ability to explain, illustrate, and apply the main audit sampling methods	7. Knowledge of the roles and responsibilities of guides and observers during an audit
8. Ability to gather appropriate evidence from the available information during an audit and evaluate it objectively	8. Knowledge of the different conflict resolution techniques
9. Ability to develop audit working papers and elaborate appropriate audit test plans in an ISMS audit	9. Knowledge of the evidence collection procedures and tools such as interview, documented information review, observation, analysis, sampling and technical verification
10. Ability to explain and apply the evidence evaluation process of drafting audit findings	10. Knowledge of the evidence analysis techniques of corroboration and evaluation
11. Ability to understand, explain, and illustrate the concept of the benefit of the doubt	11. Knowledge of the main concepts, principles, and evidence collection procedures used in an audit
12. Ability to report appropriate audit observations in accordance with audit rules and principles	12. Knowledge of the advantages and disadvantages of using audit checklists
13. Ability to conduct quality reviews to audit documentation	13. Knowledge of the main audit sampling methods and their characteristics
14. Ability to complete audit working documents	14. Knowledge of the audit plan preparation procedure
	15. Knowledge of the preparation and development of audit working papers
	16. Knowledge of the best practices for the creation of audit test plans
	17. Knowledge of the evidence evaluation process to draft audit findings

PECB

Domain 6: Closing an ISO/IEC 27001 audit **Main objective:** Ensure that the candidate is able to conclude an ISMS audit and conduct audit follow-up activities	
Competencies	**Knowledge statements**
1. Ability to explain and apply the evidence evaluation process of preparing audit conclusions 2. Ability to justify the recommendation for certification 3. Ability to draft and present audit conclusions 4. Ability to organize and conduct a closing meeting 5. Ability to write and distribute an ISO/IEC 27001 audit report 6. Ability to evaluate action plans	1. Knowledge of the evidence evaluation process of preparing audit conclusions 2. Knowledge of presenting audit conclusions 3. Knowledge of the guidelines and best practices to present audit conclusions to the management of an audited organization 4. Knowledge of the possible recommendations that an auditor can issue during the certification audit 5. Knowledge of the closing meeting agenda 6. Knowledge of the guidelines and best practices to evaluate action plans

PECB

Domain 7: Managing an ISO/IEC 27001 audit program

Main objective: Ensure that the candidate understands how to establish and manage an ISMS audit program

Competencies	Knowledge statements
1. Ability to conduct the activities following an initial audit, including audit follow-ups and surveillance activities 2. Ability to understand and explain the establishment of an audit program and the application of the PDCA cycle into an audit program 3. Ability to understand and explain the importance of protecting the integrity, availability, and confidentiality of audit records and the auditors' responsibilities in this regard 4. Ability to understand and explain the responsibilities to protect the integrity, availability and confidentiality of audit records 5. Ability to understand the requirements related to the components of the management system of an audit program as quality management, record management, complaint management 6. Ability to understand and explain the way that the combined audits are handled in an audit program 7. Ability to understand the documented information management process 8. Ability to understand the process of evaluating the efficiency of the audit program by monitoring the performance of each auditor and audit team member 9. Ability to demonstrate the application of the personal attributes and behaviors associated with professional auditors	1. Knowledge of audit follow-ups, surveillance audits, and recertification audit requirements, steps, and activities 2. Knowledge of the conditions for the modification, extension, suspension, or withdrawal of an organization's certification 3. Knowledge of the application of the PDCA cycle in the management of an audit program 4. Knowledge of the requirements, guidelines, and best practices regarding audit resources, procedures, and policies 5. Knowledge of the types of tools used by professional auditors 6. Knowledge of the requirements, guidelines, and best practices regarding the management of audit records 7. Knowledge of the application of the continual improvement concept to the management of an audit program 8. Knowledge of the particularities to implement and manage a first, second or third party audit program Knowledge of the competency concept and its application to auditors 9. Knowledge of the management of combined audits 10. Knowledge of the personal attributes and behaviors of a professional auditor

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 an information security management system (ISMS)	13	16.25	X	
	Information security management system (ISMS)	8	10	X	
	Fundamental audit concepts and principles	14	17.5		X
	Preparing an ISO/IEC 27001 audit	12	15	X	
	Conducting an ISO/IEC 27001 audit	18	22.5		X
	Closing an ISO/IEC 27001 audit	7	8.75	X	
	Managing an ISO/IEC 27001 audit program	8	10		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 27001 Lead Auditor" credential depending on their level of experience.

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 27001 standard
- Training course materials (accessed through PECB Exams app and/or printed)
- Any personal notes 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

Company A is an insurance company headquartered in Chicago. It offers various range of services and products involving medical and car insurance. The company has recently become one of the most successful and largest insurance companies with more than 70 offices nationwide.

The company's objectives are to properly maintain their assets and protect the confidentiality of information of their clients. The company decided to get certified against ISO/IEC 27001 since it would help them not only achieve their organizational objectives and comply with international laws and regulations but also increase their reputation. The company initiated the implementation of the ISMS by defining an implementation strategy based on a detailed analysis of their existing processes and the ISMS requirements. The company paid special attention to the information security risk assessment, which was crucial in understanding the threats and vulnerabilities that they faced. They also defined the risk criteria with the aim of evaluating the identified risks.

Company A experienced rapid growth which resulted in complex and intensive data processing, and based on the risk assessment results they decided to initially update their existing information classification scheme and then implement the necessary security controls based on the level of protection required by each classification of information.

The medical claims of their clients, classified as sensitive information, were encrypted using the AES encryption and then moved to the private cloud. *Company A* used cloud storage for its ease of access. Due to the frequent access of its employees to this service, the company also decided to utilize the logging process. The service was configured to automatically grant access to cloud storage for all employees responsible for handling medical claims.

Because the cloud storage services experienced security breaches either from human error or deliberate attacks, the company's IT department decided to restrict the access to sensitive information stored in the cloud if professional business emails were not used. In addition, they used a password manager software to manage the passwords of these email addresses and generate stronger passwords.

Based on this scenario, answer the following questions:

1. **The IT Department did not restrict access to cloud storage. Which of the threats below can exploit such vulnerability?**
   A. Tampering with hardware
   B. **Unauthorized use of sensitive information**
   C. Insufficient cloud storage training

2. ***Company A*** **encrypts sensitive information prior to moving them to the cloud. Which information security principle is followed in this case?**
   A. **Confidentiality, because encryption ensures that only authorized users can access the encrypted information**
   B. Availability, because encryption ensures that information is secured either at rest or in transit, therefore accessible when needed
   C. Integrity, because encryption ensures that only authorized modifications are made to the encrypted information

3. ***Company A*** **decided to restrict the access to sensitive information stored in the cloud if professional business emails were not used. Which security control was implemented in this case?**
   A. Detective control
   B. **Preventive control**
   C. Corrective control

4. ***Company A*** **defined the risk criteria when assessing its risks. Is this necessary?**
   A. **Yes, because the company should establish and maintain the risk criteria when assessing the information security risks**
   B. No, because the risk criteria should be established only when risk treatment options are defined
   C. No, because the risk criteria is established when the information security residual risks are accepted

Receiving the Exam Results

Exam results will be communicated via email.

- 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.

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, s/he 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, because 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.

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 27001 Lead Auditor

The requirements for **PECB ISO/IEC 27001** Auditor certifications are:

Credential	Exam	Professional experience	MS audit/assessment experience	Other requirements
PECB Certified ISO/IEC 27001 Provisional Auditor	PECB Certified ISO/IEC 27001 Lead Auditor exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27001 Auditor	PECB Certified ISO/IEC 27001 Lead Auditor exam or equivalent	Two years: One year of work experience in information security management	Audit activities: a total of 200 hours	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27001 Lead Auditor	PECB Certified ISO/IEC 27001 Lead Auditor exam or equivalent	Five years: Two years of work experience in information security management	Audit activities: a total of 300 hours	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27001 Senior Lead Auditor	PECB Certified ISO/IEC 27001 Lead Auditor exam or equivalent	Ten years: Seven years of work experience in information security management	Audit activities: a total of 1,000 hours	Signing the PECB Code of Ethics

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

1. Planning an audit
2. Managing an audit program
3. Drafting audit reports
4. Drafting nonconformity reports
5. Drafting audit working documents
6. Documented information review
7. On-site audit
8. Following up on nonconformities
9. Leading an audit team

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.

ISMS Audit Experience

The candidate's audit log will be checked to ensure that they have completed the required number of audit hours. The following audit types constitute valid audit experience: pre-audit, internal audits, second party audits, third party audits, or opinion audits.

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