PECB

When Recognition Matters

EXAM PREPARATION GUIDE

PECB Certified ISO 18788 Lead Implementer

The objective of the "**PECB Certified ISO 18788 Lead Implementer**" examination is to ensure that the candidate has acquired the necessary skills and competencies to support an organization in establishing, implementing, managing and maintaining a Security Operations Management System (SOMS) based on ISO 18788.

The target population for this examination:

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

The exam content covers the following competency domains:

- **Domain 1:** Fundamental principles and concepts of a Security Operations Management System (SOMS)
- **Domain 2:** Security Operations Management System (SOMS)
- **Domain 3:** Planning a SOMS implementation based on ISO 18788
- **Domain 4:** Implementing a SOMS based on ISO 18788
- **Domain 5:** Performance evaluation, monitoring and measurement of a SOMS based on ISO 18788
- **Domain 6:** Continual improvement of a SOMS based on ISO 18788
- **Domain 7:** Preparing for a SOMS certification audit

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 Implementer candidate can understand, interpret and illustrate the main Security Operations Management concepts and principles related to a Security Operations Management System (SOMS)

Competencies	Knowledge statements
1. Ability to explain the operations of the organization and the development of a Security Operations Management System (SOMS) 2. Ability to identify, analyze and evaluate the security operations management compliance requirements for an organization 3. Ability to explain and illustrate the main concepts of a security operations management system	1. Knowledge of the seven ISO management principles application in security operations management 2. Knowledge of the different sources of requirements regarding security operations management for an organization: human rights law, regulations, contracts, internal policies and common practices 3. Knowledge of the main concepts and terminology of security operations management as described in ISO 18788

Domain 2: Security Operations Management Systems (SOMS)

Main objective: Ensure that the ISO 18788 Lead Implementer candidate can understand, interpret and provide guidance on how to implement Security Operations Management requirements based on the best practices of ISO 18788

Competencies	Knowledge statements
1. Ability to identify, understand, classify and explain the requirements of the ISO 18788 clauses 2. Ability to detail and illustrate the requirements and best practices through concrete examples 3. Ability to compare possible solutions to security operations management issues when dealing with a country where governance may be weak and the rule of law undermined 4. Ability to select and demonstrate the best security operations management solutions in order to address the security operations objectives set by the organization 5. Ability to create and justify an action plan for implementing a security operations management system 6. Ability to analyze, evaluate and validate action plans to implement a specific requirement	1. Knowledge of ISO 18788 requirements 2. Knowledge of various security operations methodologies and their incorporation into the organizational security operations management system based on ISO 18788 3. Knowledge of security operations strategies 4. Knowledge of establishing and implementing security operations procedures 5. Knowledge of the best practices in security operations 6. Knowledge of the requirements of clauses 4 to 10 of ISO 18788 7. Knowledge on continual improvement and practical implementation based on ISO 18788

Domain 3: Planning a SOMS implementation based on ISO 18788

Main objective: Ensure that the ISO 18788 Lead Implementer candidate can plan the implementation of a SOMS and prepare for an ISO 18788 certification

Competencies	Knowledge statements
1. Ability to manage a SOMS implementation project by following the best practices 2. Ability to observe, analyze and interpret the necessary information to plan the SOMS implementation 3. Ability to observe, analyze and interpret the internal and external context of an organization 4. Ability to perform a Gap Analysis and clarify the Security Operations objectives of an organization 5. Ability to state and justify a SOMS scope based on the security operations objectives of an organization 6. Ability to select approaches and methodologies and tailor them to the needs of the organization 7. Ability to perform the different steps of the risk assessment phases	1. Knowledge of the main security operations concepts, terminology, process and best practices 2. Knowledge of the principal approaches and methodology frameworks to implement a SOMS 3. Knowledge of the main concepts and terminology related to organizations 4. Knowledge of the main interested parties related to an organization and their characteristics 5. Knowledge of the techniques used to gather information on an organization and perform a Gap Analysis of a management system 6. Knowledge of the characteristics of a SOMS scope in terms of organizational, security operations services and physical boundaries 7. Knowledge of different approaches and main methodology characteristics to perform a risk assessment 8. Knowledge of the main activities of the risk identification, analysis and evaluation related to the SOMS of an organization

Domain 4: Implementing a SOMS based on ISO 18788

Main objective: Ensure that the ISO 18788 Lead Implementer candidate can implement the processes of a SOMS required for an ISO 18788 certification

Competencies	Knowledge statements
1. Ability to understand and analyze the needs of the organization, and to provide guidance on the attribution of roles and responsibilities in the context of the SOMS implementation and management 2. Ability to define the documentation and record management processes needed to support the implementation and operations of a SOMS 3. Ability to define processes and properly document them 4. Ability to define and establish SOMS policies and procedures 5. Ability to implement the required processes of the SOMS 6. Ability to define and implement appropriate security operations training, awareness and communication plans	1. Knowledge for the roles and responsibilities of the key interested parties during and after the implementation and operations of a SOMS 2. Knowledge of the main organizational structures applicable for an organization to manage security operations 3. Knowledge of the best practices on documentation and record management processes and the documentation management lifecycle 4. Knowledge of the characteristics and differences between the different documents related to SOMS: policies, procedures, guidelines, standards etc. 5. Knowledge of model-building controls, process techniques and best practices 6. Knowledge of implementing processes, controls, best practices and techniques 7. Knowledge of the techniques and best practices used to establish security operations management policies, procedures and other types of documentation included in the SOMS 8. Knowledge of the characteristics and the best practices to implement security operations training, awareness and communication plans

Domain 5: Performance evaluation, monitoring and measurement of a SOMS based on ISO 18788

Main objective: Ensure that the ISO 18788 Lead Implementer candidate can evaluate, monitor and measure the performance of a SOMS in the context of an ISO 18788 certification

Competencies	Knowledge statements
1. Ability to monitor and evaluate the effectiveness of a SOMS 2. Ability to verify to what extent the identified Security Operations Management requirements have been met 3. Ability to define and implement an internal audit program for ISO 18788 4. Ability to perform regular and methodical reviews regarding the suitability, adequacy, effectiveness and efficiency of a SOMS based on the policies and objectives of the 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 a SOMS 2. Knowledge of the main concepts and components related to a Security Operations Management Measurement Programme: measures, attributes, indicators, dashboards, etc. 3. Knowledge of the characteristics and differences between operational, tactical and strategic Security Operations Management indicators and dashboards 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 of a SOMS internal audit program 6. Knowledge of the differences between the concepts of major and minor nonconformities, irregularities and observations 7. Knowledge of the guidelines and best practices to write a nonconformity report 8. Knowledge of the best practices on how to perform management reviews

Domain 6: Continual improvement of a SOMS based on ISO 18788

Main objective: Ensure that the ISO 18788 Lead Implementer candidate can provide guidance on the continual improvement of a SOMS in the context of ISO 18788

Competencies	Knowledge statements
1. Ability to understand the principles and concepts related to continual improvement 2. Ability to counsel an organization on how to continually improve the effectiveness and the efficiency of a SOMS 3. Ability to implement SOMS continual improvement processes in an organization 4. Ability to determine the appropriate tools to support continual improvement processes of a private security operations organization 5. Ability to identify and analyze the root-causes of nonconformities, and propose action plans to treat them	1. Knowledge of the main concepts related to continual improvement 2. Knowledge of the characteristics and differences between the concepts of effectiveness and efficiency 3. Knowledge of the main processes, tools and techniques used by professionals to identify the root-causes of nonconformities 4. Knowledge of the characteristics and the differences between corrective and preventive actions 5. Knowledge of the main processes, tools and techniques used by professionals to develop and propose the best corrective and preventive action plans

Domain 7: Preparing for a SOMS certification audit

Main objective: Ensure that the ISO 18788 Lead Implementer candidate can prepare and assist an organization in the certification against the ISO 18788 standard

Competencies	Knowledge statements
1. Ability to understand the main steps, processes and activities related to an ISO 18788 certification audit 2. Ability to understand, explain and illustrate the audit evidence approach in the context of an ISO 18788 audit 3. Ability to counsel an organization to identify and select a certification body that meets its' needs 4. Ability to review the readiness of an organization for an ISO 18788 certification audit 5. Ability to coach and prepare an organization's personnel for an ISO 18788 certification audit 6. Ability to argue and challenge the audit findings and conclusions with external auditors	1. Knowledge of the evidence based approach in an audit 2. Knowledge of the different types of evidence: physical, mathematical, confirmative, technical, analytical, documentary and verbal 3. Knowledge of the differences between Stage 1 and Stage 2 audits 4. Knowledge of Stage 1 audit requirements, steps and activities 5. Knowledge of the documentation review criteria 6. Knowledge of Stage 2 audit requirements, steps and activities 7. Knowledge of follow-up audit requirements, steps and activities 8. Knowledge of surveillance audits and recertification audit requirements, steps and activities 9. Knowledge of the requirements, guidelines and best practices to develop action plans following an ISO 18788 certification audit

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 System (SOMS)	5	X		1	8.33	5	6.67
	Security Operations Management System (SOMS)	5	X		1	8.33	5	6.67
	Planning a SOMS implementation based on ISO 18788	5	X		2	16.67	10	13.34
		5	X					
	Implementing a SOMS based on ISO 18788	10		X	4	33.34	25	33.35
		5		X				
		5		X				
		5		X				
	Performance evaluation, monitoring and measurement of a SOMS based on ISO 18788	10		X	2	16.67	20	26.68
		10		X				
	Continual improvement of a SOMS based on ISO 18788	5		X	1	8.33	5	6.67
	Preparing for a SOMS certification audit	5		X	1	8.33	5	6.67
	Total points	75	4	8				
	Number of questions per level of understanding							
	% of test devoted to each level of understanding (cognitive/taxonomy)		33.32	66.64				

The passing score is **70%**.

After successfully passing the exam, candidates will be able to apply for the "**PECB Certified ISO 18788 Lead Implementer**" credential, 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 that arrive 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 start of the examination).

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 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 failure, the results will be accompanied with the list of domains in which the candidate had received low grading as to provide guidance in case of retaking the 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: *Candidates, who have completed the full training but failed the written exam, are eligible to retake the exam once free of charge 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 FILES

Closing a file is equivalent to rejecting a candidate's application. As a result, 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 request to reopen their file must do so in writing, and pay the associated fees.

EXAMINATION SECURITY

A significant component of a successful and respected professional certification credential is maintaining the security and confidentiality of the examination content. 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 the PECB examination content, they violate the PECB Code of Ethics. PECB will take action against individuals who violate the PECB Policies and 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 remedies against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property rights.

SAMPLE EXAM QUESTIONS AND POSSIBLE ANSWERS

1. Interpretation of ISO clauses

For each of the following clauses of ISO 18788, please provide an action plan with at least two concrete actions to ensure conformity to the clause.

Clauses:

1. **Clause 7.4.5** Communicating whistle blower policy
2. **Clause 9.1** Monitoring, measurement, analysis and evaluation

Please refer to the example below:

Clause 5.1 *Leadership and commitment*

- *Establish the security operations policy and objectives compatible with the organization's strategic direction*
- *Integrate the requirements of ISO 18788 into the security organization*

Possible answer:

1. **Clause 7.4.5** Communicating whistle blower policy

- *Organize awareness sessions to communicate the whistle blower policy and its importance to all employees within the organization*
- *Develop a communication strategy and document it*

2. **Clause 9.1** Monitoring, measurement, analysis and evaluation

- *Monitor the effectiveness of the SOMS to ensure that the security operations objectives and targets are achieved*
- *Analyze the results from monitoring and measurement, and evaluate them accordingly*

2. Recommendations

The organization's management would like you to provide recommendations to improve the processes in place so as to comply with the ISO 18788 requirements on the control of documented information.

Possible answer:

- *Document and implement a procedure for the control of documented information.*
- *Maintain a log for documenting changes with records of approvals.*
- *Communicate the new process and organize the training sessions.*