PECB BEYOND RECOGNITION

Exam Preparation Guide

ISO/IEC 27001 Internal Auditor

General

The objective of the "PECB Certified **ISO/IEC 27001 Internal Auditor**" exam is to ensure that the candidate has the necessary expertise to plan and perform the information security management system (ISMS) audit compliant with the ISO/IEC 27001 standard. Furthermore, the objective of the exam 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 ISO/IEC 27001 Internal Auditor exam is intended for:

- Internal Auditors seeking to perform and lead information security management System (ISMS) internal audits
- Individuals responsible for maintain conformance with an Information Security Management system
- Members of an information security team
- Information security managers
- Information security consultants
- Members of an ISMS implementation team
- IT professionals
- Individuals responsible for undertaking internal audits of an ISMS

The exam covers the following competency domains:

- **Domain 1:** Fundamental principles and concepts of an information security management system (ISMS)
- **Domain 2:** Fundamental audit concepts and principles
- **Domain 3:** Preparing and conducting an ISO/IEC 27001 internal audit
- **Domain 4:** Managing an ISO/IEC 27001 internal audit program
- **Domain 5:** Preparing 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: 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 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. Ability to understand, interpret and illustrate the relationship between the concepts of asset, vulnerability, threat, impact and controls 6. Ability to understand and explain the components of an information security management system based on ISO/IEC 27001 and its principal processes 7. Ability to interpret and analyze ISO/IEC 27001 requirements 8. Ability to understand, explain and illustrate the main steps to establish, implement, operate, monitor, review, maintain and improve an organization's ISMS 9. Ability to formulate security objectives and select the appropriate controls based upon Annex A of ISO/IEC 27001	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 9. Knowledge of the principal characteristics of an integrated management system 10. Knowledge of the main advantages of a certification for an organization 11. Knowledge of the ISO/IEC 27001 requirements presented in the clauses 4 to 8 12. 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) 13. Knowledge of the concept of continual improvement and its application to an ISMS 14. Knowledge of security objectives and controls

Domain 2: 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 the context of an ISO/IEC 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, auditee and law enforcement or regulatory authorities 4. Ability to explain, illustrate and apply the audit evidence approach in the context of an ISO/IEC 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/IEC 27001 audit 8. Ability to judge the appropriate level of reasonable assurance needed for a specific ISO/IEC 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

PECB

Domain 3: Preparing and conducting the ISO/IEC 27001 audit

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

Competencies	Knowledge statements
1. Ability to understand and explain the steps and activities to prepare an ISMS audit, taking in consideration the specific context and conditions of the mission 2. Ability to 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/IEC 27001 audit mission 4. Ability to do a feasibility study of an audit in the context of a specific ISO/IEC 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 auditee in the context of a specific ISO/IEC 27001 audit mission 6. Ability to develop audit working papers and to elaborate appropriate audit test plans in the context of a specific ISO/IEC 27001 audit mission 7. Ability to organize and conduct the opening meeting in the context of a specific ISO/IEC 27001 audit mission 8. Ability to conduct a stage 1 audit in the context of a specific ISO/IEC 27001 audit mission and taking into account the documentation review conditions and criteria 9. 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.	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 auditee 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 12. Knowledge of the objectives and the content of the opening meeting of an audit 13. Knowledge of the difference of the stage 1 audit and the stage 2 audit 14. Knowledge of stage 1 audit requirements, steps and activities 15. Knowledge of the documentation review criteria 16. Knowledge of the documentation requirements stated in ISO/IEC 27001 17. Knowledge of stage 2 audit requirements, steps and activities 18. Knowledge of best practices of communication during an audit 19. Knowledge of the roles and responsibilities of guides and observers during an audit 20. Knowledge of the conflict resolution techniques

10. Ability to conduct a stage 2 audit in the context of a specific ISO/IEC 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 11. Ability to conduct audit tests, appropriate procedures, as well as the non-conformity reports 12. Ability to explain, illustrate and apply statistical techniques and main audit sampling methods 13. Ability to gather appropriate evidences objectively from the available information in an audit and to evaluate them objectively	21. Knowledge of evidence collection procedures: observation, documentation review, interviews, analysis and technical verification 22. Knowledge of evidence analysis procedures: corroboration and evaluation 23. Knowledge of main concepts, principles and statistical techniques used in an audit 24. Knowledge of the main audit sampling methods and their characteristics

PECB

Domain 4: Managing an ISO/IEC 27001 internal audit programme

Main objective: Ensure that the candidate understands how to establish and manage an ISMS internal audit program

Competencies	Knowledge statements
1. Ability to understand and explain the establishment of an audit program and the application of the PDCA model 2. Ability to understand and explain the implementation of an ISO/IEC 27001 audit program (first party, second party and third party) 3. Ability to understand and explain the responsibilities to protect the integrity, availability and confidentiality of audit records 4. Ability to understand the requirements related to the components of the management system of an audit program as quality management, record management, complaint management 5. Ability to 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. Ability to 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

Domain 5: Preparing for an ISMS certification audit

Main objective: Ensure that the candidate can prepare and assist an organization for the certification 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 the above-mentioned domains and their relevance, 7 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
Competence Domains	Fundamental principles and concepts of an Information security management system (ISMS)	5	X		2	28.57	10	20
		5	X					
	Fundamental audit concepts and principles	5	X		2	28.57	15	30
		10		X				
	Preparing and conducting an ISO/IEC 27001 internal audit	5		X	1	14.29	5	10
	Managing an ISO/IEC 27001 internal audit programme	10		X	1	14.29	10	20
	Preparing for an ISMS certification audit	10	X		1	14.29	10	20
	Total points	50						
	Number of questions per level of understanding		4	3				
	% of Test Devoted to each level of understanding (cognitive/taxonomy)		57.14	42.86				

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

After successfully passing the exam, candidates will be able to apply for the "PECB Certified ISO/IEC 27001 Internal Auditor" 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 the 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 attempts to copy, collude, or otherwise cheat during the exam session will automatically lead to failure of the exam.

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: 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 answer:

- ***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: 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 answer:
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: 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 answer:

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

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 law requirement)

Question 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 answer:

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

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.

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

www.pecb.com