PECB

When Recognition Matters

EXAM PREPARATION GUIDE

PECB Certified ISO 18788 Lead Auditor

The objective of the "**PECB Certified ISO 18788 Lead Auditor**" exam is to ensure that the candidate possesses the necessary expertise to perform a Security Operations Management System (SOMS) audit and to manage an audit team by applying widely recognized audit principles, procedures and techniques. The aim of the exam is to evaluate that the candidate possesses the knowledge and skills to proficiently plan and carry out internal and external audits in compliance with ISO 19011 and ISO/IEC 17021-1 certification process.

The ISO 18788 Lead Auditor exam is intended for:

- Auditors seeking to perform and lead Security Operations Management System (SOMS) certification audits
- Managers or consultants seeking to master a Security Operations Management System audit process
- Individuals responsible for maintaining conformance with SOMS requirements
- Technical experts seeking to prepare for a Security Operations Management System audit
- Expert advisors in a Security Operations Management

The exam covers the following competency domains:

- **Domain 1:** Fundamental principles and concepts of a Security Operations Management System (SOMS)
- **Domain 2:** Security Operations Management Systems (SOMS)
- **Domain 3:** Fundamental audit concepts and principles
- **Domain 4:** Preparation of an ISO 18788 audit
- **Domain 5:** Conducting an ISO 18788 audit
- **Domain 6:** Closing an ISO 18788 audit
- **Domain 7:** Managing an ISO 18788 audit programme

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts of a Security Operations Management System (SOMS)

Main objective: Ensure that the ISO 18788 Lead Auditor candidate understands, and is able to interpret and illustrate the main Security Operations Management concepts and principles.

Competencies	Knowledge statements
1. Ability to understand and explain the organization`s operations and the development of Security Operations Management standards. 2. Ability to explain and illustrate the main concepts of Security Operations Management. 3. Ability to interpret the advantages of effective Security Operations Management in an organization. 4. Ability to understand the Security Operations Management principles.	1. Knowledge of the application of the seven ISO management principles in Security Operations Management. 2. Knowledge of the main concepts and terminology as described in the ISO 18788 standard. 3. Knowledge of the different sources of Security Operations Management requirements for an organization, including: laws, regulations, international and industry standards, contracts, market practices, internal policies. 4. Knowledge of the main advantages and benefits that organizations can gain by the effective implementation of a risk management process. 5. Knowledge of the main Security Operations Management concepts and terminology as described in ISO 18788.

Domain 2: Security Operations Management Systems (SOMS)

Main objective: Ensure that the ISO 18788 Lead Auditor candidate can understand,interpret and illustrate the main concepts and components of a Security Operations Management System based on ISO 18788.

Competencies	Knowledge statements
1. Ability to understand and explain the components of a Security Operations Management System based on ISO 18788 and its principal processes. 2. Ability to interpret and analyze the ISO 18788 requirements. 3. Ability to understand and explain the main steps to establish, implement, operate, monitor, review, maintain and improve an organization's SOMS.	1. Knowledge of the concepts, principles and terminology related to management systems. 2. Knowledge of the principal characteristics of an integrated management system. 3. Knowledge of the main advantages of a certification to an organization. 4. Knowledge of the ISO 18788 requirements. 5. Knowledge of the main steps to establish the security operations objectives, processes and procedures relevant to managing and improving Security Operations so as 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 a SOMS.

Domain 3: Fundamental audit concepts and principles

Main objective: Ensure that the ISO 18788 Lead Auditor candidate can understand, interpret and apply the main concepts and principles related to a SOMS audit in the context of ISO 18788.

Competencies	Knowledge statements
1. Ability to understand, explain and illustrate the application of the audit principles in the context of an ISO 18788 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 18788 audit. 5. Ability to explain and compare the types and characteristics of evidence. 6. Ability to determine and evaluate the level of materiality and apply the risk-based approach during the different phases of an ISO 18788 audit. 7. Ability to judge the approproate level of reasonable assurance needed for a specific ISO 18788 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 audits. 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 the 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 the 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 risks 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 application in an audit.

Domain 4: Preparation of an ISO 18788 audit

Main objective: Ensure that the ISO 18788 Lead Auditor candidate can prepare appropriately a SOMS audit in the context of ISO 18788.

Competencies	Knowledge statements
1. Ability to understand and explain the steps and activities to prepare a SOMS audit taking into 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 18788 audit mission. 4. Ability to do a feasibility study of an audit in the context of a specific ISO 18788 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 18788 audit mission. 6. Ability to develop audit working papers and to elaborate appropriate audit test plans in the context of a specific ISO 18788 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 in an audit. 3. Knowledge of the definitions related to the audit objectives, audit scope and audit criteria. 4. Knowledge of the difference between the SOMS 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 papers. 10. Knowledge of the advantages and disadvantages of using audit checklists. 11. Knowledge of the best practices to create audit test plans.

Domain 5: Conducting an ISO 18788 audit

Main objective: Ensure that the ISO 18788 Lead Auditor candidate can efficiently conduct a SOMS audit in the context of ISO 18788.

Competencies	Knowledge statements
1. Ability to organize and conduct the opening meeting in the context of a specific ISO 18788 audit mission. 2. Ability to conduct a stage 1 audit in the context of a specific ISO 18788 audit mission and take into account the documentation review conditions and criteria. 3. Ability to conduct a stage 2 audit in the context of a specific ISO 18788 audit mission by applying the best practices of communication to collect the appropriate evidence and take into account the roles and responsibilities of all the individuals 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 between stage 1 audit and 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 18788. 6. Knowledge of stage 2 audit requirements, steps and activities. 7. Knowledge of the best practices of communication during an audit. 8. Knowledge of the roles and responsibilities of guides and observers during an audit. 9. Knowledge of 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 the 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 18788 audit

Main objective: Ensure that the ISO 18788 Lead Auditor candidate can conclude a SOMS audit and conduct follow-up activities in the context of ISO 18788.

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 benefit of the doubt principle. 3. Ability to report appropriate audit observations in order to help an organization improve its SOMS by respecting the audit rules and principles. 4. Ability to complete audit working documents and conduct a quality review of an ISO 18788 audit. 5. Ability to draft audit conclusions and present them to the management of the audited organization. 6. Ability to organize and conduct an audit closing meeting. 7. Ability to write an ISO 18788 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, and observation. 3. Knowledge of the guidelines and best practices to write a nonconformity report. 4. Knowledge of the guidelines and best practices used to draft and report audit observations. 5. Knowledge of the principle of the benefit of the doubt and its application in the context of an audit. 6. Knowledge of the guidelines and best practices used to complete audit working documents and conduct a quality review of an audit. 7. Knowledge of the guidelines and best practices to present audit findings and conclusions to the 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 audits, surveillance audits and recertification audit requirements, steps and activities. 11. Knowledge of the conditions for the modification, extension, suspension or withdrawal of a certification for an organization.

Domain 7: Managing an ISO 18788 audit programme

Main objective: Ensure that the ISO 18788 Lead Auditor understands how to establish and manage a SOMS audit programme.

Competencies	Knowledge statements
1. Ability to understand and explain the establishment of an audit program. 2. Ability to understand and explain the implementation of an ISO 18788 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, record management, and complaint management. 5. Ability to understand the evaluation of the efficiency of the audit program by monitoring the performance of each auditor, each team and the entire certification body. 6. Ability to understand and explain the way combined audits are handled in an audit program. 7. Ability to demonstrate the application of the personal attributes and behavior of a professional auditor.	1. Knowledge of the management of an audit program. 2. Knowledge of the 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 the requirements, guidelines and best practices regarding the management of audit records. 5. Knowledge of the application of the concept of continual improvement 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 management of combined audit activities. 8. Knowledge of the concept of competency and its application to auditors. 9. Knowledge of the personal attributes and behavior of a professional auditor.

Based on these 7 domains and their relevance, 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 Security Operations Management Systems (SOMS)	5	X		1	8.33	5	6.67
	Security Operations Management Systems (SOMS)	5	X		1	8.33	5	6.67
	Fundamental audit concepts and principles	5	X		3	25.00	15	20.01
		5	X					
		5	X					
	Preparation of an ISO 18788 audit	5		X	1	8.33	5	6.67
	Conducting an ISO 18788 audit	5		X	4	33.32	35	46.69
		10		X				
		10		X				
		10		X				
	Closing an ISO 18788 audit	5		X	1	8.33	5	6.67
	Managing an ISO 18788 audit programme	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)		41.67	58.33				

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

After successfully passing the exam, candidates will be able to apply for the "PECB Certified ISO 18788 Lead Auditor" credential, depending on their level of experience.

TAKE A CERTIFICATION EXAM

Candidates will be required to arrive at least thirty (30) minutes before the start of the certification exam. Candidates arriving late will not be given compensatory time for the late arrival and may be denied entry to the exam.

All candidates are required to present a valid identity card such as a national ID card, driver's license, or passport to the invigilator.

The exam duration is three (3) hours. Non-native speakers recive an additional of thirty (30) minutes.

The exam contains essay type questions: This type of format was selected as a means of determining whether an examinee can clearly answer training related questions, by assessing problem solving techniques and formulating arguments supported with reasoning and evidence. The exam is set to be “open book”, and does not measure the recall of data or information. The examination evaluates the candidates’ comprehension, application and analyzing skills. Therefore, candidates will have to justify their answers by providing concrete explanations as to demonstrate that they have been capable of understanding the training concepts. At the end of this document, you will find samples of exam questions and potential answers.

As the exam is “open book”; candidates are authorized to use:

- A copy of the ISO 18788 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 attempts to copy, collude or otherwise cheat during the exam will automatically lead to the failure of the exam.

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 within a period of 6 to 8 weeks from your examination date. The candidate will be provided with only two possible examination results: pass or fail, rather than an exact grade.

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

In case of a failure, the results will be accompanied with the list of domains where the candidate failed to fully answer the question. This can help the candidate better prepare for a retake exam.

Candidates who disagree with the exam results may file a complaint by writing to examination@pecb.com. 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 the 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 the candidate to retake 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 A CASE

If an applicant does not apply for his/her certificate within three years, their case will be closed. Even though an applicant's certification period expires they have the right to reopen their case, however, PECB will no longer be responsible for any changes regarding the conditions, standards, policies, candidate handbook or exam preparation guide that were applicable before the applicant's case was closed. Applicants requesting their case to reopen 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 behavior 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, he/she violates 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 ANSWER

Question 1: Evaluation of corrective actions

You have received a corrective action plan to review. Please evaluate the adequacy of the proposed corrective actions by justifying your answer in case you find the corrective actions suitable, and propose alternative corrective actions if you consider them to be inappropriate.

Nonconformity: A nonconformity was detected because only 5 out of 18 employees were not aware of the existence of a security operations policy within the organization.

Corrective action: Inform the top management (timeframe: immediately), and take appropriate actions to communicate the security operations policy within the organization, and make it available.

Possible answer:

The corrective actions taken eliminate the identified problem at its root. The auditor can then evaluate whether the corrective action has been implemented effectively during the surveillance audit.

Question 2: Writing of a test plan

Please write a test plan to validate whether the requirements of the following clauses are fulfilled by employing the different applicable audit procedures (observation, documentation review, interview, technical verification, and analysis).

- **Clause 7.5.3 Control of documented information**

Possible answer:

Clause 7.5.3 Control of documented information Documented information required by the SOMS and by this International Standard shall be controlled to ensure: a) it is available and suitable for use, where and when it is needed; b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).	
Observation	Observe how employees ensure the protection of documented information and whether those actions are consistent with the organization's policies and procedures.
Document	Review the policy on documented information management and the procedures on information lifecycle management: their identification, storage, backup, protection, accessibility and conservation.
Interview	Conduct an interview with a member of management (to confirm the policies and the organization's needs related to documented information) and the personnel responsible for information management and archiving (to obtain the documented information management details).
Technical verification	Validate the electronic structure for classifying and storing documented information, verify their protection mechanisms, and observe the compilation of the automated journals report.
Analysis	Select documented information samples and verify if they respect the documentation structure and policy criteria on documented information.