PECB

When Recognition Matters

EXAM PREPARATION GUIDE

PECB Certified ISO 28000 Lead Implementer

The objective of the “PECB Certified ISO 28000 Lead Implementer” examination is to ensure that the candidate has the knowledge and the skills to support an organization in implementing and managing a Supply Chain Security Management System (SCSMS) as specified in ISO 28000:2007.

The target population for this examination is:

- Managers or consultants involved in Supply Chain Security Management
- Expert advisors seeking to master the implementation of a Supply Chain Security Management System
- Individuals responsible for maintaining conformance with SCSMS requirements
- SCSMS team members

The exam content covers the following 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:** Planning a SCSMS implementation based on ISO 28000
- **Domain 4:** Implementing a SCSMS based on ISO 28000
- **Domain 5:** Performance evaluation, monitoring and measurement of SCSMS based on ISO 28000
- **Domain 6:** Continual improvement of a SCSMS based on ISO 28000
- **Domain 7:** Preparing for a SCSMS certification audit

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts in Supply Chain Security Management System (SCSMS)

Main objective: To ensure that the ISO 28000 Lead Implementer candidate can understand, interpret and illustrate the main Supply Chain Security Management concepts related to a Supply Chain Security Management System (SCSMS).

Competencies	**Knowledge statements**
1. Understand and explain the operations of the ISO organization and the development of Supply Chain Security Management standards. 2. Understand ISO 28000 related standards and their importance, including ISO 28001, ISO 28002, ISO 28003 and ISO 28004. 3. Ability to identify for which industries and sectors is ISO 28000 standard flexible and applicable. 4. Understand the main SCSMS advantages. 5. Ability to explain and illustrate the main concepts in Supply Chain Security Management System. 6. Ability to understand the importance of the supply chain in the global economy. 7. Ability to interpret supply chain security activities 8. Ability to interpret concepts related to risk management	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 industries and sectors that use ISO 28000 including rail/air transport, sea transport, port facilities etc. 4. Knowledge of the main SCSMS advantages including improvement of security, good governance, conformity to applicable laws and regulations and other industry standards, cost reduction, etc. 5. 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. 6. Knowledge of the main Supply Chain Security Management concepts and terminology as described in ISO 28000. 7. Knowledge of the complexity of the transportation of goods in the global economy 8. Knowledge of activities such as inspection of cargo on entry, security of cargo while in-transit via the use of locks and tamper-proof seals, screening and validation of the contents of cargo being shipped, etc. 9. Knowledge of risk management concepts including, likelihood, occurrence, threat, vulnerability and countermeasures. 10. Knowledge on how to identify supply chain security management threats, vulnerabilities and impacts.

Domain 2: Supply Chain Security Management System (SCSMS)

Main objective: To ensure that the ISO 28000 Lead Implementer candidate can understand, interpret and provide guidance on how to implement Supply Chain Security Management System requirements provided by ISO 28000.

Competencies

1. Ability to identify, understand, classify and explain the clauses with requirements from ISO 28000.
2. Ability to detail and illustrate the requirements and best practices by concrete examples.
3. Ability to establish a security management policy
4. Ability to assess security risks
5. Ability to set SCSMS objectives and targets
6. Ability to understand top management responsibilities based on ISO 28000
7. Ability to train and aware organizations personnel regarding ISO 28000
8. Ability to establish plans and procedures regarding emergency preparedness, response and security recovery
9. Ability to measure and monitor SCSMS
10. Ability to evaluate security management plans and procedures
11. Ability to evaluate and initiate preventive actions.
12. Ability to implement preventive actions.
13. Ability to review the effectiveness of the implemented preventive actions.
14. Ability to conduct internal audits at planned intervals.

Knowledge statements

1. Knowledge of ISO 28000 requirements including security management policy, security risk assessment planning, implementation and operation, checking and corrective action and management review and continual improvement.
2. Knowledge of the required elements of a security management policy
3. Knowledge on how to establish and maintain procedures that support the identification and assessment of security threats
4. Knowledge on how to establish objectives and targets that lead to a successful SCSMS by considering threats, risks and their impacts, all legal and regulatory requirements, views of interested parties, technology, organizations finances, organization operations and other critical assets
5. Knowledge on how to periodically review the established targets in order to ensure their consistency and relevance to the SCSMS
6. Knowledge on how to communicate the established targets to all organization's employees and third parties
7. Knowledge on how to define roles and responsibilities regarding the SCSMS implementation and management.
8. Knowledge of preventive, detective and corrective measures that shall be taken to prevent and detect security incidents.
9. Knowledge on how to establish and maintain procedures to monitor and measure the performance of organization security management system.
10. Knowledge on how to conduct periodic reviews, tests and establish post-incident reports
11. Knowledge on how to keep records of the results of the periodic evaluations.
12. Knowledge on how to analyze and evaluate the preventive actions.

	13. Knowledge on how to mitigate consequences 14. Knowledge of the inputs and outputs of management reviews.

Domain 3: Planning a SCSMS implementation based on ISO 28000

Main objective: To ensure that the ISO 28000 Lead Implementer candidate can plan the implementation of an SCSMS based on ISO 28000 requirements

Competencies	Knowledge statements
1. Ability to manage an SCSMS implementation project following project management best practices. 2. Ability to gather, analyze and interpret the necessary information to plan the SCSMS implementation. 3. Ability to observe, analyze and interpret the external and internal environment of an organization. 4. Ability to perform a gap analysis and clarify the Supply Chain Security Management objectives of an organization. 5. Ability to state and justify an SCSMS scope adapted to the security objectives of a specific organization. 6. Ability to establish a supply chain security policy 7. Ability to manage risks related to the SCSMS 8. Ability to set security objectives, targets and programmes 9. Ability to identify all legal and regulatory requirements before implementing a SCSMS	1. Knowledge of the main project management concepts, terminology, process and best practice as described in ISO 10006. 2. Knowledge of the principal approaches and methodology frameworks to implement an SCSMS. 3. Knowledge of the main concepts and terminology related to organizations. 4. Knowledge of an organization's external and internal environment. 5. Knowledge of the main interested parties related to an organization and their characteristics. 6. Knowledge of techniques to gather information on an organization and to perform a gap analysis of a management system. 7. Knowledge of the characteristics of an SCSMS scope in terms of organizational, technological and physical boundaries. 8. Knowledge of the policy drafting process 9. Knowledge of the importance of management commitment 10. Knowledge of the different approaches and main methodology characteristics to perform a risk assessment. 11. Knowledge of the main activities of the risk management activities including context establishment, risk identification, risk analysis, risk evaluation, risk treatment, risk acceptance 12. Knowledge on how to set security objectives, determine targets and create security programmes

Domain 4: Implementing a SCSMS Based on ISO 28000

Main objective: To ensure that the ISO 28000 Lead Implementer candidate can implement the processes and security controls of an SCSMS based on ISO 28000 standard

Competencies	Knowledge statements
1. Ability to understand, analyze needs and provide guidance on the attribution of roles and responsibilities in the context of the implementation and management of an SCSMS. 2. Ability to define the document and record management processes needed to support the implementation and the operations of an SCSMS. 3. Ability to define and design security controls & processes and document them 4. Ability to implement Supply Chain Security Management policies & procedures. 5. Ability to define and implement appropriate Supply Chain Security Management training, awareness and communication plans. 6. Ability to establish and implement a SCSMS communication plan 7. Ability to implement the required processes and security controls of an SCSMS. 8. Ability to identify potential emergency situations 9. Ability to establish and implement emergency procedures	1. Knowledge of the roles and responsibilities of the key actors during the implementation of an SCSMS and in its operation after the end of the implementation project. 2. Knowledge of the main organizational structures applicable for an organization to manage Supply Chain Security Management. 3. Knowledge of the best practices on document and record management processes and the document management life cycle. 4. Knowledge of the characteristics and the differences between the different documents related to SCSMS: policy, procedure, guideline, standard, baseline, worksheet, etc. 5. Knowledge of techniques and best practices to write Supply Chain Security Management policies, procedures and others types of documents include in an SCSMS. 6. Knowledge of the characteristics and the best practices to implement Supply Chain Security Management training, awareness and communication plans. 7. Knowledge of the principles of an efficient communication strategy 8. Knowledge of model-building controls and processes techniques and best practices. 9. Knowledge of controls and processes deployment techniques and best practices. 10. Knowledge of organizational controls, human resource controls, asset management controls, secure areas controls, infrastructure security controls, access controls, information security controls and legal controls 11. Knowledge of situations that can lead to emergency situations 12. Knowledge of emergency response equipment’s

	13. Knowledge on how to periodically test emergency procedures

Domain 5: Performance evaluation, monitoring and measurement of a SCSMS based on ISO 28000

Main objective: To ensure that the ISO 28000 Lead Implementer candidate can evaluate, monitor and measure the performance of a SCSMS based on ISO 28000 standard

Competencies	Knowledge statements
1. Ability to monitor and evaluate the effectiveness of an SCSMS in operation. 2. Ability to verify the extent to which identified security requirements have been met. 3. Ability to define and implemented an internal audit program for ISO 28000. 4. Ability to perform regular and methodical reviews regarding the suitability, adequacy, effectiveness and efficiency of an SCSMS with policies and security objectives of an organization. 5. Ability to define and implement a management review process and counsel management on it.	1. Knowledge of the techniques and best practices to monitor the effectiveness of an SCSMS. 2. Knowledge of the main concepts and components related to a Supply Chain Security Management Measurement Programme: measures, attributes, indicators, dashboard, etc. 3. Knowledge of the characteristics and the differences between an operational, tactical and strategic Supply Chain Security Management indicators and dashboard. 4. Knowledge of the techniques and methods to define and document adequate and reliable indicators. 5. Knowledge of the main concepts and components related to the implementation and operation of an SCSMS internal audit program. 6. Knowledge of the differences between the concepts of major nonconformity, minor nonconformity, anomaly and observation. 7. Knowledge of the guidelines and best practices to write nonconformity report. 8. Knowledge of the best practices on how to perform management reviews.

Domain 6: Continual improvement of a SCSMS based on ISO 28000

Main objective: To ensure that the ISO 28000 Lead Implementer candidate can continually improve the SCSMS based on ISO 28000 requirements and best practices

Competencies	Knowledge statements
1. Ability to identify, analyze the root-causes of nonconformities and proposed action plans to treat them. 2. Ability to identify, analyze the root-cause of potential nonconformities and proposed action plans to treat them 3. Ability to understand the principle and concepts related to continual improvement. 4. Ability to counsel an organization on how to continually improve the effectiveness and the efficiency of an SCSMS. 5. Ability to implement SCSMS continual improvement processes in an organization. 6. Ability to determine the appropriate business improvement tools to support continual improvement processes of a specific organization.	1. Knowledge of the main processes, tools and techniques used by professionals to identify the root-causes of nonconformities. 2. Knowledge of the characteristics and the difference between corrective actions and preventive actions. 3. Knowledge of the main processes, tools and techniques used by professionals to develop and proposed the best corrective and preventive action plans. 4. Knowledge on how to draft action plans and submitting such plans to the top management for approval 5. Knowledge of the main concepts related to continual improvement. 6. Knowledge of the characteristics and the difference between the concept of effectiveness and the efficiency. 7. Knowledge on how to continually monitor the change factors that can influence SCSMS effectiveness

Domain 7: Preparing for a SCSMS certification audit

Main objective: To ensure that the ISO 28000 Lead Implementer candidate can prepare and assist an organization for the certification of an SCSMS against the ISO 28000 standard.

Competencies	Knowledge statements
1. Ability to understand the main steps processes and activities related to an ISO 28000 certification audit. 2. Ability to select a certification body 3. Ability to review the readiness of an organization for an ISO 28000 certification audit. 4. Ability to prepare organizations personnel for an ISO 28000 certification audit. 5. Ability to understand the difference between certification audit steps	1. Knowledge of the certification process steps such as SCSMS implementation, internal audit and management review, selection of the certification body, audit preparation, stage 1 audit, stage 2 audit, follow up audit, confirmation of registration and continuous improvement and surveillance audit 2. Knowledge of the main criteria for selecting a certification body 3. Knowledge on how to conduct self –evaluation, prepare the personnel and practice audit to determine whether the organization is ready for the certification audit 4. Knowledge of the difference of the stage 1 audit and the stage 2 audit. 5. Knowledge of stage 1 audit requirements, steps and activities. 6. Knowledge of the documentation review criteria 7. Knowledge of stage 2 audit requirements, steps and activities. 8. Knowledge of follow-up audit requirements, steps and activities. 9. Knowledge of surveillance audits and recertification audit requirements, steps and activities. 10. Knowledge of the requirements, guidelines and best practices to develop action plans following an ISO 28000 certification audit.

Based on these seven domains and their relevance, twelve (12) questions are included in the exam, as summarized in the following table:

			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 a Supply Chain Security Management System (SCSMS)	5	X		1	8.33	5	6.67
	Supply Chain Security Management System (SCSMS)	10		X	8.33	16.66	10	13.34
	Planning a SCSMS implementation based on ISO 28000	5		X	3	25	15	20.01
		5		X				
		5	X					
	Implementing a SCSMS based on ISO 28000	5		X	2	16.66	15	20.01
		10	X					
	Performance evaluation, monitoring and measurement of a SCSMS based on ISO 28000	5		X	3	25	20	26.68
		5		X				
		10	X					
	Continual improvement of a SCSMS based on ISO 28000	5		X	1	8.33	5	6.67
	Preparing for a SCSMS certification audit	5	X		1	8.33	5	6.67
	Total Points	75	5	7				
	Number of questions per level of understanding							
	% of test devoted to each level of understanding (cognitive taxonomy)		42	58				

The passing score is established at **70%.**

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

TAKE A CERTIFICATION EXAM

Candidates will be required to arrive at least thirty (30) minutes before the beginning of the certification exam. Candidates arriving late will not be given additional time to compensate for the late arrival and may be denied entry to the exam room (if they arrive more than 5 minutes after the beginning of the exam scheduled time).

All candidates will need to present a valid identity card with a picture such as a driver's license or a government ID to the invigilator.

The exam duration is three (3) hours.

The questions are essay type questions. This type of format was chosen because the intent is to determine whether an examinee can write a clear coherent answer/argument and to assess problem solving techniques. Because of this particularity, the exam is set to be “open book” and does not measure the recall of data or information. The examination evaluates, instead, comprehension, application, analysis, synthesis and evaluation, which mean that even if the answer is in the course material, candidates will have to justify and give explanations, to show they really understood the concepts. At the end of this document, you will find sample exam questions and their possible answers.

As the exams are “open book”; candidates are authorized to use the following reference materials:

- A copy of the ISO 28000:2007 standard,
- Course notes from the Participant Handout,
- Any personal notes made by the student during the course and
- A hard copy dictionary.

The use of electronic devices, such as laptops, cell phones, etc., is not allowed.

All attempt to copy, collude or otherwise cheat during the exam will automatically lead to the exam's failure.

PECB exams are available in English. For availability of the exam in a language other than English, please contact examination@pecb.com.

RECEIVE YOUR EXAM RESULTS

Results will be communicated by email in a period of 6 to 8 weeks, after taking the exam. The results will not include the exact grade of the candidate, only a mention of pass or fail.

Candidates who successfully complete the examination will be able to apply for a certified scheme.

In the case of a failure, the results will be accompanied with the list of domains in which the candidate had a low grade, to provide guidance for exams' retake preparation.

Candidates who disagree with the exam results may file a complaint. For more information, please refer to www.pecb.com

EXAM RETAKE POLICY

There is no limit on the number of times a candidate may retake an exam. However, there are some limitations in terms of allowed time-frame in between exam retakes, such as:

- If a candidate does not pass the exam on the first attempt, he/she must wait 15 days for the next attempt (1st retake). Retake fee applies.

Note: *Students, who have completed the full training but failed the written 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 second attempt, he/she must wait 3 months (from the initial date of the exam) for the next attempt (2nd retake). Retake fee applies.
- If a candidate does not pass the exam on the third attempt, he/she must wait 6 months (from the initial date of the exam) for the next attempt (3rd retake). Retake fee applies.

After the fourth attempt, a waiting period of 12 months from the last session date is required, in order for candidate to sit again for the same exam. Regular fee applies.

For the candidates that fail the exam in the 2nd retake, PECB recommends to attend an official training in order to be better prepared for the exam.

To arrange exam retakes (date, time, place, costs), the candidate needs to contact the PECB partner who has initially organized the session.

CLOSING FILES

Closing a file is equivalent to rejecting a candidate’s application. As a result, when candidates request that their file be reopened, PECB will no longer be bound by the conditions, standards, policies, candidate handbook or exam preparation guide that were in effect before their file was closed.

Candidates who want to request that their file be reopened must do so in writing, and pay the required fees.

EXAMINATION SECURITY

A significant component of a successful and respected professional certification credential is maintaining the security and confidentiality of the examination. PECB relies upon the ethical behaviour of certificate holders and applicants to maintain the security and confidentiality of PECB examinations. When someone who holds PECB credentials reveals information about PECB examination content, they violate the PECB Code of Ethics. PECB will take action against individuals who violate PECB Policies and the Code of Ethics. Actions taken may include permanently barring individuals from pursuing PECB credentials and revoking certifications from those who have been awarded the credential. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

SAMPLE EXAM QUESTIONS AND POSSIBLE ANSWERS

1. Interpretation of ISO clauses

For each of the following clauses of the ISO 28000 standard, please provide an action plan with at least two concrete actions that would be acceptable to ensure conformity to the clause.

4.3.4 Security management targets

Possible answers:

- Document realistic targets consistent with the security management objectives
- Communicate the targets to the employees

2. Development of metrics

For each of the following clauses of the ISO 28000 standard, please provide two examples of metrics that would be acceptable to measure the conformity to the clause.

- **4.6 Management review and continual improvement**

Possible answers:

- Management review meetings completed to date
- Average participation rates in management review meetings to date