PECB

When Recognition Matters

EXAM PREPARATION GUIDE

PECB Certified ISO/IEC 27001 Lead Implementer

The objective of the “PECB Certified ISO/IEC 27001 Lead Implementer” examination is to ensure that the candidate has the knowledge and the skills to support an organization in implementing and managing an Information Security Management System (ISMS) based on ISO/IEC 27001:2013.

The target population for this examination is:

- Project managers or consultants seeking to prepare and to support an organization in the implementation of an Information Security Management System (ISMS)
- ISO/IEC 27001 auditors who wish to fully understand the Information Security Management System implementation process
- Managers responsible for the IT governance of an enterprise and the management of its risks
- Members of an information security team
- Expert advisors in information technology
- Technical experts seeking to prepare for an information security function or an ISMS project management function

The exam content covers the following domains:

- **Domain 1**: Fundamental principles and concepts of an Information Security Management System (ISMS)
- **Domain 2**: Information Security Management System controls and best practices based on ISO/IEC 27002
- **Domain 3**: Planning an ISMS implementation based on ISO/IEC 27001
- **Domain 4**: Implementing an ISMS based on ISO/IEC 27001
- **Domain 5**: Performance evaluation, monitoring and measurement of an ISMS based on ISO/IEC 27001
- **Domain 6:** Continual improvement of an ISMS based on ISO/IEC 27001
- **Domain 7**: Preparation for an ISMS certification audit

The content of the exam is divided as follows:

Domain 1: Fundamental Principles and Concepts of an Information Security Management System (ISMS)

Main objective: To ensure that the ISO/IEC 27001 Lead Implementer candidate can understand, interpret and illustrate the main information security concepts related to an Information Security Management System (ISMS).

Competencies	Knowledge statements
1. Understand and explain the operations of the ISO organization and the evolution of information security standards. 2. Ability to identify, analyze and evaluate the information security compliance requirements for an organization. 3. Ability to explain and illustrate the main concepts in information security and information security risk management. 4. Ability to distinguish and explain the difference between information asset, data and record. 5. Understand, interpret and illustrate the relationship between the concepts of asset, vulnerability, threat, impact and controls.	1. Knowledge of the application of the eight ISO management principles to information security. 2. Knowledge of the main standards in information security. 3. Knowledge of the different sources of information security requirement for an organization: laws, regulations, international and industry standards, contracts, market practices, internal policies. 4. Knowledge of the main information security concepts and terminology as described in ISO 27000. 5. Knowledge of the concept of risk and its application in information security. 6. Knowledge of the relationship between the concepts of asset, vulnerability, threat, impact and controls. 7. Knowledge of the difference and characteristics of security objectives and controls. 8. Knowledge of the difference between preventive, detective and corrective controls and their characteristics.

Domain 2: Information Security Management System controls and best practices based on ISO/IEC 27002

Main objective: To ensure that the ISO/IEC 27001 Lead Implementer candidate can understand, interpret and provide guidance on how to implement and manage information security controls best practices based on ISO/IEC 27001.

Competencies	Knowledge statements
1. Ability to identify, understand, classify and explain the 10 clauses, 34 security categories and 114 controls of ISO/IEC 27001. 2. Ability to detail and illustrate the security controls best practices by concrete examples. 3. Ability to compare possible solutions to a real security issue of an organization and identify/analyze the strength and weakness of each solution. 4. Ability to select and demonstrate the best security controls in order to address information security control objectives stated by the organization. 5. Ability to create and justify a detailed action plan to implement a security control by listing the activities related. 6. Ability to analyze, evaluate and validate action plans to implement a specific control.	1. Knowledge of Information Security Policy Controls Best Practices. 2. Knowledge of Organizing Information Security Controls Best Practices. 3. Knowledge of Asset Management Controls Best Practices. 4. Knowledge of Human Resources Security Controls Best Practices. 5. Knowledge of Physical and Environmental Security Physical and Environmental Security Controls Best Practices. 6. Knowledge of Communications and Operations Management Controls Best Practices. 7. Knowledge of Access Control Controls Best Practices. 8. Knowledge of Information Systems Acquisition, Development and Maintenance Controls Best Practices. 9. Knowledge of Information Security Incident Management Controls Best Practices. 10. Knowledge of Business Continuity Management Controls Best Practices. 11. Knowledge of Compliance Controls Best Practices.

Domain 3: Planning an ISMS implementation based on ISO/IEC 27001

Main objective: To ensure that the ISO/IEC 27001 Lead Implementer candidate can plan the implementation of an ISMS in preparation for an ISO/IEC 27001 certification.

Competencies	Knowledge statements
1. Ability to manage an ISMS implementation project following project management best practices. 2. Ability to gather, analyze and interpret the necessary information to plan the ISMS 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 information security objectives of an organization. 5. Ability to state and justify an ISMS scope adapted to the security objectives of a specific organization. 6. Ability to select and justify the selected approach and methodology adapted to the needs of the organization. 7. Ability to perform the different steps of the risk assessment and risk treatment phases. 8. 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 ISMS. 9. Ability to state and justify a Statement of Applicability for a specific organization	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 ISMS. 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 ISMS scope in terms of organizational, technological and physical boundaries. 8. Knowledge of the different approaches and main methodology characteristics to perform a risk assessment. 9. Knowledge of the main activities of the risk identification, estimation, evaluation related to the assets included in the ISMS of an organization. 10. Knowledge of the main activities of the risk treatment related to the assets included in the ISMS of an organization 11. Knowledge of the main organizational structures applicable for an organization to manage information security. 12. Knowledge of the characteristics of a statement of applicability.

Domain 4: Implementing an ISMS based on ISO/IEC 27001

Main objective: To ensure that the ISO/IEC 27001 Lead Implementer candidate can implement the processes and security controls of an ISMS required for an ISO/IEC 27001 certification.

Competencies	Knowledge statements
1. Ability to define and design security controls & processes and document them. 2. Ability to implement the required processes and security controls of an ISMS. 3. Ability to define the document and record management processes needed to support the implementation and the operations of an ISMS. 4. Ability the define and writing a ISMS policy and information security policies & procedures. 5. Ability to define and implement appropriate information security training, awareness and communication plans. 6. Ability to transfer an ISMS project to operations and manage the change management process. 7. Ability to define and implement an incident management process based on information security best practices.	1. Knowledge of the roles and responsibilities of the key actors during and after the end of the implementation of an ISMS 2. Knowledge of model-building controls and processes techniques and best practices. 3. Knowledge of controls and processes deployment techniques and best practices. 4. Knowledge of the best practices on document and record management processes and the document management life cycle. 5. Knowledge of the characteristics and the differences between the different documents related to ISMS: policy, procedure, guideline, standard, baseline, worksheet, etc. 6. Knowledge of techniques and best practices to write information security policies, procedures and others types of documents include in an ISMS. 7. Knowledge of the characteristics and the best practices to implement information security training, awareness and communication plans. 8. Knowledge of change management techniques best practices. 9. Knowledge of the characteristics and main processes of an information management incident management process based on best practices.

Domain 5: Performance Evaluation, Monitoring and Measurement of an ISMS Based on ISO/IEC 27001

Main objective: To ensure that the ISO/IEC 27001 Lead Implementer candidate can evaluate, monitor and measure the performance of an ISMS in the context of an ISO/IEC 27001 certification.

Competencies	Knowledge statements
1. Ability to monitor and evaluate the effectiveness of an ISMS in operation. 2. Ability to verify the extent to which identified security requirements have been met. 3. Ability to define and implement an internal audit program for ISO/IEC 27001. 4. Ability to perform regular and methodical reviews regarding the suitability, adequacy, effectiveness and efficiency of an ISMS with policies and security objectives of an organization. 5. Ability to define and implement a management review process.	1. Knowledge of the techniques and best practices to monitor the effectiveness of an ISMS. 2. Knowledge of the main concepts and components related to an Information Security Measurement Programme: measures, attributes, indicators, dashboard, etc. 3. Knowledge of the characteristics and the differences between an operational, tactical and strategic information security 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 ISMS 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 an ISMS based on ISO/IEC 27001

Main objective: To ensure that the ISO/IEC 27001 Lead Implementer candidate can provide guidance on the continuous improvement of an ISMS in the context of ISO/IEC 27001.

Competencies	Knowledge statements
1. Ability to understand the principle and concepts related to continual improvement. 2. Ability to counsel an organization on how to continually improve the effectiveness and the efficiency of an ISMS. 3. Ability to implement ISMS continual improvement processes in an organization. 4. Ability to determine the appropriate business improvement tools to support continual improvement processes of a specific organization. 5. Ability to identify, analyze the root-causes of potential nonconformities and propose action plans to treat them.	1. Knowledge of the main concepts related to continual improvement. 2. Knowledge of the characteristics and the differences between the concept of effectiveness and the efficiency. 3. Knowledge of the concept and techniques to perform a benchmarking. 4. Knowledge of the main processes, tools and techniques used by professionals to identify the root-causes of nonconformities. 5. Knowledge of the characteristics and the difference between corrective actions and preventive actions. 6. Knowledge of the main processes, tools and techniques used by professionals to develop and proposed the best corrective and preventive action plans.

Domain 7: Preparing for an ISMS certification audit

Main objective: To ensure that the ISO/IEC 27001 Lead Implementer candidate can prepare and assist an organization for the certification of an ISMS against the ISO/IEC 27001 standard.

Competencies	Knowledge statements
1. Ability to understand the main steps processes and activities related to an ISO/IEC 27001 certification audit. 2. Ability to understand, explain and illustrate the audit evidence approach in the context of an ISO/IEC 27001 audit. 3. Ability to counsel an organization to identify and select a certification body that meets their needs. 4. Ability to review the readiness of an organization for an ISO/IEC 27001 certification audit. 5. Ability to coach and prepare the personnel of an organization for an ISO/IEC 27001 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 evidences: physical, mathematical, confirmative, technical, analytical, documentary and verbal. 3. Knowledge of the difference of the stage 1 audit and the stage 2 audit. 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/IEC 27001 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 content area	% of test devoted to each content area	Number of points per competency domain	% of Points per competency domain
Content Area/Competence Domains	Fundamental principles and concepts of Information Security Management System (ISMS)	5	X		3	25	20	26.67
		5	X					
		10	X					
	Information Security Management System controls and best practices based on ISO/IEC 27002	5	X		1	8.33	5	6.67
	Planning an ISMS implementation based on ISO/IEC 27001	5		X	1	8.33	5	6.67
	Implementing an ISMS based on ISO/IEC 27001	10	X		1	8.33	10	13.33
	Performance evaluation, monitoring and measurement of an ISMS based on ISO/IEC 27001	5		X	3	25	20	26.67
		10		X				
		5		X				
	Continual improvement of an ISMS based on ISO/IEC 27001	5		X	2	16.67	10	13.33
		5		X				
	Preparing for an ISMS certification audit	5		X	1	8.33	5	6.67
Total Points		75						
Number of Questions per level of understanding			5	7				
% 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 credentials of PECB Certified ISO/IEC 27001 Lead Implementer, depending on their level of experience.

TAKE THE 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/IEC 27001:2013 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. Security controls

For each of the following clauses of the ISO/IEC 27001 standard, please provide an action plan with at least two concrete actions that would be acceptable to ensure conformity to the clause and satisfy the control objectives.

- **Determining the necessary competencies of person(s) doing work under its control that affects its information security performance (Clause 7.2 a)**

Possible answers:

- Determine the qualifications necessary for the operations of each security control included in the ISMS.
- Describe the necessary qualifications for each position occupied by the personnel related to ISMS operations.

2. Development of information security indicators

For each of the following clauses of the ISO/IEC 27001 standard, please provide two examples of metrics that would be acceptable to measure the conformity to the clause.

- **Nonconformity and corrective action (Clause 10.1.)**

Possible answers:

- Number of corrective actions implemented in the last year.
- % corrective action requests being processed within three months.
- Average delay in days to resolve a non-compliance.

3. Selection of controls

For each risk identified, provide the appropriate controls (by providing the clause number of the control) which allows to reduce, transfer or avoid risks.

Possible answers:

Statements	Vulnerabilities	Threats	C	I	A	Potential Impacts	Controls
The former vice-president of Accounting is hired by a competitor	Lack of an end of contract management process The former VP has knowledge of sensitive data (payroll, financial results, etc.)	Revealing confidential data to a rival company	x			Loss of customers	A.13.2.4 A.7.1.2 A.7.3.1 A.8.1.4 A.9.2.6

4. Classification of controls

For each of the following 5 controls, indicate if it used as a preventive, corrective, and/or detective control; and indicate, if the control is an administrative, technical, managerial or legal measure. Explain your answer.

- **Encryption of electronic communications**

Possible answers:

Preventive control: prevents unauthorized people reading messages
Technical (could be legal) measure: encryption is a technical solution to ensure information confidentiality (could be a legal requirement)

5. Recommendations

The management of the organization would like to receive recommendations from you to improve the processes in place to comply with the requirements of ISO/IEC 27001 on change management.

Possible answers:

1. Document and implement formal change control procedures (documentation, specification, testing, quality control and implementation).
2. This process should provide a risk assessment, impact analysis of the change and a specification of required security controls.
3. Maintain a change log with records of the approvals.
4. Communicating the new process and organize training session.