PECB

When Recognition Matters

EXAM PREPARATION GUIDE

PECB Certified ISO/IEC 27001 Lead Auditor

The objective of the "Certified ISO/IEC 27001 Lead Auditor" examination is to ensure that the candidate has the knowledge and the skills to plan and perform an Information Security Management System (ISMS) audit compliant with the ISO/IEC 27001:2013 standard. Furthermore, the objective of the examination is to ensure that the candidate has acquired the knowledge to master audit principles and techniques, and to manage (or be part of) audit teams and audit programs in compliance with ISO/IEC 17021-1 certification process and guidelines of ISO 19011.

The target population for this examination is:

- Auditors seeking to perform and lead Information Security Management System (ISMS) certification audits
- Project managers or consultants seeking to master the Information Security Management System audit process
- Individuals responsible for maintaining conformance with Information Security Management System audit process
- Members of an information security team
- Expert advisors in information technology
- Technical experts seeking to prepare for an Information Security Management System audit

The exam content covers the following domains:

- **Domain 1**: Fundamental principles and concepts of Information Security Management System (ISMS)
- **Domain 2**: Information Security Management System (ISMS)
- **Domain 3**: Fundamental audit concepts and principles
- **Domain 4**: Preparation of an ISO 27001 audit
- **Domain 5**: Conducting an ISO 27001 audit
- **Domain 6**: Closing an ISO 27001 audit
- **Domain 7**: Managing an ISO 27001 audit program

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts of Information Security Management System (ISMS)

Main objective: To ensure that the ISO 27001 Lead Auditor 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 development 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 (ISMS)

Main objective: To ensure that the ISO 27001 Lead Auditor candidate can understand, interpret and illustrate the main concepts and components of an Information Security Management System based on ISO 27001

Competencies	Knowledge statements
1. Understand and explain the components of an Information Security Management System based on ISO 27001 and its principal processes 2. Ability to interpret and analyze ISO 27001 requirements 3. Understand, explain and illustrate the main steps to establish, implement, operate, monitor, review, maintain and improve an organization's ISMS 4. Ability to formulate security objectives and select the appropriate controls based upon Annex A of ISO 27001	1. Knowledge of the concepts, principles and terminology related to management systems and the "Plan-Do-Check-Act" (PDCA) model 2. Knowledge of the principal characteristics of an integrated management system 3. Knowledge of the main advantages of a certification for an organization 4. Knowledge of the ISO 27001 requirements presented in the clauses 4 to 8 5. Knowledge of the main steps to establish the ISMS and security policies, security objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives (Awareness level) 6. Knowledge of the concept of continual improvement and its application to an ISMS 7. Knowledge of security objectives and controls

Domain 3: Fundamental Audit Concepts and Principles

Main objective: To ensure that the ISO 27001 Lead Auditor candidate can understand, interpret and apply the main concepts and principles related to an ISMS audit in the context of ISO 27001

Competencies	Knowledge statements
1. Understand, explain and illustrate the application of the audit principles in the context of an ISO 27001 audit 2. Ability to identify and judge situations that would discredit the professionalism of the auditor and the PECB code of ethics 3. Ability to identify and evaluate ethical problems taking into account the obligations related to sponsors, audittee and law enforcement or regulatory authorities 4. Ability to explain, illustrate and apply the audit evidence approach in the context of an ISO 27001 audit 5. Ability to explain and compare the types and characteristics of evidence 6. Ability to determine and justify what type of evidence and how much evidence will be required in the context of a specific ISMS audit mission 7. Ability to determine and evaluate the level of materiality and apply the risk based approach during the different phases of an ISO 27001 audit 8. Ability to judge the appropriate level of reasonable assurance needed for a specific ISO 27001 audit mission	1. Knowledge of the main audit concepts and terminology as described in ISO 19011 2. Knowledge of the differences between the types of audits such as first party, second party and third party audit 3. Knowledge of the following audit principles: integrity, fair presentation, due professional care, confidentiality independence and evidence-based approach. 4. Knowledge of professional responsibility of an auditor and the PECB code of ethics 5. Knowledge of evidence based approach in an audit 6. Knowledge of the different types of evidences: physical, mathematical, confirmative, technical, analytical, documentary and verbal 7. Knowledge of the quality of audit evidences (appropriate, reliable, reliable and sufficient) and the factors that will influence them. 8. Knowledge of the risk based approach in an audit and the different types of risk related to audit activities such as: Inherent risk, control risk and detection risk 9. Knowledge of the concept of materiality and its application in an audit 10. Knowledge of the concept of reasonable assurance and its applicable in an audit

Domain 4: Preparation of an ISO/IEC 27001 audit

Main objective: To ensure that the ISO/IEC 27001 Lead Auditor candidate can prepare appropriately an ISMS audit in the context of ISO/IEC 27001

Competencies	Knowledge statements
1. Understand and explain the steps and activities to prepare an ISMS audit, taking in consideration the specific context and conditions of the mission 2. Understand and explain the roles and responsibilities of the audit team leader, audit team members and technical experts 3. Ability to determine, evaluate and confirm the audit objectives, the audit criteria and the audit scope for a specific ISO 27001 audit mission 4. Ability to do a feasibility study of an audit in the context of a specific ISO 27001 audit mission 5. Ability to explain, illustrate and define the characteristics of the audit terms of engagement and apply the best practices to establish a first contact with an audittee in the context of a specific ISO 27001 audit mission 6. Ability to develop audit working papers and to elaborate appropriate audit test plans in the context of a specific ISO 27001 audit mission	1. Knowledge of the main responsibilities of the audit team leader and audit team members 2. Knowledge of the roles and responsibilities of technical experts used for an audit 3. Knowledge of the definition of audit objectives, audit scope and audit criteria 4. Knowledge of the difference between the ISMS scope and the audit scope 5. Knowledge of the elements to review during the feasibility study of an audit 6. Knowledge of the cultural aspects to consider in an audit 7. Knowledge of the characteristics of audit terms of engagement and the best practices to establish a first contact with an audittee 8. Knowledge of the preparation of an audit plan 9. Knowledge of the preparation and development of audit working paper 10. Knowledge of advantages and disadvantages of using audit checklists 11. Knowledge of the best practices to creation audit test plans

Domain 5: Conducting an ISO/IEC 27001 audit

Main objective: To ensure that the ISO/IEC 27001 Lead Auditor candidate can conduct efficiently an ISMS audit in the context of ISO/IEC 27001

Competencies	Knowledge statements
1. Ability to organize and conduct the opening meeting in the context of a specific ISO 27001 audit mission 2. Ability to conduct a stage 1 audit in the context of a specific ISO 27001 audit mission and taking into account the documentation review conditions and criteria 3. Ability to prepare the audit plan for stage 2 audit, containing all the necessary documents and the assignment of the auditors and technical experts for the stage. 4. Ability to conduct a stage 2 audit in the context of a specific ISO 27001 audit mission by applying the best practices of communication to collect the appropriate evidence and taking into account the roles and responsibilities of all people involved 5. Ability to conduct audit tests, appropriate procedures, as well as the non-conformity reports 6. Ability to explain, illustrate and apply statistical techniques and main audit sampling methods 7. Ability to gather appropriate evidences objectively from the available information in an audit and to evaluate them objectively	1. Knowledge of the objectives and the content of the opening meeting of an audit 2. Knowledge of the difference of the stage 1 audit and the stage 2 audit 3. Knowledge of stage 1 audit requirements, steps and activities 4. Knowledge of the documentation review criteria 5. Knowledge of the documentation requirements stated in ISO 27001 6. Knowledge of stage 2 audit requirements, steps and activities 7. Knowledge of best practices of communication during an audit 8. Knowledge of the roles and responsibilities of guides and observers during an audit 9. Knowledge of the conflict resolution techniques 10. Knowledge of evidence collection procedures: observation, documentation review, interviews, analysis and technical verification 11. Knowledge of evidence analysis procedures: corroboration and evaluation 12. Knowledge of main concepts, principles and statistical techniques used in an audit 13. Knowledge of the main audit sampling methods and their characteristics

Domain 6: Closing an ISO/IEC 27001 audit

Main objective: To ensure that the ISO/IEC 27001 Lead Auditor candidate can conclude an ISMS audit and conduct follow-up activities in the context of ISO/IEC 27001

Competencies	Knowledge statements
1. Ability to explain and apply the evaluation process of evidences to draft audit findings and prepare audit conclusions 2. Understand, explain and illustrate the different levels of conformity and the concept of benefits of doubt 3. Ability to report appropriate audit observations in order to help an organization to improve an ISMS in respect of audit rules and principles 4. Ability to complete audit working documents and do a quality review of an ISO 27001 audit 5. Ability to draft audit conclusions and present these to the management of the audited organization 6. Ability to organize and conduct an audit closing meeting 7. Ability to write an ISO 27001 audit report and justify a certification recommendation 8. Ability to conduct the activities following an initial audit including the evaluation of action plans, follow up audits, surveillance audits and recertification audits 9. Ability to make the certification decision based on the results and conclusions of the audit	1. Knowledge of the evaluation process of evidences to draft audit findings and prepare audit conclusions 2. Knowledge of the differences and the characteristics between the concepts of conformity, minor nonconformity, major nonconformity, anomaly and observation 3. Knowledge of the guidelines and best practices to write nonconformity report 4. Knowledge of the guidelines and best practices to draft and report audit observation 5. Knowledge of the principle of benefits of doubt and his application in the context of an audit 6. Knowledge of the guidelines and best practices to complete audit working documents and do a quality review of an audit 7. Knowledge of the guidelines and best practices to present audit findings and conclusions to management of an audited organization 8. Knowledge of the possible recommendations that an auditor can issue in the context of a certification audit and the certification decision process 9. Knowledge of the guidelines and best practices to evaluate action plans 10. Knowledge of follow-up audit, surveillance audits and recertification audit requirements, steps and activities 11. Knowledge of the conditions for modification, extension, suspension or withdrawal of a certification for an organization

Domain 7: Managing an ISO/IEC 27001 audit program

Main objective: To ensure that the ISO/IEC 27001 Lead Auditor understands how to establish and manage an ISMS audit program

Competencies	Knowledge statements
1. Understand and explain the establishment of an audit program and the application of the PDCA model 2. Understand and explain the implementation of an ISO 27001 audit program (first party, second party and third party) 3. Understand and explain the responsibilities to protect the integrity, availability and confidentiality of audit records 4. Understand the requirements related to the components of the management system of an audit program as quality management, record management, complaint management 5. Understand the evaluation of the efficiency of the audit program by monitoring the performance of each auditor, each team and the entire certification body 6. Understand and explain the way combined audits are handled in an audit program 7. Ability to demonstrate the application of the personal attributes and behaviors associated to professional auditors	1. Knowledge of the application of the PDCA model in the management of an audit program 2. Knowledge of requirements, guidelines and best practices regarding audit resources, procedures and policies 3. Knowledge of the types of tools used by professional auditors 4. Knowledge of requirements, guidelines and best practices regarding the management of audit records 5. Knowledge of the application of the concept of continual improvement to the management of an audit program 6. Knowledge of the particularities to implement and manage a first, second or third party audit program 7. Knowledge of the management of combined audit activities 8. Knowledge of the concept of competency and its application to auditors 9. Knowledge of the personal attributes and behavior of a professional auditor

Based on these 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		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
	Preparation of an ISO/IEC 27001 audit	5	X		1	8.33	5	6.67
	Conducting an ISO/IEC 27001 audit	5	X		1	8.33	5	6.67
	Closing an ISO/IEC 27001 audit	10		X	3	25	25	33.33
		5		X				
		10		X				
	Managing an ISO/IEC 27001 audit program	5		X	2	16.67	10	13.33
		5		X				
Total Points		75						
Number of Questions per level of understanding			7	5				
% of Test Devoted to each level of understanding (cognitive/taxonomy)			58.33	41.67				

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

After successfully passing the exam, candidates will be able to apply for the credentials of Certified ISO 27001 Lead Auditor, 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 allowed 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. Evidence in an audit

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.)

2. Evaluation of corrective actions

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.

3. Risk evaluation and selection of controls

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
1. 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

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 law requirement)

5. Writing of a test plan

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.