


The logo for PECB, featuring the letters 'PECB' in a bold, white, sans-serif font. The letters are slightly spaced out, and the 'E' and 'C' have a unique, modern design with internal cutouts.

PECB

BEYOND RECOGNITION

A background image showing a modern office environment with large glass windows. In the foreground, a woman in a dark suit and a man in a light suit are walking and looking at a tablet together. The scene is dimly lit, suggesting an evening or indoor lighting.

ISO 28000 LEAD AUDITOR

Candidate Handbook

Table of Contents

SECTION I: INTRODUCTION	3
About PECB	3
The Value of PECB Certification.....	4
PECB Code of Ethics.....	5
Introduction to ISO 28000 Lead Auditor	6
SECTION II: EXAMINATION PREPARATION, RULES, AND POLICIES	7
Preparing for and scheduling the exam.....	7
Competency domains.....	8
Taking the exam.....	18
Exam Security Policy.....	21
Exam results.....	22
Exam Retake Policy.....	22
SECTION III: CERTIFICATION PROCESS AND REQUIREMENTS	23
PECB ISO 28000 credentials	23
Applying for certification	23
Professional experience	24
Professional references	24
SeMS audit experience	24
Evaluation of certification applications	24
SECTION IV: CERTIFICATION POLICIES	25
Denial of certification.....	25
Certification status options	25
Upgrade and downgrade of credentials	26
Renewing the certification.....	26
Closing a case	26
Complaint and Appeal Policy	26
SECTION V: GENERAL POLICIES	27
Exams and certifications from other accredited certification bodies	27
Non-discrimination and special accommodations	27
Behavior Policy.....	27
Refund Policy	27

SECTION I: INTRODUCTION

About PECB

PECB is a certification body that provides education¹, certification, and certificate programs for individuals on a wide range of disciplines.

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

Our key objectives are:

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

Our mission

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

Our vision

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

Our values

Integrity, Professionalism, Fairness

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

The Value of PECB Certification

Global recognition

PECB credentials are internationally recognized and endorsed by many accreditation bodies, so professionals who pursue them will benefit from our recognition in domestic and international markets.

The value of PECB certifications is validated by the accreditation from the International Accreditation Service (IAS-PCB-111), the United Kingdom Accreditation Service (UKAS-No. 21923) and the Korean Accreditation Board (KAB-PC-08) under ISO/IEC 17024 – General requirements for bodies operating certification of persons. The value of PECB certificate programs is validated by the accreditation from the ANSI National Accreditation Board (ANAB-Accreditation ID 1003) under ANSI/ASTM E2659-18, Standard Practice for Certificate Programs.

PECB is an associate member of The Independent Association of Accredited Registrars (IAAR), a full member of the International Personnel Certification Association (IPC), a signatory member of IPC MLA, and a member of Club EBIOS, CPD Certification Service, CLUSIF, Credential Engine, and ITCC. In addition, PECB is an approved Licensed Partner Publisher (LPP) from the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) for the Cybersecurity Maturity Model Certification standard (CMMC), is approved by Club EBIOS to offer the EBIOS Risk Manager Skills certification, and is approved by CNIL (Commission Nationale de l'Informatique et des Libertés) to offer DPO certification. For more detailed information, click [here](#).

High-quality products and services

We are proud to provide our clients with high-quality products and services that match their needs and demands. All of our products are carefully prepared by a team of experts and professionals based on the best practices and methodologies.

Compliance with standards

Our certifications and certificate programs are a demonstration of compliance with ISO/IEC 17024 and ASTM E2659. They ensure that the standard requirements have been fulfilled and validated with adequate consistency, professionalism, and impartiality.

Customer-oriented service

We are a customer-oriented company and treat all our clients with value, importance, professionalism, and honesty. PECB has a team of experts who are responsible for addressing requests, questions, and needs. We do our best to maintain a 24-hour maximum response time without compromising the quality of the services.

Flexibility and convenience

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

PECB Code of Ethics

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

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

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

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

PECB professionals are responsible for:

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

To read the complete version of PECB’s Code of Ethics, go to [Code of Ethics | PECB](#).

Introduction to ISO 28000 Lead Auditor

ISO 28000 specifies the requirements for establishing, implementing, maintaining, and continually improving a security management system (SeMS). It requires organizations to determine the security environment in which they operate (including its supply chain), ensure that security measures are in place to address security risks, ensure conformity to the regulatory, statutory, and voluntary obligations, and ensure the alignment of security processes and controls with their overall objectives. A security management system based on ISO 28000 helps organizations enhance business capabilities and create and protect value.

In addition to the initial implementation of the SeMS, organizations need assurance that the controls and processes they have established as part of the SeMS are achieving the desired outcomes. Auditing is the most effective way in this regard. However, auditing requires skills and abilities to effectively plan and perform it. The ISO 28000 Lead Auditor training course enables you to master the audit techniques and obtain the necessary competencies to effectively audit security management systems based on ISO 28000.

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

This document specifies the PECB ISO 28000 Lead Auditor certification scheme in compliance with ISO/IEC 17024:2012. It also outlines the steps that candidates should take to obtain and maintain their credentials. As such, it is very important to carefully read all the information included in this document before completing and submitting your application. If you have questions or need further information after reading it, please contact the PECB international office at certification.team@pecb.com.

SECTION II: EXAMINATION PREPARATION, RULES, AND POLICIES

Preparing for and scheduling the exam

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

To schedule the exam, candidates have two options:

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

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

Rescheduling the exam

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

Application fees for examination and certification

Candidates may take the exam without attending the training course. The applicable prices are as follows:

- Lead Exam: \$1000²
- Manager Exam: \$700
- Foundation Exam: \$500
- Transition Exam: \$500

The application fee for certification is \$500.

For the candidates that have attended the training course via one of PECB's partners, the application fee covers the costs of the exam (first attempt and first retake), the application for certification, and the first year of Annual Maintenance Fee (AMF).

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

Competency domains

The “ISO 28000 Lead Auditor” credential is a professional certification for individuals aiming to demonstrate the competence to audit a security management system based on ISO 28000 and lead an audit team.

The most important skills required in the market are the ability to effectively plan and perform audits in conformity to the certification process, apply audit techniques and practices, and manage (or be part of) audit teams and audit programs.

The ISO 28000 Lead Auditor certification is intended for:

- Auditors seeking to perform and lead SeMS audits
- Managers or consultants seeking to master the SeMS audit process
- Individuals responsible for maintaining conformity to the SeMS requirements in an organization
- Technical experts seeking to prepare for SeMS audits
- Expert advisors in security management

The content of the exam is divided as follows:

- **Domain 1:** Fundamental principles and concepts of a security management system
- **Domain 2:** Security management system requirements
- **Domain 3:** Fundamental audit concepts and principles
- **Domain 4:** Preparing an ISO 28000 audit
- **Domain 5:** Conducting an ISO 28000 audit
- **Domain 6:** Closing an ISO 28000 audit
- **Domain 7:** Managing an ISO 28000 audit program

Domain 1: Fundamental principles and concepts of a security management system

Main objective: Ensure that the candidate understands and is able to interpret ISO 28000 principles and concepts.

Competencies	Knowledge statements
1. Ability to explain the scope and applicability of ISO 28000	1. Knowledge of ISO 28000 and its applicability
2. Ability to explain the relationship between ISO 28000 and other standards and regulatory frameworks	2. Knowledge of the relationship between ISO 28000 and other standards and regulatory frameworks
3. Ability to communicate the advantages of a security management system based on ISO 28000	3. Knowledge of the benefits of a security management system based on ISO 28000
4. Ability to explain a management system	4. Knowledge of the main components of a management system
5. Ability to explain integrated management systems and how they can help organizations	5. Knowledge of integrated management systems
6. Ability to explain the certification process and the roles and responsibilities of the parties involved in the certification scheme	6. Knowledge of the certification process and the roles and responsibilities of the parties involved in the certification scheme
7. Ability to explain the main concepts of a security management system	7. Knowledge of the main concepts and terminology of ISO 28000
8. Ability to explain supply chain and supply chain management	8. Knowledge of the supply chain and supply chain management
9. Ability to explain security-related terms and definitions	9. Knowledge of the main security-related terms and definitions
10. Ability to explain the principles of security management	10. Knowledge of the security management principles as outlined in ISO 28000
11. Ability to explain security concepts, such as threat, vulnerability, consequence, and likelihood	11. Knowledge of the security concepts, including threat, vulnerability, consequence, and likelihood
12. Ability to establish countermeasures for a security threat scenario	12. Knowledge of the countermeasures for a security threat scenario
13. Ability to explain the process approach and its role	13. Knowledge of the process approach

Domain 2: Security management system requirements

Main objective: Ensure that the candidate understands and is able to interpret and identify the requirements for a security management system based on ISO 28000.

Competencies	Knowledge statements
1. Ability to explain the structure and requirements of ISO 28000	1. Knowledge of the harmonizes structure of ISO and ISO 28000 requirements
2. Ability to interpret ISO 28000 requirements regarding the context of the organization (clause 4)	2. Knowledge of the requirements of clause 4 Context of the organization of ISO 28000
3. Ability to interpret ISO 28000 requirements regarding the leadership of the organization (clause 5)	3. Knowledge of the requirements of clause 5 Leadership of ISO 28000
4. Ability to interpret ISO 28000 requirements regarding the planning for the security management system (clause 6)	4. Knowledge of the requirements of clause 6 Planning of ISO 28000
5. Ability to interpret ISO 28000 requirements regarding the support required for the security management system (clause 7)	5. Knowledge of the requirements of clause 7 Support of ISO 28000
6. Ability to interpret ISO 28000 requirements regarding the operation of the security management system (clause 8)	6. Knowledge of the requirements of clause 8 Operation of ISO 28000
7. Ability to interpret ISO 28000 requirements regarding the performance evaluation of the security management system (clause 9)	7. Knowledge of the requirements of clause 9 Performance evaluation of ISO 28000
8. Ability to interpret ISO 28000 requirements regarding the improvement of the security management system (clause 10)	8. Knowledge of the requirements of clause 10 Improvement of ISO 28000

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 an SeMS audit.

Competencies	Knowledge statements
1. Ability to differentiate between first, second, and third party audits	1. Knowledge of the characteristics of first, second, and third party audits
2. Ability to understand, explain, and establish audit objectives and audit criteria	2. Knowledge of the audit objectives and audit criteria
3. Ability to understand, explain, and apply the audit principles in an SeMS audit	3. Knowledge of audit principles: integrity, fair presentation, due professional care, confidentiality, independence, evidence-based approach, and risk-based approach
4. Ability to demonstrate integrity during an audit	4. Knowledge of the elements to consider in order to demonstrate integrity during an audit
5. Ability to report truthfully and accurately about the auditee's SeMS performance	5. Knowledge of the necessary aspects for providing a fair presentation of the auditee's SeMS performance in the audit findings, conclusions, and reports
6. Ability to demonstrate due professional care during an audit	6. Knowledge of the necessary aspects for demonstrating due professional care during an audit
7. Ability to maintain the confidentiality of the information obtained during an audit	7. Knowledge of the prerequisites for ensuring confidentiality of the information obtained during an audit
8. Ability to maintain objectivity throughout the audit process	8. Knowledge of the aspects that could compromise the independence of the audit process
9. Ability to apply a systematic and structured approach to the audit	9. Knowledge of the components of a systematic and structured approach to the audit
10. Ability to apply a risk-based approach during the different stages of an SeMS audit	10. Knowledge of the risk-based approach and the importance of its application
11. Ability to utilize technology in auditing	11. Knowledge of the usage of big data and other technologies in an audit
12. Ability to explain, compare, and obtain the different types of audit evidence and their characteristics	12. Knowledge of the different types of audit evidence: physical, mathematical, confirmative, technical, analytical, documentary, and verbal
13. Ability to determine the reliability of audit evidence	13. Knowledge of the main factors that determine the reliability of audit evidence
14. Ability to obtain reasonable assurance needed for an SeMS audit	14. Knowledge of the concept of reasonable assurance and its application in an audit

Domain 4: Preparing an ISO 28000 audit

Main objective: Ensure that the candidate is able to prepare an SeMS audit.

Competencies	Knowledge statements
<ol style="list-style-type: none"> 1. Ability to understand the steps and conduct the activities for preparing an SeMS audit considering the specific context of the audit 2. Ability to define and explain audit mandate and audit offer 3. Ability to understand and explain the roles and responsibilities of the audit team leader and audit team members 4. Ability to understand and explain scenarios in which an auditor can be rejected from the auditee 5. Ability to determine the audit feasibility 6. Ability to determine, evaluate, and confirm the audit objectives, criteria, and scope for an SeMS 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 8. Ability to define the audit schedule 	<ol style="list-style-type: none"> 1. Knowledge of the steps and activities necessary for preparing an SeMS audit 2. Knowledge of the audit mandate and audit offer 3. Knowledge of the roles and responsibilities of the audit team leader and audit team members 4. Knowledge of the valid reasons for which an auditor can be rejected from an auditee 5. Knowledge of how to conduct an audit feasibility study 6. Knowledge of the audit objectives, scope, and criteria 7. Knowledge of the characteristics of terms of the audit engagement and the best practices to establish initial contact with an auditee 8. Knowledge of the audit schedule

Domain 5: Conducting an ISO 28000 audit

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

Competencies	Knowledge statements
<ol style="list-style-type: none"> 1. Ability to conduct the stage 1 audit, taking into account the documented information evaluation criteria 2. Ability to prepare for and conduct on-site activities during the stage 1 audit 3. Ability to conduct interviews with key interested parties during the stage 1 audit 4. Ability to plan and conduct the stage 2 audit 5. Ability to assign work to audit team members 6. Ability to prepare audit test plans 7. Ability to organize and conduct an opening meeting 8. Ability to apply the best practices of communication to collect the appropriate audit evidence 9. Ability to consider the roles and responsibilities of all the interested parties involved in an audit 10. Ability to manage conflicts during an audit 11. Ability to use evidence collection procedures and tools 12. Ability to analyze evidence 13. Ability to develop audit test plans 14. Ability to differentiate the types of possible audit findings 15. Ability to draft a nonconformity report 16. Ability to report audit observations 17. Ability to understand, explain, and apply the concept of the benefit of the doubt 18. Ability to conduct quality reviews to audit documentation 	<ol style="list-style-type: none"> 1. Knowledge of the objectives and requirements of stage 1 audit, considering documented information evaluation criteria and ISO 28000 requirements 2. Knowledge of the steps and activities to be taken during the stage 1 audit 3. Knowledge of the points to validate during the interviews with key interested parties in the stage 1 audit 4. Knowledge of the stage 2 audit steps and activities 5. Knowledge of the competence needed when assigning responsibilities to each audit team member 6. Knowledge of the procedures to develop audit test plans 7. Knowledge of the process of conducting an effective opening meeting in an audit 8. Knowledge of the best communication practices during an audit 9. Knowledge of the roles and responsibilities of all interested parties (e.g., guides and observers) during an audit 10. Knowledge of the different conflict resolution techniques 11. Knowledge of the evidence collection procedures and tools, such as interview, documented information review, observation, analysis, sampling, and technical verification 12. Knowledge of the evidence analysis techniques (i.e., corroboration and evaluation) 13. Knowledge of the best practices used to develop audit test plans 14. Knowledge of the characteristics and differences between the concepts of conformity, minor nonconformity, major nonconformity, anomaly, and observation 15. Knowledge of the guidelines and best practices to draft nonconformity reports

16. Knowledge of the guidelines and best practices to draft and report audit observations
17. Knowledge of the benefit of the doubt and its application in an audit
18. Knowledge of the guidelines and best practice to complete audit working documents and perform a quality review

Domain 6: Closing an ISO 28000 audit

Main objective: Ensure that the candidate is able to conclude an SeMS audit and conduct audit follow-up activities.

Competencies	Knowledge statements
<ol style="list-style-type: none"> 1. Ability to draft audit findings and prepare audit conclusions 2. Ability to create an audit report and justify the recommendation for certification 3. Ability to present the audit conclusions 4. Ability to organize and conduct a closing meeting 5. Ability to close the audit 6. Ability to conduct the activities following an initial audit, including the evaluation of action plans, audit follow-ups, and surveillance activities 7. Ability to plan and conduct recertification audits 	<ol style="list-style-type: none"> 1. Knowledge of the evidence evaluation process and the processes of drafting audit findings and preparing audit conclusions 2. Knowledge of the guidelines and best practices to write and audit report and possible recommendations an auditor can give during the certification audit 3. Knowledge of the guidelines and best practices to draft audit conclusions and present audit findings and conclusions to the management of an audited organization 4. Knowledge of the closing meeting agenda 5. Knowledge of the aspects that should be considered when closing an audit 6. Knowledge of audit follow-ups, and surveillance activities and audits 7. Knowledge of the recertification audit requirements, steps, and activities, and conditions for the modification, extension, suspension, or withdrawal of an organization's certification

Domain 7: Managing an ISO 28000 audit program

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

Competencies	Knowledge statements
<ol style="list-style-type: none"> 1. Ability to establish an audit program and integrate the PDCA cycle within an audit program 2. Ability to differentiate internal and external audits 3. Ability to conduct the main activities in an internal audit 4. Ability to manage audit program records 5. Ability to monitor, evaluate, review, and improve an audit program 	<ol style="list-style-type: none"> 1. Knowledge of an audit program and the role of the PDCA cycle in its management 2. Knowledge of the differences between internal and external audits 3. Knowledge of the main activities in an internal audit 4. Knowledge of the requirements, guidelines, and best practices regarding the management of audit records 5. Knowledge of the points to evaluate in an audit program, and the factors indicating the need for the modification of the audit program

Based on the above-mentioned domains and their relevance, the exam contains 80 multiple-choice questions, as summarized in the table below:

				Level of understanding (Cognitive/Taxonomy) required	
		Number of questions/points per competency domain	% of the exam devoted/points to/for each competency domain	Questions that measure comprehension, application, and analysis	Questions that measure evaluation
Competency domains	Fundamental principles and concepts of a security management system	9	11.25	X	
	Security management system requirements	11	13.75	X	
	Fundamental audit concepts and principles	12	15	X	
	Preparing an ISO 28000 audit	9	11.25	X	
	Conducting an ISO 28000 audit	18	22.5		X
	Closing an ISO 28000 audit	11	13.75		X
	Managing an ISO 28000 audit program	10	12.5		X
Total		80	100%		
Number of questions per level of understanding				41	39
% of the exam devoted to each level of understanding (cognitive/taxonomy)				51.25%	48.75%

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

After successfully passing the exam, candidates will be able to apply for obtaining the “PECB Certified ISO 28000 Lead Auditor” credential.

Taking the exam

General information about the exam

Candidates are required to arrive/be present at least 30 minutes before the exam starts.

Candidates who arrive late will not be given additional time to compensate for the late arrival and may not be allowed to sit for the exam.

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

If requested on the day of the exam (paper-based exams), additional time can be provided to candidates taking the exam in a non-native language, as follows:

- 10 additional minutes for Foundation exams
- 20 additional minutes for Manager exams
- 30 additional minutes for Lead exams

PECB exam format and type

1. **Paper-based:** Exams are provided on paper, where candidates are not allowed to use anything but the exam paper and a pen. The use of electronic devices, such as laptops, tablets, or phones, is not allowed. The exam session is supervised by a PECB approved Invigilator at the location where the Partner has organized the training course.
2. **Online:** Exams are provided electronically via the PECB Exams application. The use of electronic devices, such as tablets and cell phones, is not allowed. The exam session is supervised remotely by a PECB Invigilator via the PECB Exams application and an external/integrated camera.

For more information about online exams, go to the [PECB Online Exam Guide](#).

PECB exams are available in two types:

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

This exam comprises multiple-choice questions: The multiple-choice exam can be used to evaluate candidates' understanding on both simple and complex concepts. It comprises both stand-alone and scenario-based questions. Stand-alone questions stand independently within the exam and are not context-dependent, whereas scenario-based questions are context-dependent, i.e., they are developed based on a scenario which a candidate is asked to read and is expected to provide answers to five questions related to that scenario. When answering stand-alone and scenario-based questions, candidates will have to apply various concepts and principles explained during the training course, analyze problems, identify and evaluate alternatives, combine several concepts or ideas, etc.

Each multiple-choice question has three options, of which one is the correct response option (keyed response) and two incorrect response options (distractors).

This is an open-book exam. The candidate is allowed to use the following reference materials:

- A hard copy of the ISO 28000 standard
- Training course materials (accessed through the PECB Exams app and/or printed)
- Any personal notes taken during the training course (accessed through the PECB Exams app and/or printed)
- A hard copy dictionary

A sample of exam questions will be provided below.

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

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

Sample exam questions

1. **Which of the following is NOT included in an audit offer?**
 - A. The auditor's payment
 - B. **The responsibilities of technical experts**
 - C. The limits to the audit engagement

2. ***T-Poll* has two management systems which are being audited simultaneously on a single auditee? What type of audit is being conducted?**
 - A. Joint audit
 - B. Surveillance audit
 - C. **Combined audit**

3. **Which of the following is an example of technical evidence?**
 - A. Calculating the number of training hours provided to employees
 - B. **Analysis of the results of simulation tests**
 - C. Analysis of security-related incident tickets to detect trends

4. **Which of the following indicates a major nonconformity?**
 - A. Some of the nonconformities were not corrected as planned (on time) and no justification was provided or documented
 - B. A few employees involved in the SeMS have not received adequate training
 - C. **The organization has not conducted an internal audit**

5. **What should the audit schedule reflect?**
 - A. **The status and importance of the activities to be audited**
 - B. The expected amount of nonconformities that will be detected
 - C. The cooperation of the auditee representatives

Exam Security Policy

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

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

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

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

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

Any violation of the points mentioned above will cause PECB irreparable damage for which no monetary remedy can make up. Therefore, PECB can take the appropriate actions to remedy or prevent any unauthorized disclosure or misuse of exam materials, including obtaining an immediate injunction. PECB will take action against individuals that violate the rules and policies, including permanently banning them from pursuing PECB credentials and revoking any previous ones. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

Exam results

Exam results will be communicated via email.

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

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

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

Candidates that disagree with the results may request a re-evaluation by writing to examination.team@pecb.com within 30 days of receiving the results. Re-evaluation requests received after 30 days will not be processed. If candidates do not agree with the results of the reevaluation, they have 30 days from the date they received the reevaluated exam results to file a complaint through the [PECB Ticketing System](#). Any complaint received after 30 days will not be processed.

Exam Retake Policy

There is no limit to the number of times a candidate can retake an exam. However, there are certain limitations in terms of the time span between exam retakes.

If a candidate does not pass the exam on the 1st attempt, they must wait 15 days after the initial date of the exam for the next attempt (1st retake).

Note: Candidates who have completed the training course with one of our partners, and failed the first exam attempt, are eligible to retake for free the exam within a 12-month period from the date the coupon code is received (the fee paid for the training course, includes a first exam attempt and one retake). Otherwise, retake fees apply.

For candidates that fail the exam retake, PECB recommends they attend a training course in order to be better prepared for the exam.

To arrange exam retakes, based on exam format, candidates that have completed a training course, must follow the steps below:

1. Online Exam: when scheduling the exam retake, use initial coupon code to waive the fee
2. Paper-Based Exam: candidates need to contact the PECB Partner/Distributor who has initially organized the session for exam retake arrangement (date, time, place, costs).

Candidates that have not completed a training course with a partner, but sat for the online exam directly with PECB, do not fall under this Policy. The process to schedule the exam retake is the same as for the initial exam.

SECTION III: CERTIFICATION PROCESS AND REQUIREMENTS

PECB ISO 28000 credentials

All PECB certifications have specific requirements regarding education and professional experience. To determine which credential is right for you, take into account your professional needs and analyze the criteria for the certifications.

The credentials in the PECB ISO 28000 scheme have the following requirements:

Credential	Education	Exam	Professional experience	MS audit/assessment experience	Other requirements
PECB Certified ISO 28000 Provisional Auditor	At least secondary education	PECB Certified ISO 28000 Lead Auditor exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified ISO 28000 Auditor			Two years: One year of work experience in security management	Audit activities: a total of 200 hours	
PECB Certified ISO 28000 Lead Auditor			Five years: Two years of work experience in security management	Audit activities: a total of 300 hours	
PECB Certified ISO 28000 Senior Lead Auditor			Ten years: Seven years of work experience in security management	Audit activities: a total of 1,000 hours	

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. Reviewing and managing documented information related to the audit
7. Conducting on-site audits
8. Following up on nonconformities
9. Leading an audit team

Applying for certification

All candidates who successfully pass the exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credential they were assessed for. Specific educational and professional requirements need to be fulfilled in order to obtain a PECB certification. Candidates are required to fill out the online certification application form (that can be accessed via their PECB account), including contact details of individuals who will be contacted to validate the candidates' professional experience. Candidates can submit their

application in English, French, German, Spanish or Korean languages. They can choose to either pay online or be billed. For additional information, please contact certification.team@pecb.com.

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

- [Register](#) your account
- Check your email for the confirmation link
- [Log in](#) to apply for certification

For more information on how to apply for certification, click [here](#).

The Certification Department validates that the candidate fulfills all the certification requirements regarding the respective credential. The candidate will receive an email about the application status, including the certification decision.

Following the approval of the application by the Certification Department, the candidate will be able to download the certificate and claim the corresponding Digital Badge. For more information about downloading the certificate, click [here](#), and for more information about claiming the Digital Badge, click [here](#).

PECB provides support both in English and French.

Professional experience

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

Professional references

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

SeMS 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, or third party audits.

Evaluation of certification applications

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

SECTION IV: CERTIFICATION POLICIES

Denial of certification

PECB can deny certification/certificate program if candidates:

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

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

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

Certification status options

Active

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

Suspended

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

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

Revoked

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

Additional reasons for revoking certification can be if the candidates:

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

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

Other statuses

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

Upgrade and downgrade of credentials

Upgrade of credentials

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

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

Downgrade of credentials

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

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

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

Renewing the certification

PECB certifications are valid for three years. To maintain them, PECB certified professionals must meet the requirements related to the designated credential, e.g., they must fulfill the required number of continual professional development (CPD) hours. In addition, they need to pay the annual maintenance fee (\$120). For more information, go to the [Certification Maintenance](#) page on the PECB website.

Closing a case

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

Complaint and Appeal Policy

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

For more information about the Complaint and Appeal Policy, click [here](#).

SECTION V: GENERAL POLICIES

Exams and certifications from other accredited certification bodies

PECB accepts certifications and exams from other recognized accredited certification bodies. PECB will evaluate the requests through its equivalence process to decide whether the respective certification(s) or exam(s) can be accepted as equivalent to the respective PECB certification (e.g., ISO 28000 Lead Auditor certification).

Non-discrimination and special accommodations

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

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations³ 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 arrangements⁴. Any information that candidates provide regarding their disability/special needs will be treated with confidentiality. To download the Candidates with Disabilities Form, click [here](#).

Behavior Policy

PECB aims to provide top-quality, consistent, and accessible services for the benefit of its external stakeholders: distributors, partners, trainers, invigilators, examiners, members of different committees and advisory boards, and clients (trainees, examinees, certified individuals, and certificate holders), as well as creating and maintaining a positive work environment which ensures safety and well-being of its staff, and holds the dignity, respect and human rights of its staff in high regard.

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

Refund Policy

PECB will refund your payment, if the requirements of the Refund Policy are met. To read the Refund Policy, click [here](#).

³ According to ADA, the term "reasonable accommodation" may include: (A) making existing facilities used by employees readily accessible to and usable by individuals with disabilities; and (B) job restructuring, part-time or modified work schedules, reassignment to a vacant position, acquisition or modification of equipment or devices, appropriate adjustment or modifications of examinations, training materials or policies, the provision of qualified readers or interpreters, and other similar accommodations for individuals with disabilities.

⁴ ADA Amendments Act of 2008 (P.L. 110–325) Sec. 12189. Examinations and courses. [Section 309]: Any person that offers examinations or courses related to applications, licensing, certification, or credentialing for secondary or post-secondary education, professional, or trade purposes shall offer such examinations or courses in a place and manner accessible to persons with disabilities or offer alternative accessible arrangements for such individuals.



Address:

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



Tel./Fax:

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



Emails:

Examination:

examination.team@pecb.com

Certification:

certification.team@pecb.com

Customer Service:

support@pecb.com



PECB Help Center

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

www.pecb.com