PECB BEYOND RECOGNITION

EXAM PREPARATION GUIDE

PECB Certified ISO/IEC 27001 Lead Auditor

GENERAL

The objective of the “PECB Certified ISO/IEC 27001 Lead Auditor” exam is to ensure that the candidate has the necessary competence to: perform an information security management system (ISMS) audit in compliance with the ISO/IEC 27001 standard requirements; manage an audit team by applying widely recognized audit principles, procedures, and techniques; and, lastly, plan and carry out internal and external audits as per the guidelines of ISO 19011 and in compliance with the ISO/IEC 17021-1 certification processes.

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

- Auditors seeking to perform and lead information security management system (ISMS) audits
- Managers or consultants seeking to master the information security management system audit process
- Individuals responsible to maintain conformity with the ISMS requirements in an organization
- Technical experts seeking to prepare for an information security management system audit
- Expert advisors in information security management

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 (ISMS)
- **Domain 3:** Fundamental audit concepts and principles
- **Domain 4:** Preparing an ISO/IEC 27001 audit
- **Domain 5:** Conducting an ISO/IEC 27001 audit
- **Domain 6:** Closing an ISO/IEC 27001 audit
- **Domain 7:** Managing an ISO/IEC 27001 audit program

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts of an information security management system (ISMS)

Main objective: Ensure that the candidate understands and is able to interpret ISO/IEC 27001 principles and concepts

Competencies	Knowledge statements
1. Ability to understand and explain the main concepts of the information security management system 2. Ability to understand and explain the organization’s operations and the development of information security standards 3. Ability to identify, analyze, and evaluate the information security compliance requirements for an organization 4. Ability to explain and illustrate the main concepts in information security and information security risk management 5. Ability to distinguish and explain the difference between information asset, data and record 6. Ability to understand, interpret, and illustrate the relationship between information security aspects such as controls, vulnerabilities, threats, risks, and assets 7. Ability to identify and illustrate big data, artificial intelligence, machine learning, cloud computing, and outsourcing operations	1. Knowledge of the information security laws, regulations, international and industry standards, contracts, market practices, internal policies, etc., an organization must comply with 2. Knowledge of the main standards related to information security 3. Knowledge the main concepts and terminology of ISO/IEC 27001 4. Knowledge of the concept of risk and its application in information security 5. Knowledge of the relationship between information security aspects 6. Knowledge of the difference and characteristics of security objectives and controls 7. Knowledge of the difference between preventive, detective, and corrective controls 8. Knowledge of the main characteristics of big data, artificial intelligence, machine learning, cloud computng, and outsourcing operations

Domain 2: Information security management system (ISMS)

Main objective: Ensure that the candidate understands, is able to interpret, and identify the requirements for an information security management system based on ISO/IEC 27001

Competencies	Knowledge statements
1. Ability to understand the ISO/IEC 27001 requirements and the structure of the standard 2. Ability to understand the components of an information security management system based on ISO/IEC 27001 and its principal processes 3. Ability to understand, interpret, and analyze the requirements of ISO/IEC 27001 4. Ability to understand whether the organization has satisfied the needs of the interested parties 5. Ability to understand, explain, and illustrate the main steps to establish, implement, operate, monitor, review, maintain, and improve an organization's ISMS 6. Ability to understand the risk assessment approach and methodology 7. Ability to understand the selection of appropriate controls based upon Annex A of ISO/IEC 27001	1. Knowledge of the supporting standards of ISO/IEC 27001 2. Knowledge of the concepts, principles and terminology related to management systems 3. Knowledge of the principal characteristics of an integrated management system 4. Knowledge of the ISO/IEC 27001 requirements presented in the clauses 4 to 10 5. Knowledge of the main steps to establish the ISMS and security policies, security objectives, processes and procedures relevant to managing risks, and improving information security to deliver results in accordance with an organization's overall policies and objectives 6. Knowledge of risk assessment approach and methodology 7. Knowledge of the concept of continual improvement and its application to an ISMS 8. Knowledge of security objectives and controls 9. Knowledge of the Statement of Applicability document

Domain 3: Fundamental audit concepts and principles

Main objective: Ensure that the candidate understands, is able to interpret, and apply the main concepts and principles related to an ISMS audit

Competencies	Knowledge statements
1. Ability to understand, explain, and illustrate the application of the audit principles in an ISMS audit	1. Knowledge of the main audit concepts and principles as described in ISO 19011
2. "Ability to differentiate first, second, and third party audits"	2. Knowledge of the differences between first, second, and third party audits
3. Ability to identify and judge situations that would discredit the professionalism of the auditor and violate the PECB Code of Ethics	3. Knowledge of the principles of auditing: integrity, fair presentation, due professional care, confidentiality, independence, evidence-based approach, and risk-based approach
4. Ability to identify and judge ethical issues considering the obligations related to the audit client, auditee, law enforcement, and regulatory authorities	4. Knowledge of an auditor's professional responsibility and the PECB Code of Ethics
5. Ability to understand the legal implications related to any irregularities committed by the auditee	5. Knowledge of evidence based approach in an audit
6. Ability to understand the impact of trends and technology in auditing	6. Knowledge of the different types of audit evidence: physical, mathematical, confirmative, technical, analytical, documentary, and verbal
7. Ability to explain, illustrate, and apply the audit evidence approach in the context of an ISMS audit	7. Knowledge of the laws and regulations applicable to the auditee and the country it operates in, etc.
8. Ability to explain and compare evidence types and their characteristics	8. Knowledge of the use of big data in audits
9. Ability to determine and justify the type and amount of evidence required in an ISMS audit	9. Knowledge of the auditing of outsourced operations

Domain 4: Preparing an ISO/IEC 27001 audit

Main objective: Ensure that the candidate is able to prepare an information security management system audit

Competencies

1. Ability to determine and evaluate the level of materiality and apply the risk-based approach during the different stages of an ISMS audit
2. Ability to judge the appropriate level of reasonable assurance needed for an ISMS audit
3. Ability to understand and illustrate the steps and activities to prepare an ISMS audit considering the specific context of the audit
4. Ability to understand and explain the roles and responsibilities of the audit team leader, audit team members, and technical experts
5. Ability to determine and evaluate the level of materiality during the different stages of an ISMS audit
6. Ability to determine the audit feasibility
7. Ability to determine, evaluate, and confirm the audit objectives, the audit criteria, and the audit scope for an ISMS audit
8. Ability to explain, illustrate, and define the characteristics of the terms of the audit engagement and apply the best practices to establish the initial contact with an auditee

Knowledge statements

1. Knowledge of the risk-based approach to an audit and the different types of risks related to audit activities such as inherent risk, control risk, and detection risk
2. Knowledge of the concept of materiality and its application to an audit
3. Knowledge of the concept of reasonable assurance and its application to an audit
4. Knowledge of the main responsibilities of the audit team leader and audit team members
5. Knowledge of the roles and responsibilities of technical experts
6. Knowledge of the audit objectives, audit scope, and audit criteria
7. Knowledge of the difference between an ISMS scope and the audit scope
8. Knowledge of the factors to take into account during the audit feasibility
9. Knowledge of the cultural aspects to consider in an audit
10. Knowledge of the characteristics of terms of the audit engagement and the best practices to establish the initial contact with an auditee

Domain 5: Conducting an ISO/IEC 27001 audit

Main objective: Ensure that the candidate can efficiently conduct an ISMS audit

Competencies

1. Ability to conduct the stage 1 audit, taking into account the documented information evaluation criteria
2. Ability to organize and conduct an opening meeting
3. Ability to conduct the stage 2 audit by appropriately following the procedures that this stage entails
4. Ability to apply the best practices of communication to collect the appropriate audit evidence
5. Ability to consider the roles and responsibilities of all the interested parties involved
6. Ability to explain, illustrate, and apply evidence collection procedures and tools
7. Ability to explain, illustrate, and apply the main audit sampling methods
8. Ability to gather appropriate evidence from the available information during an audit and evaluate it objectively
9. Ability to explain, illustrate, and apply the audit evidence approach in an ISMS audit
10. Ability to develop audit working papers and elaborate appropriate audit test plans in an ISMS audit
11. Ability to explain and apply the evidence evaluation process: drafting audit findings
12. Ability to understand, explain, and illustrate the concept of the benefit of the doubt
13. Ability to report appropriate audit observations in accordance with audit rules and principles
14. Ability to conduct quality reviews to audit documentation
15. Ability to complete audit working documents

Knowledge statements

1. Knowledge of the objectives and the content of the opening meeting in 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 documented information evaluation criteria and ISO/IEC 27001 requirements
5. Knowledge of stage 2 audit requirements, steps, and activities
6. Knowledge of the best communication practices during an audit
7. Knowledge of the roles and responsibilities of guides and observers during an audit
8. Knowledge of the different conflict resolution techniques
9. Knowledge of the evidence collection procedures and tools such as interview, documented information review, observation, analysis, sampling and technical verification
10. Knowledge of the evidence analysis techniques: corroboration and evaluation
11. Knowledge of the main concepts, principles, and evidence collection procedures used in an audit
12. Knowledge of the advantages and disadvantages of using audit checklists
13. Knowledge of the main audit sampling methods and their characteristics
14. Knowledge of the audit plan preparation procedure
15. Knowledge of the preparation and development of audit working papers
16. Knowledge of the best practices for the creation of audit test plans
17. Knowledge of the evidence evaluation process: to draft audit findings

	18. Knowledge of the characteristics and differences between the concepts of conformity, minor nonconformity, major nonconformity, anomaly, and observation 19. Knowledge of the guidelines and best practices to draft nonconformity reports 20. Knowledge of the guidelines and best practices to draft and report audit observations 21. Knowledge of the benefit of the doubt principle and its application in the management system audits 22. Knowledge of the guidelines and best practices to complete audit working documents and perform a quality review

Domain 6: Closing an ISO/IEC 27001 audit

Main objective: Ensure that the candidate is able to conclude an ISMS audit

Competencies	Knowledge statements
1. Ability to explain and apply the evidence evaluation process: preparing audit conclusions	1. Knowledge of the evidence evaluation process: to prepare audit conclusions
2. Ability to justify the recommendation for certification	2. Knowledge of the guidelines and best practices to present audit conclusions to the management of an audited organization
3. Ability to draft and present audit conclusions	3. Knowledge of the possible recommendations that an auditor can issue during the certification audit
4. Ability to organize and conduct a closing meeting	4. Knowledge of the closing meeting agenda
5. Ability to write and distribute an ISO/IEC 27001 audit report	5. Knowledge of the guidelines and best practices to evaluate action plans
6. Ability to evaluate action plans	

Domain 7: Managing an ISO/IEC 27001 audit program

Main objective: Ensure that the candidate understands how to establish and manage an ISMS audit program and conduct audit follow-up activities

Competencies	Knowledge statements
1. Ability to conduct the activities following an initial audit, including audit follow-ups and surveillance activities 2. Ability to understand and explain the establishment of an audit program and the application of the PDCA cycle into an audit program 3. Ability to understand and explain the importance of protecting the integrity, availability, and confidentiality of audit records and the auditors' responsibilities in this regard 4. Ability to understand and explain the responsibilities to protect the integrity, availability and confidentiality of audit records 5. Ability to understand the requirements related to the components of the management system of an audit program as quality management, record management, complaint management 6. Ability to understand and explain the way that the combined audits are handled in an audit program 7. Ability to understand the documented information management process 8. Ability to understand the process of evaluating the efficiency of the audit program by monitoring the performance of each auditor and audit team member 9. Ability to demonstrate the application of the personal attributes and behaviors associated with professional auditors	1. Knowledge of audit follow-ups, surveillance audits, and recertification audit requirements, steps, and activities 2. Knowledge of the conditions for the modification, extension, suspension, or withdrawal of an organization's certification 3. Knowledge of the application of the PDCA cycle in the management of an audit program 4. Knowledge of the requirements, guidelines, and best practices regarding audit resources, procedures, and policies 5. Knowledge of the types of tools used by professional auditors 6. Knowledge of the requirements, guidelines, and best practices regarding the management of audit records 7. Knowledge of the application of the continual improvement concept to the management of an audit program 8. Knowledge of the particularities to implement and manage a first, second or third party audit program Knowledge of the competency concept and its application to auditors 9. Knowledge of the management of combined audits 10. Knowledge of the personal attributes and behaviors of a professional auditor

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
Competency domains	Fundamental principles and concepts of an information security management system (ISMS)	5	X		2	16.67	15	20
		10	X					
	Information security management system (ISMS)	5	X		2	16.67	10	13.33
		5	X					
	Fundamental audit concepts and principles	5	X		1	8.33	5	6.67
	Preparing an ISO/IEC 27001 audit	5	X		1	8.33	5	6.67
	Conducting an ISO/IEC 27001 audit	5	X	X	1	8.33	5	6.67
	Closing an ISO/IEC 27001 audit	10		X	3	25	25	3.33
		5		X				
		10		X				
	Managing an ISO/IEC 27001 audit program	5		X	2	16.67	10	13.34
		5		X				
	Total points	75						
	Number of questions per level of understanding		7	5				
	% of the exam devoted to each level of understanding (cognitive/taxonomy)		58.33	41.67				

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 Auditor" credential depending on their level of experience.

TAKING THE EXAM

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/IEC 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.

RECEIVE YOUR 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.

CLOSING A CASE

If a candidate does not apply for the certificate within three years, their case will be closed. Even though the certification period expires, the candidate has 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 case was closed. A candidate requesting their case to reopen must do so in writing and pay the required fees.

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. If candidates or someone who hold PECB credentials reveal information about PECB exam 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

Question 1:

Determine how you would verify each of the following control measures. You must provide examples of evidence you would look for to have a reasonable guarantee that the control measure has been effectively implemented. State at least two elements of proof for each.

- ***Policies for information security (A.5.1.1):***

Possible answers:

- Documentation review of the information security policy to validate the content
- Interview with the person in charge of information security to validate the approval and distribution process of the policy
- Verification of the policy distribution media (Website, hard copy version, information in the employee manual, etc.)

Question 2:

You have received a plan for corrective actions. Evaluate the adequacy of the proposed corrective actions. If you agree with the corrective actions, explain why. If you disagree, explain why and propose what you think would be adequate corrective actions.

- **A non-conformity was observed because the Human Resources team was not aware of the procedure that requires them to validate all future employee references before hiring them**

- **Corrective action: Inform (Timeframe: immediately) and train (Timeframe: within 6 months) the Human Resources team with this procedure and require that each member of the team follow it**

Possible answers:

I agree. This solves the problem that was ignorance of the procedure. As auditor, a sampling will be performed during the surveillance audit to find out if the procedure is followed.

Question 3:

Determine threats and vulnerabilities associated to the following situations and indicate the possible impacts. Also indicate if the risks would affect confidentiality, data integrity and/or availability.
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 webmaster who designed the corporate Website takes care of the updates and the uploading of the site	Absence of segregation of duties. Only one person is available for this function	Treatment errors Malicious act Webmaster leaves the company or becomes sick		X	X	Website containing erroneous information: loss of credibility Unavailable website: loss in revenues	A.12.1.1 A.6.1.2 A.9.2.3 A.14.1.2 A.12.4.3 A.14.2.2

Question 4:

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 law requirement)

Question 5:

Write a test plan to validate the following control identifying the different applicable audit procedures (observation, documentation review, interview, technical verification and analysis):

- **Protection of journalized information (A.12.4.2). Logging facilities and log information shall be protected against tampering and unauthorized access**

Possible answers:

Protection of logged information (A.12.4.2): Logging facilities and log information shall be protected against tampering and unauthorized access.	
Observation	Observation of protection measures implemented against sabotage and unauthorized accesses
Document	Documentation of controls in place to protect information logged against sabotage and unauthorized accesses, information logging policy and related procedures, intrusion test reports
Interview	Interview with the information security manager and validate the logging policy objectives, interview with the network administrator to validate the operation of the controls in place to protect the logged information against sabotage and unauthorized accesses
Technical verification	Observation of logging equipment configurations to verify their compliance to the organization's policies and procedures
Analysis	Analysis of a sample of logged information