PECB BEYOND RECOGNITION

Exam Preparation Guide

ISO/IEC 27701 Lead Auditor

GENERAL

The objective of the "PECB Certified ISO/IEC 27701 Lead Auditor" exam is to ensure that the candidate has acquired the necessary expertise to: perform the privacy information management system (PIMS) audit in compliance with the ISO/IEC 27701 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 in compliance with the ISO 19011 and ISO/IEC 17021-1 certification proceses.

The ISO/IEC 27701 Lead Auditor exam is intended for:

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

The exam covers the following competency domains:

- **Domain 1:** Fundamental principles and concepts of the privacy information management system (PIMS)
- **Domain 2:** Privacy information management system (PIMS)
- **Domain 3:** Fundamental audit concepts and principles
- **Domain 4:** Preparing the ISO/IEC 27701 audit
- **Domain 5:** Conducting the ISO/IEC 27701 audit
- **Domain 6:** Closing the ISO/IEC 27701 audit
- **Domain 7:** Managing the ISO/IEC 27701 audit program

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts of the privacy information management system (PIMS)

Main objective: Ensure that the ISO/IEC 27701 Lead Auditor candidate understands, is able to interpret, and illustrate the ISO/IEC 27701 principles and concepts

Competencies	Knowledge statements
1. Ability to understand and explain the ISO operations and the development of ISO/IEC 27701 standard 2. Ability to identify, analyze, and evaluate the ISO/IEC 27701 requirements 3. Ability to explain and illustrate the main concepts of privacy information management system 4. Ability to identify information security and privacy-related standards 5. Ability to outline the relationship between PIMS and ISMS 6. Ability to list applicable privacy-related controls for PII controllers and PII processors 7. Ability to map the ISO/IEC 27701 requirements to GDPR 8. Ability to understand the privacy principles	1. Knowledge of the main standards related to information security and privacy 2. Knowledge of the main concepts and terminology described in ISO/IEC 27701 3. Knowledge of the laws, regulations, international and industry standards, contracts, market practices, internal policies, etc. an organization must comply with 4. Knowledge of the main differences between PIMS and ISMS 5. Knowledge of the mapping between the ISO/IEC 27701 requirements and GDPR 6. Knowledge of other information security and privacy-related standards 7. Knowledge of the application of the privacy principles to comply with ISO/IEC 27701 requirements

Domain 2: Privacy information management system (PIMS)

Main objective: Ensure that the ISO/IEC 27701 Lead Auditor candidate understands, is able to interpret, and illustrate the main concepts and principles of the privacy information management system

Competencies	Knowledge statements
1. Ability to identify, understand, classify, and explain the requirements of ISO/IEC 27701 2. Ability to distinguish and illustrate the information security and privacy requirements and best practices by using concrete examples 3. Ability to understand, explain, and illustrate the main steps to establish, implement, monitor, review, maintain, and improve an organization's PIMS 4. Ability to analyze, evaluate, and validate action plans to implement a specific control or process	1. Knowledge of the ISO/IEC 27701 requirements 2. Knowledge of the best practices in information security and privacy management 3. Knowledge of the establishment, implementation, and maintenance of information security and privacy management procedures 4. Knowledge of the implementation and management of action plans to support the PIMS

Domain 3: Fundamental audit concepts and principles

Main objective: Ensure that the ISO/IEC Lead Auditor candidate understands, is able to interpret, and apply the main concepts and principles related to the PIMS audit

Competencies	Knowledge statements
1. Ability to understand, explain, and apply the principles of auditing based on ISO 19011 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 exceptions to the confidentiality principle required by law and authorized interested parties 4. Ability to explain, illustrate, and apply the evidence-based and risk-based auditing approach in the context of an ISO/IEC 27701 audit 5. Ability to explain and compare the types and characteristics of audit evidence 6. Ability to determine and evaluate the level of materiality and apply the risk-based approach during the different phases of an ISO/IEC 27701 audit 7. Ability to judge the appropriate level of reasonable assurance in the context of an ISO/IEC 27701 audit	1. Knowledge of the main audit concepts and terminology based on ISO 19011 2. Knowledge of types of audits such as first party audit (internal audit), second party audit, and third party audit 3. Knowledge of audit objectives and audit criteria 4. Knowledge of principles of auditing such as integrity, fair presentation, due professional care, confidentiality, independence, evidence-based approach, and risk-based approach 5. Knowledge of professional responsibilities of an auditor and the PECB code of ethics 6. Knowledge of the types of audit evidece such as physical, mathematical, confirmative, technical, analytical, documentary, and verbal 7. Knowledge of the quality and reliability of audit evidence 8. Knowledge of the audit approach based on risk 9. Knowledge of the concepts of materiality and reasonable assurance and their applicability in an audit

Domain 4: Preparing the ISO/IEC 27701 audit

Main objective: Ensure that the ISO/IEC 27701 Lead Auditor candidate is able to prepare the privacy information management system audit

Competencies	Knowledge statements
1. Ability to understand and explain the steps and activities needed to prepare a PIMS audit 2. Ability to understand and explain the roles and responsibilities of the audit team leader and audit team members 3. Ability to explain, illustrate, and define the audit engagement procedures 4. Ability to determine the audit feasibility 5. Ability to determine, evaluate, and confirm the audit objectives, the audit criteria, and the audit scope in the context of ISO/IEC 27701 6. Ability to define the audit schedule	1. Knowledge of the main responsibilities of the audit team leader and the audit team members 2. Knowledge of the audit engagement procedures and the steps in accepting an audit engagement 3. Knowledge of the elements to review during the audit feasability study 4. Knowledge of the audit objectives, the audit criteria, and the audit scope 5. Knowledge of the difference between the PIMS scope and the audit scope 6. Knowledge of the audit schedule

Domain 5: Conducting the ISO/IEC 27701 audit

Main objective: Ensure that the ISO/IEC 27701 Lead Auditor candidate can efficiently conduct the PIMS audit

Competencies	Knowledge statements
1. Ability to conduct a stage 1 audit 2. Ability to prepare and conduct on-site activities 3. Ability to plan the stage 2 audit and assign work to the audit team 4. Ability to prepare audit test plans and the documented information for stage 2 audit 5. Ability to conduct a stage 2 audit 6. Ability to organize and conduct an opening meeting 7. Ability to conduct audit tests 8. Ability to explain, illustrate, and apply evidence collection procedures 9. Ability to explain, illustrate, and apply evidence analysis procedures	1. Knowledge of the objectives and steps of the stage 1 audit 2. Knowledge of the points to validate during the stage 1 audit 3. Knowledge of types of documented information to be audited 4. Knowledge of the verification of internal audit documents 5. Knowledge of audit planning steps and how to prepare audit test plans 6. Knowledge of the principles of maintaining audit working documents 7. Knowledge of the objectives and the content of the opening meeting of an audit 8. Knowledge of the audit tests 9. Knowledge of the responsibility of guides and observers 10. Knowledge of evidence collection procedures: observation, documented information review, interview, analysis, and technical verification 11. Knowledge of evidence analysis procedures: corroboration and evaluation

Domain 6: Closing the ISO/IEC 27701 audit

Main objective: Ensure that the ISO/IEC 27701 Lead Auditor candidate is able to conclude the PIMS audit and conduct audit follow-up activities

Competencies	Knowledge statements
1. Ability to determine audit finding, draft nonconformities, and conduct quality review 2. Ability to draft a nonconformity report 3. Ability to determine, agree, and draft the audit conclusions 4. Ability to conduct the closing meeting 5. Ability to prepare and distribute the audit report 6. Ability to make the certification decision and give recommendations for improvement 7. Ability to evaluate action plans by the auditor 8. Ability to conduct audit follow-up activities and conduct surveillance activities 9. Ability to plan and conduct recertification audit	1. Knowledge of audit findings, nonconformities, observations, and anomalies 2. Knowledge of the differences between major nonconformity, minor nonconformity, observation, and anomaly 3. Knowledge of documenting the audit findings and drafting a nonconformity report 4. Knowledge of the best practices to draft nonconformity report 5. Knowledge of the evaluation process of evidences to determine, agree, and draft the audit conclusions 6. Knowledge of the guidelines and best practices to present audit findings and audit conclusion to the auditee 7. Knowledge of the organization and content of the closing meeting 8. Knowledge of content and distribution of the audit report 9. Knowledge of content and evaluation of action plans 10. Knowledge of audit follow-up activities and surveillance activities 11. Knowledge of the certification cycle and conditions for extension, suspension or withdrawal, and trasfer of the certification

Domain 7: Managing the ISO/IEC 27701 audit program

Main objective: Ensure that the ISO/IEC 27701 Lead Auditor candidate understands how to establish and manage the PIMS audit program

Competencies	Knowledge statements
1. Ability to understand and explain the audit program and the use of the PDCA model 2. Ability to understand and explain the implementation of the ISO/IEC 27701 audit program 3. Ability to understand and explain the responsibilities to protect the integrity, availability, and confidentiality of the audit records 4. Ability to achieve independence, objectivity, and impartiality of the audit function 5. Ability to evaluate the efficiency of the audit program by monitoring, reviewing, and improving the audit program	1. Knowledge of the use of the PDCA model in the management of an audit program 2. Knowledge of the audit program resources and records 3. Knowledge of the differences between the internal and external audits 4. Knowledge of the structure of the audit charter 5. Knowledge of the main internal audit services and activities 6. Knowledge of the continual internal audit program 7. Knowledge of the monitoring, evaluating, reviewing, and improving an audit program

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 the privacy information management system (PIMS)	5	X		2	16.67	10	13.33
		5	X					
	Privacy information management system (PIMS)	5	X		1	8.33	5	6.67
	Fundamental audit concepts and principles	5	X		1	8.33	5	6.67
	Preparing the ISO/IEC 27701 audit	5	X		2	16.67	15	20
		10		X				
	Conducting the ISO/IEC 27701 audit	5	X		3	25	15	20
		5		X				
		5	X					
	Closing the ISO/IEC 27701 audit	10		X	2	16.67	20	26.66
		10		X				
	Managing the ISO/IEC 27701 audit program	5	X		1	8.33	5	6.67
	Total points	75	8	4				
	Number of questions per level of understanding							
	% of the exam devoted to each level of understanding (cognitive/taxonomy)		66.7	33.3				

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

After successfully passing the exam, candidates will be able to apply for the "PECB Certified ISO/IEC 27701 Lead Auditor" credential, depending on their level of experience.

TAKE THE EXAM

Candidates will be required to arrive at least 30 minutes before the exam starts. Candidates arriving late will not be given additional time to compensate for the late arrival and may even be denied entry to the exam.

All candidates are required to present a valid identity card such as a national ID card, driver's license, or passport to the invigilator.

The duration of the exam is three hours. Non-native speakers will receive an additional 30 minutes.

The exam contains essay type questions: This type of format was selected as a means of determining whether a candidate can clearly answer training course related questions, by assessing problem-solving techniques and formulating arguments that are supported with reasoning and evidence. The exam is set to be "open book" and does not measure the recall of data or information. The exam evaluates candidates' comprehension, application, and analytical skills. Therefore, candidates will have to justify their answers by providing concrete explanations to demonstrate that they have been capable of understanding the training course concepts. At the end of this document, you will find samples of exam questions and possible answers.

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

- A copy of the **ISO/IEC 27701** standard
- Course notes from the Participant Handout
- Any personal notes made by the candidate during the training course
- A hard copy dictionary

The use of electronic devices, such as smartphones, are not allowed.

All attempts to copy, collude, or otherwise cheat during the exam will automatically lead to the failure of the exam.

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 via email within a period of six to eight weeks from the exam date. The candidate will be provided with only two possible exam results: pass or fail, rather than an exact grade.

Candidates who successfully complete the exam will be able to apply for a certified scheme.

In case of exam failure, the results will be accompanied with the list of domains in which the candidate has failed to fully answer the question(s). This can help the candidate better prepare for a retake exam.

Candidates who disagree with the exam results may file a complaint by writing to examination@pecb.com. 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 the allowed time frame in between exam retakes, such as:

- If a candidate does not pass the exam on the first attempt, the candidate must wait 15 days (from the initial date of the exam) for the next attempt (first retake). The retake fee applies.

  Note: *Candidates who have completed the full training course 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, the candidate must wait three months (from the initial date of the exam) for the next attempt (second retake). The retake fee applies.
- If a candidate does not pass the exam on the third attempt, the candidate must wait six months (from the initial date of the exam) for the next attempt (third retake). The retake fee applies.
- After the fourth attempt, a waiting period of 12 months from the last session date is required, in order for the candidate to retake the same exam. The regular fee applies.

For the candidates that fail the exam in the second retake, PECB recommends to attend an official training course 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 training course 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 AND POSSIBLE ANSWERS

Question 1: For each of the following clauses of ISO/IEC 27701, provide at least two types of evidence that would be sufficient to verify the conformity. In addition, indicate the type of evidence used.

1. *Clause 7.3.9 Handling requests*
2. *Clause 7.4.5 PII de-identification and deletion at the end of processing*

Example: *Clause 6.9.4.1 Event logging*

- *Event log records of access to PII (physical evidence)*
- *Interview with the person in charge of monitoring the process of event logging (verbal evidence)*

Possible answer:

1. ***Clause 7.3.9 Handling requests***
   - *Verification of a sample of handled requests to determine if they have been handled within the defined response time (analytical evidence)*
   - *Verification of the policies and procedures for handling and responding to legitimate requests from PII principals (documentary evidence)*

2. ***Clause 7.4.5 PII de-identification and deletion at the end of processing***
   - *Observaction of mechanisms used to erase the PII (technical evidence)*
   - *Interview with the person in charge of implementing de-identification techniques (verbal evidence)*

Question 2: Prepare an audit test plan by selecting at least three appropriate audit procedures to validate conformity to clause 8.5.4 Notification of PII disclosure requests of ISO/IEC 27701. Mark "N/A" for the procedures that do not apply.

AUDIT TEST PLAN	
Audit criteria: *The organization should notify the customer of any legally binding requests for disclosure of PII.*	
Observation	*The audit team should observe how the organization notifies its customers in case of any legally binding requests for disclosure of PII*
Documented information review	*The audit team should review the documented information related to the notification of customer if case of any legally binding requests for disclosure of PII*
Interview	*The audit team should interview personnel responsible for the implementation of procedures on how to notify the customer for disclosure of PII*
Technical verification	*N/A*
Analysis	*The audit team should select a sample of notifications sent to customers to ensure that they have been notified for any legally binding requests for disclosure of PII within agreed timeframes*

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