PECB BEYOND RECOGNITION

Exam Preparation Guide

ISO/IEC 27001 Lead Implementer

GENERAL

The objective of the "PECB Certified ISO/IEC 27001 Lead Implementer" exam is to ensure that the candidate has the necessary competence to support an organization in establishing, implementing, managing, and maintaining an information security management system (ISMS).

The ISO/IEC 27001 Lead Implementer exam is intended for:

- 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 covers the following competency 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
- **Domain 4:** Implementing an ISMS
- **Domain 5:** Performance evaluation, monitoring, and measurement of ISMS
- **Domain 6:** Continual improvement of an ISMS
- **Domain 7:** Preparing for an ISMS certification audit

The content of the exam is divided as follows:

<table>
<tr><th colspan="2">Domain 1: Fundamental principles and concepts of an information security management system (ISMS)

<b>Main objective:</b> Ensure that candidate understands and is able to interpret ISO/IEC 27001 principles and concepts</th></tr>
<tr><th>Competencies</th><th>Knowledge statements</th></tr>
<tr><td>1. Ability to understand and explain the operations of the ISO organizations and the evolution of the information security standards
2. Ability to identify, analyze and evaluate the information security compliance requirements for an organizations
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. Ability to understand, interpret and illustrate the relationship between the concepts of assets, vulnerability, threat, impact and controls</td><td>1. Knowledge of the application 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/IEC 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</td></tr>
</table>

Domain 2: Information security management system (ISMS)

Main objective: Ensure that the candidate understands, is able to interpret, and provide guidance on how to implement and manage an information security management system requirements based on the best practices of ISO/IEC 27001

Competencies

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

Knowledge statements

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 Procedures
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 Control Best Practices
10. Knowledge of Business Continuity Management Control Best Practices
11. Knowledge of Compliance Controls Best Practices

Domain 3: Planning an ISMS implementation

Main objective: Ensure that the candidate is able to plan the implementation of the ISMS based on ISO/IEC 27001

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 organizational	1. Knowledge of the main project management concepts, terminology, processes, and best practices 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 organization 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

Main objective: Ensure that the candidate is able to implement the processes of an ISMS required for an ISO/IEC 27001 certification

Competencies

1. Ability to define and design security controls & processes and document them
2. Ability to implement the required process and security controls of an ISMS
3. Ability to define the document and management process needed to support the implementation and operations of an ISMS
4. Ability to define and writing an 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

Knowledge statements

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

Main objective: Ensure that the candidate is able to evaluate, monitor, and measure the performance of an ISMS

Competencies	Knowledge statements
1. Ability to monitor and evaluate the effectiveness of the 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 observations 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

Main objective: Ensure that the candidate is able to provide guidance on the continual improvement of an ISMS

Competencies	Knowledge statements
1. Ability to understand the principle and concepts related to continual improvement	1. Knowledge of the main concepts related to continual improvement
2. Ability to counsel an organization on how to continually improve the effectiveness and the efficiency of an ISMS	2. Knowledge of the characteristics and the differences between the concept of effectiveness and the efficiency
3. Ability to implement ISMS continual improvement processes in an organization	3. of the concept and techniques to perform a benchmarking
4. Ability to determine the appropriate business improvement tools to support continual improvement processes of a specific organization	4. Knowledge of the main processes, tools and techniques used by professionals to identify the root-causes of nonconformities
5. Ability to identify, analyze the root-causes of potential nonconformities and propose action plans to treat them	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: Ensure that the ISO 27001 Lead Implementer candidate is able to prepare and assist an organization for the certification against ISO/IEC 27001

Competencies

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 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

Knowledge statements

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 activitiess
8. Knowledge of surveillance audits and recertification audit requirements, steps and activitiess
9. Knowledge of the requirements, guidelines and best practices to develop action plans following an ISO/IEC 27001 certification audit

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

				Level of understanding (Cognitive/Taxonomy) required				
		Points per question	Questions that measure comprehension, application, and analysis	Questions that measure synthesis and evaluation	Number of questions per competency domain	% of the exam devoted to each competency domain	Number of points per competency domain	% of points per competency domain
Content Area/Competence Domains	Fundamental principles and concepts of the information security management system (ISMS)	5	X		3	25	20	26.67
		5	X					
		10	X					
	Information security management system controls and best practices	5	X		1	8.33	5	6.67
	Planning the ISMS implementation	5		X	1	8.33	5	6.67
	Implementing the ISMS	10	X		1	8.33	10	13.33
	Performance evaluation, monitoring, and measurement of the ISMS	5		X	3	25	20	26.67
		10		X				
		5		X				
	Continual improvement of the ISMS	5		X	2	16.67	10	13.33
		5		X				
	Preparing for the ISMS certification audit	5		X	1	8.33	5	6.67
	Total points	75						
	Number of questions per level of understanding		5	7				
	% of the exam devoted to each level of understanding (cognitive/taxonomy)		41.67	58.33				

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

After successfully passing the exam, candidates will be able to apply for the “PECB Certified ISO/IEC 27001 Lead Implementer” credential depending on their level of experience.

General Information on the Exam

Candidates are required to arrive/be present at least 30 minutes before the exam starts. Candidates who arrive late will not be given additional time to compensate for the late arrival and may not be allowed to sit for the exam.

Candidates are required to bring a valid identity card (a national ID card, driver's license, or passport) and show it to the invigilator.

If requested on the day of the exam (paper-based exams), additional time can be provided to candidates taking the exam in a non-native language, as follows:

- 10 additional minutes for Foundation exams
- 20 additional minutes for Manager exams
- 30 additional minutes for Lead exams

PECB Exam Format and Type

1. Paper-based: Exams are provided on paper, where candidates are not allowed to use anything but the exam paper and a pen. The use of electronic devices, such as laptops, tablets, or phones, is not allowed. The exam session is supervised by a PECB approved Invigilator at the location where the Reseller has organized the training course.

2. Online: Exams are provided electronically via the PECB Exams application. The use of electronic devices, such as tablets and cell phones, is not allowed. The exam session is supervised remotely by a PECB Invigilator via the PECB Exams application and an external/integrated camera.

For more detailed information about the online format, please refer to the PECB Online Exam Guide.

PECB exams are available in two types:
1. Essay-type question exam
2. Multiple-choice question exam

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

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

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

- A hard copy of ISO 27001 standard
- Training course materials (accessed through PECB Exams app and/or printed)
- Any personal notes taken during the training course (accessed through PECB Exams app and/or printed)
- A hard copy dictionary

Any attempt to copy, collude, or otherwise cheat during the exam session will lead to automatic failure.

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

Note: PECB will progressively transition to multiple-choice exams. They will also be open book and comprise scenario-based questions that will allow PECB to evaluate candidates' knowledge, abilities, and skills to use information in new situations (apply), draw connections among ideas (analyze), and justify a stand or decision (evaluate). All PECB multiple-choice exams have one question and three alternatives, of which only one is correct.

For specific information about exam types, languages available, and other details, visit the List of PECB Exams.

Receiving the Exam Results

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

- The time span for the communication starts from the exam date and lasts three to eight weeks for essay type exams and two to four weeks for multiple-choice paper-based exams

- For online multiple-choice exams, candidates receive their results instantly

Candidates who successfully complete the exam will be able to apply for one of the credentials of the respective certification scheme.

For candidates who fail the exam, a list of the domains where they have performed poorly will be added to the email to help them prepare better for a retake.

Candidates that disagree with the results may request for a re-evaluation by writing to results@pecb.com within 30 working days of receiving the results. Re-evaluation requests received after 30 days will not be processed. If candidates do not agree with the results of the reevaluation, they have 30 working days from the date when they received the reevaluated exam results to file a complaint through the PECB Ticketing System. Complaints received after 30 days will not be processed.

Exam Retake Policy

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

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

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

Reschedule the Exam

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

Closing a Case

If candidates do not apply for certification within three years, their case will be closed. Even though the certification period expires, candidates have the right to reopen their case. However, PECB will no longer be responsible for any changes regarding the conditions, standards, policies, and candidate handbook that were applicable before the case was closed. A candidate requesting their case to reopen must do so in writing and pay the required fee.

Exam Security

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

SAMPLE EXAM QUESTIONS

Question 1: Security controls

For each of the following clauses of an 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 answer:

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

Question 2: Development of information security indicators

For each of the following clauses of an 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 answer:

- 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

Question 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 answer:

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

Question 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 answer:

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)

Question 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 answer:

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

PECB BEYOND RECOGNITION

Address:
Head Quarters
6683 Jean Talon E,
Suite 336 Montreal,
H1S 0A5, QC,
CANADA

Tel./Fax.
T: +1-844-426-7322
F: +1-844-329-7322

PECB Help Center

Visit our Help Center to browse Frequently Asked Questions (FAQ), view manuals for using PECB website and applications, read documents related to PECB processes, or to contact us via Support Center's online tracking system. Visit Help Center here: www.pecb.com/help

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

www.pecb.com