PECB BEYOND RECOGNITION

Exam Preparation Guide

ISO 28000 Lead Auditor

GENERAL

The objective of the "PECB Certified ISO 28000 Lead Auditor" exam is to ensure that the candidate has the necessary competence to: perform a supply chain security management system (SCSMS) audit in compliance with the ISO 28000 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 28000 Lead Auditor exam is intended for:

- Auditors seeking to perform and lead supply chain security management system (SCSMS) audits
- Managers or consultants seeking to master the supply chain security management system audit process
- Individuals responsible for maintaining conformity with the SCSMS requirements
- Technical experts seeking to prepare for a supply chain security management system audit
- Expert advisors in supply chain security management

The exam covers the following competency domains:

- **Domain 1:** Fundamental principles and concepts of a supply chain security management system (SCSMS)
- **Domain 2:** Supply chain security management system (SCSMS)
- **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

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts of a supply chain security management system (SCSMS)

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

Competencies	Knowledge statements
1. Ability to understand and explain the operations of the ISO organization and the development of supply chain security management standards 2. Ability to identify, analyze and evaluate the supply chain security management compliance requirements for an organization 3. Ability to explain and illustrate the main concepts in supply chain security management System 4. Ability to understand relationship between different standards of ISO 28000 family	1. Knowledge of the application of the eight ISO management principles to supply chain security management system 2. Knowledge of the main standards in supply chain security management 3. Knowledge of the different sources of Supply chain security management system requirement for an organization: laws, regulations, international and industry standards, contracts, market practices, internal policies Knowledge of the main supply chain security management concepts and terminology as described in ISO 28000

Domain 2: Supply chain security management system (SCSMS) and ISO 28000 requirements

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

Competencies	Knowledge statements
1. Ability to understand and explain the components of a supply chain security Management System based on ISO 28000 and its principal processes 2. Ability to interpret and analyze ISO 28000 requirements 3. Ability to understand, explain and illustrate the main steps to establish, implement, operate, monitor, review, maintain and improve an organization's SCSMS	1. Knowledge of the concepts, principles and terminology related to supply chain security management system based SCSMS and the "Plan-Do-Check-Act" (PDCA) model 2. Knowledge of the principal characteristics of an integrated management system 3. Knowledge of the main advantages of a certification for an organization 4. Knowledge of the ISO 28000 requirements 5. Knowledge of the main steps to establish the SCSMS objectives, processes and procedures relevant to managing and improving supply chain security management to deliver results in accordance with an organization's overall policies and objectives (Awareness level) 6. Knowledge of the concept of continual improvement and its application to an SCSMS

Domain 3: Fundamental audit concepts and principles

Main objective: Ensure that the candidate understands, is able to interpret, and apply the main concepts and principles related to an SCSMS audit

Competencies	Knowledge statements
1. Ability to understand, explain and illustrate the application of the audit principles in the context of an ISO 28000 audit 2. Ability to identify and judge situations that would discredit the professionalism of the auditor and the PECB code of ethics 3. Ability to identify and evaluate ethical problems taking into account the obligations related to sponsors, auditee and law enforcement or regulatory authorities 4. Ability to explain, illustrate and apply the audit evidence approach in the context of an ISO 28000 audit 5. Ability to explain and compare the types and characteristics of evidence 6. Ability to determine and justify what type of evidence and how much evidence will be required in the context of a specific SCSMS audit mission 7. Ability to determine and evaluate the level of materiality and apply the risk based approach during the different phases of an ISO 28000 audit 8. Ability to judge the appropriate level of reasonable assurance needed for a specific ISO 28000 audit mission	1. Knowledge of the main audit concepts and terminology as described in ISO 19011 2. Knowledge of the differences between first party, second party and third party audit 3. Knowledge of the following audit principles: integrity, fair presentation, due professional care, professional judgment, professional skepticism, confidentiality and independence 4. Knowledge of professional responsibility of an auditor and the PECB code of ethics 5. Knowledge of evidence based approach in an audit 6. Knowledge of the different types of evidences: physical, mathematical, confirmative, technical, analytical, documentary and verbal 7. Knowledge of quality of audit evidences (competent, appropriate, reliable and sufficient) and the factors that will influence them 8. Knowledge of the risk based approach in an audit and the different types of risk related to audit activities 9. Knowledge of the concept of materiality and its application in an audit 10. Knowledge of the concept of reasonable assurance and its applicable in an audit

Domain 4: Preparing an ISO 28000 audit

Main objective: Ensure that the candidate is able to prepare a supply chain security management system audit

Competencies	Knowledge statements
1. Ability to understand and explain the steps and activities to do to prepare an SCSMS audit taking in consideration the specific context and conditions of the mission 2. Ability to understand and explain the roles and responsibilities of the audit team leader, audit team members and technical experts 3. Ability to determine, evaluate and confirm the audit objectives, the audit criteria and the audit scope for a specific ISO 28000 audit mission 4. Ability to do a feasibility study of an audit in the context of a specific ISO 28000 audit mission 5. Ability to explain, illustrate and define the characteristics of the audit terms of engagement and apply the best practices to establish a first contact with an auditee in the context of a specific ISO 28000 audit mission 6. Ability to develop audit working papers and to elaborate appropriate audit test plans in the context of a specific ISO 28000 audit mission	1. Knowledge of the main responsibilities of the audit team leader and audit team members 2. Knowledge of the roles and responsibilities of technical experts used for an audit 3. Knowledge of the definition of audit objectives, audit scope and audit criteria 4. Knowledge of the difference between the SCSMS scope and the audit scope 5. Knowledge of the elements to review during the feasibility study of an audit 6. Knowledge of the cultural aspects to consider in an audit 7. Knowledge of the characteristics of audit terms of engagement and the best practices to establish a first contact with an auditee 8. Knowledge of the preparation of an audit plan 9. Knowledge of the preparation and development of audit working paper 10. Knowledge of advantages and disadvantages of using audit checklists 11. Knowledge of the best practices to creation audit test plans

Domain 5: Conducting an ISO 28000 audit

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

Competencies	Knowledge statements
1. Ability to organize and conduct the opening meeting in the context of a specific ISO 28000 audit mission 2. Ability to conduct a stage 1 audit in the context of a specific ISO 28000 audit mission and taking into account the documentation review conditions and criteria 3. Ability to conduct a stage 2 audit in the context of a specific ISO 28000 audit mission by applying the best practices of communication to collect the appropriate evidence and taking into account the roles and responsibilities of all people involved 4. Ability to explain, illustrate and apply statistical techniques and main audit sampling methods 5. Ability to gather appropriate evidences objectively from the available information in an audit and to evaluate them objectively	1. Knowledge of the objectives and the content of the opening meeting of an audit 2. Knowledge of the difference of the stage 1 audit and the stage 2 audit 3. Knowledge of stage 1 audit requirements, steps and activities 4. Knowledge of the documentation review criteria 5. Knowledge of the documentation requirements stated in ISO 28000 6. Knowledge of stage 2 audit requirements, steps and activities 7. Knowledge of best practices of communication during an audit 8. Knowledge of the roles and responsibilities of guides and observers during an audit 9. Knowledge of the conflict resolution techniques 10. Knowledge of evidence collection procedures: observation, documentation review, interviews, analysis and technical verification 11. Knowledge of evidence analysis procedures: corroboration and evaluation 12. Knowledge of main concepts, principles and statistical techniques used in an audit 13. Knowledge of the main audit sampling methods and their characteristics

Domain 6: Closing an ISO 28000 audit

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

Competencies	Knowledge statements
1. Ability to explain and apply the evaluation process of evidences to draft audit findings and prepare audit conclusions 2. Ability to understand, explain and illustrate the different levels of conformity and the concept of benefits of doubt 3. Ability to report appropriate audit observations in order to help an organization to improve an SCSMS in respect of audit rules and principles 4. Ability to complete audit working documents and do a quality review of an ISO 28000 audit 5. Ability to draft audit conclusions and present these to the management of the audited organization 6. Ability to organize and conduct an audit closing meeting 7. Ability to write an ISO 28000 audit report and justify a certification recommendation 8. Ability to conduct the activities following an initial audit including the evaluation of action plans, follow up audits, surveillance audits and recertification audits	1. Knowledge of the evaluation process of evidences to draft audit findings and prepare audit conclusions 2. Knowledge of the differences and the characteristics between the concepts of conformity, minor nonconformity, major nonconformity, anomaly and observation 3. Knowledge of the guidelines and best practices to write nonconformity report 4. Knowledge of the guidelines and best practices to draft and report audit observation 5. Knowledge of the principle of benefits of doubt and his application in the context of an audit 6. Knowledge of the guidelines and best practices to complete audit working documents and do a quality review of an audit 7. Knowledge of the guidelines and best practices to present audit findings and conclusions to management of an audited organization 8. Knowledge of the possible recommendations that an auditor can issue in the context of a certification audit and the certification decision process 9. Knowledge of the guidelines and best practices to evaluate action plans 10. Knowledge of follow-up audit, surveillance audits and recertification audit requirements, steps and activities 11. Knowledge of the conditions for modification, extension, suspension or withdrawal of a certification for an organization

Domain 7: Managing an ISO 28000 audit program

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

Competencies	Knowledge statements
1. Ability to understand and explain the establishment of an audit program and the application of the PDCA model 2. Ability to understand and explain the implementation of an ISO 28000 audit program (first party, second party and third party) 3. Ability to understand and explain the responsibilities to protect the integrity, availability and confidentiality of audit records 4. Ability to understand the requirements related to the components of the management system of an audit program as quality management, record management, complaint management 5. Ability to understand the evaluation of the audit program efficiency by monitoring the performance of each auditor, each team and the entire certification body 6. Ability to understand and explain the way that the combined audits are handled in an audit program 7. Ability to demonstrate the application of the personal attributes and behaviors associated to professional auditors	1. Knowledge of the application of the PDCA model in the management of an audit program 2. Knowledge of requirements, guidelines and best practices regarding audit resources, procedures and policies 3. Knowledge of the types of tools used by professional auditors 4. Knowledge of requirements, guidelines and best practices regarding the management of audit records 5. Knowledge of the application of the continual improvement concept to the management of an audit program 6. Knowledge of the particularities to implement and manage a first, second or third party audit program 7. Knowledge of the managing the combined audit activities 8. Knowledge of the competency concept and its application to auditors 9. Knowledge of the personal attributes and behavior of a professional auditor

Based on the above-mentioned domains and their relevance, 12 questions are included in the exam, as summarized in the table below:

			Level of understanding (Cognitive/Taxonomy) required					
		Points per question	Questions that measure comprehension, application and analysis	Questions that measure synthesis and evaluation	Number of questions per competency domain	% of test devoted to each competency domain	Number of points per competency domain	% of points per competency domain
Competency domains	Fundamental principles and concepts of the supply chain security management system (SCSMS)	5	X		1	8.33	5	6.67
	Supply chain security management system (SCSMS)	5	X		3	16.66	15	20.01
		10		X				
	Fundamental audit concepts and principles	5		X	3	25	15	20.01
		5	X					
		5	X					
	Preparing an ISO 28000 audit	5	X		2	16.66	10	13.34
		5		X				
	Conducting an ISO 28000 audit	10		X	2	16.66	15	20.01
		5	X					
	Closing an ISO 28000 audit	10		X	1	8.33	10	13.34
	Managing an ISO 28000 audit program	5		X	1	8.33	5	6.67
	Total points	75						
	Number of questions per level of understanding		6	6				
	% of test devoted to each level of understanding (cognitive/taxonomy)		50	50				

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

After successfully passing the exam, candidates will be able to apply for the "PECB Certified ISO 28000 Lead Auditor" credential depending on their level of experience.

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 Reseller 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 comprises essay-type questions. They are used to determine and evaluate whether a candidate can clearly answer questions related to the defined competency domains. Additionally, problem-solving techniques and arguments that are supported with reasoning and evidence will also be evaluated.

The exam is open book and is not intended to measure memorizing or recalling information. It aims to evaluate candidates' comprehension, analytical skills, and applied knowledge. Therefore, candidates are required to provide logical and convincing answers and explanations in order to demonstrate that they have understood the content and the main concepts of the competency domains.

Since the exam is "open book," candidates are authorized to use the following reference materials:

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

Any attempts to copy, collude, or otherwise cheat during the exam session will automatically lead to failure of the exam.

PECB exams are available in English and other languages. For the availability of the exam 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.

Receiving the Exam Results

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

- The time span for the communication starts from the exam date and lasts 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 for a re-evaluation by writing to results@pecb.com within 30 working 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 working days from the date when they received the reevaluated exam results to file a complaint through the PECB Ticketing System. Complaints received after 30 days will not be processed.

Exam Retake Policy

There is no limit on the number of times that a candidate may retake an exam. However, there are certain limitations in terms of the allowed time frames between exam retakes.

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

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

Reschedule the Exam

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

Closing a Case

If a candidate does not apply for the certificate within three years, their case will be closed. Candidates whose case has been closed due to the expiration of the certification period have the right to request to reopen their case. However, PECB will no longer be responsible for any changes in the conditions, standards, policies, candidate handbook, or exam preparation guide 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.

Exam Security

A significant component of a successful and respected professional certification credential is maintaining the security and confidentiality of the exam. PECB relies upon the ethical behavior of certificate holders and applicants to maintain the security and confidentiality of PECB exams. Any disclosure of information about the content of PECB exams indicates violation of PECB's Code of Ethics. PECB will take action against individuals who violate PECB Policies and the Code of Ethics. These actions include permanently barring individuals from pursuing PECB credentials and revoking the awarded credentials. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

Sample Exam Questions

Question 1: Evidence in an audit

For each of the following clauses of the ISO 28000 standard, please provide at least two different evidences that would be acceptable to verify the existence and effectiveness of the requirement.

- **4.3.4 Security management targets:**

Possible answer:

- Monthly targets' metrics
- Emails showing targets have been communicated to employees

Question 2: Evaluation of corrective actions

You have received a plan for corrective actions. Evaluate the adequacy of the proposed corrective actions. If you agree with the corrective actions, explain why. If you disagree, explain why and propose what you think would be adequate corrective actions.

- **A nonconformity was observed because the Human Resources team was not aware of the procedure that requires them to record the education, training, and experience of all employees.**
- **Corrective action: Inform (Timeframe: immediately) and train (Timeframe: within 6 months) the Human Resources team with this procedure and require that each member of the team follow it.**

Possible answer:

I agree. This solves the problem that was ignorance of the procedure. As auditor, a sampling will be performed during the surveillance audit to find out if the procedure is followed.

Address:
Head Quarters
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. Visit Help Center here: www.pecb.com/help

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