PECB BEYOND RECOGNITION

2019

Exam Preparation Guide

ISO/IEC 27701 LEAD IMPLEMENTER

The objective of the "PECB Certified ISO/IEC 27701 Lead Implementer" exam is to ensure that the candidate has acquired the necessary expertise to support an organization in establishing, implementing, maintaining, and continually improving the privacy information management system (PIMS).

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

- PII controllers and PII processors
- Managers or consultants involved in and concered with the implementation of a privacy information management system in an organization
- Project managers, consultants, or expert advisers seeking to master the implementation of the privacy information management system
- Individuals responsible for maintaining conformity with the information security and privacy requirements in an organization
- Members of the PIMS or ISMS implementation team

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:** Planning the PIMS implementation
- **Domain 4:** Implementing the PIMS
- **Domain 5:** Performance evaluation, monitoring, and measurement of the PIMS
- **Domain 6:** Continual improvement of the PIMS
- **Domain 7:** Preparing for the PIMS certification audit

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 Implementer candidate understands, is able to interpret, and illustrate the main ISO/IEC 27701 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 9. Ability to identify and interpret PIMS risks and their impacts 10. Ability to understand and set information security and privacy objectives	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 the concept of risk and its application in the privacy information management system 7. Knowledge of other information security and privacy-related standards 8. Knowledge of the information security and privacy hazards, threats, potential incidents and their impact 9. Knowledge of the application of the information security and privacy objectives and how to achieve specific results

Domain 2: Privacy information management system (PIMS)

Main objective: Ensure that the ISO/IEC 27701 Lead Implementer candidate understands, is able to interpret, and provide guidance on how to implement and manage the privacy information management system requirements and controls based on the best practices of ISO/IEC 27701

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 find different solutions to the information security and privacy management issues, identify and analyze the strengths and weaknesses of each proposed solution 4. Ability to work toward the best information security and privacy management solutions in order to address the management objectives set by the organization 5. Ability to analyze, evaluate, and validate action plans to implement a specific control or process	1. Knowledge of the ISO/IEC 27701 requirements and controls 2. Knowledge of the best practices in information security and privacy management 3. Knowledge of the best information security and privacy management strategies and techniques used to identify and analyze solutions to information security and privacy management issues 4. Knowledge of the establishment, implementation, and maintenance of information security and privacy management procedures 5. Knowledge of the implementation and management of action plans to support the PIMS

Domain 3: Planning the PIMS implementation

Main objective: Ensure that the ISO/IEC Lead Implementer candidate is able to plan the implementation of the PIMS required for an ISO/IEC 27701 certification

Competencies	Knowledge statements
1. Ability to manage the implementation of the PIMS by following the best practices 2. Ability to collect, analyze, and interpret the information required to plan the PIMS implementation 3. Ability to analyze and consider the role of a PII controller and PII processor in an organization 4. Ability to identify the resources required for the PIMS implementation 5. Ability to draft, and review the PIMS project plan 6. Ability to define and justify the PIMS scope adapted to the organization's specific information security and privacy objectives 7. Ability to develop and establish the PIMS policy 8. Ability to perform the different steps of the privacy risk assessment and the privacy impact assessment processes	1. Knowledge of the main project management concepts, terminology, processes, and best practices 2. Knowledge of the principal approaches and methodology used to implement the PIMS 3. Knowledge of an organization's role as a PII controller, PII processor, or both 4. Knowledge of the resources required for the PIMS implementation 5. Knowledge of the PIMS project plan and the PIMS project team 6. Knowledge of the characteristics of the PIMS scope in terms of organizational, technological, and physical boundaries 7. Knowledge of the best practices and techniques used to draft and establish information security and privacy policies and procedures 8. Knowledge of the different approaches and methodologies used to perform the privacy risk assessment and the privacy impact assessment processes

Domain 4: Implementing the PIMS

Main objective: Ensure that the ISO/IEC 27701 Lead Implementer candidate is able to implement the processes of the PIMS required for an ISO/IEC 27701 certification

Competencies	Knowledge statements
1. Ability to manage, estimate, and monitor the required resources for the PIMS implementation 2. Ability to identify, analyze, and evaluate privacy risks and opportunities 3. Ability to manage capacity building processes for the successful implementation of the PIMS 4. Ability to define the documentation and record management processes needed to support the implementation and operations of the PIMS 5. Ability to define and design processes and properly document them 6. Ability to define and implement appropriate information security and privacy training and awareness programs, and communication plans 7. Ability to establish the PIMS communication plan to assist in the understanding of an organization's information security and privacy issues, policies, performance, and providing inputs or suggestions for improving the performance of the PIMS	1. Knowledge of resource management in PIMS implementation processes 2. Knowledge of the process of identifying, analyzing, and evaluating privacy risks and opportunities 3. Knowledge of the required capacities for the successful implementation of the PIMS 4. Knowledge of the roles and responsibilities of key interested parties during and after the implementation and operation of the PIMS 5. Knowledge of the main organizational structures applicable for an organization to manage the PIMS 6. Knowledge of the best practices on documented information life cycle management 7. Knowledge of the characteristics and the differences between the different documented information related to the PIMS policy, procedure, guideline, standard, baseline, worksheet, etc. 8. Knowledge of the characteristics and the best practices of implementing information security and privacy training and awareness programs and communication plans 9. Knowledge of the communication objectives, activities, and interested parties to enhance their support and confidence

Domain 5: Performance evaluation, monitoring, and measurement of the PIMS

Main objective: Ensure that the ISO/IEC 27701 Lead Implementer candidate is able to evaluate, monitor, and measure the performance of the PIMS

Competencies	Knowledge statements
1. Ability to monitor and evaluate the effectiveness of the PIMS 2. Ability to verify to what extent the identified PIMS objectives have been met 3. Ability to define and implement the PIMS internal audit program 4. Ability to perform regular and methodical reviews to ensure the suitability, adequacy, effectiveness, and efficiency of the PIMS based on the organization's policies and objectives 5. Ability to define and perform a management review process	1. Knowledge of the best practices and techniques used to monitor and evaluate the effectiveness of the PIMS 2. Knowledge of the concepts related to measurement and evaluation 3. Knowledge of the main concepts and components related to the implementation and operation of the PIMS internal audit program 4. Knowledge of the difference between a major and a minor nonconformity 5. Knowledge of the best practices used to perform management reviews

Domain 6: Continual improvement of the PIMS

Main objective: Ensure that the ISO/IEC 27701 Lead Implementer candidate is able to provide guidance on the continual improvement of the PIMS

Competencies	Knowledge statements
1. Ability to track and take action on nonconformities 2. Ability to identify and analyze the root causes of nonconformities, and propose action plans to treat them 3. Ability to counsel an organization on how to continualy improve the effectiveness and efficiency of the PIMS 4. Ability to implement continual improvement processes in an organization 5. Ability to determine the appropriate improvement tools to support the continual improvement processes of an organization 6. Ability to determine the appropriate improvement tools to support the continual improvement processes of an organization	1. Knowledge of the main processes, tools, and techniques used to identify the root causes of nonconformities 2. Knowledge of the treatment of nonconformities process 3. Knowledge of the main processes, tools, and techniques used to develop corrective and preventive action plans 4. Knowledge of the main concepts related to continual improvement 5. Knowledge of the processes related to the continual monitoring of change factors 6. Knowledge of the maintenance and improvement of the PIMS

Domain 7: Preparing for the PIMS certification audit

Main objective: Ensure that the ISO/IEC 27701 Lead Implementer candidate is able to prepare an organization for the certification against ISO/IEC 27701

Competencies	Knowledge statements
1. Ability to understand the main steps, processes, and activities related to the ISO/IEC 27701 certification audit 2. Ability to counsel an organization to identify and select a certification body that meets their expectations 3. Ability to determine whether an organization is ready and prepared for the ISO/IEC 27701 certification audit 4. Ability to train and prepare an organization's personnel for the ISO/IEC 27701 certification audit 5. Ability to argue and challenge the audit findings and conclusions with external auditors	1. Knowledge of the types of audit and their differences 2. Knowledge of the differences between Stage 1 and Stage 2 audits 3. Knowledge of the Stage 1 audit requirements, steps, and activities 4. Knowledge of the Stage 2 audit requirements, steps, and activities 5. Knowledge of the audit follow-up requirements, steps, and activities 6. Knowledge of the surveillance audits and recertification audit requirements, steps, and activities 7. Knowledge of the requirements, guidelines, and best practices for developing action plans following the ISO/IEC 27701 certification audit

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

			Level of understanding (Cognitive/Taxonomy) required					
		Points per question	Questions that measure comprehension, application, and analysis	Questions that measure synthesis and evaluation	Number of questions per competency domain	% of the exam devoted to each competency domain	Number of points per competency domain	% of points per competency domain
Competency domains	Fundamental principles and concepts of the privacy information management system (PIMS)	5	X		1	8.33	5	6.67
	Privacy information management system (PIMS)	5	X		1	8.33	5	6.67
	Planning the PIMS implementation	5	X		2	16.68	15	20
		10		X				
	Implementing the PIMS	5	X		5	41.67	35	46.66
		10		X				
		10		X				
		5		X				
		5		X				
	Performance evaluation, monitoring, and measurement of the PIMS	5		X	1	8.33	5	6.67
	Continual improvement of the PIMS	5	X		1	8.33	5	6.67
	Preparing for the PIMS certification audit	5	X		1	8.33	5	6.67
	Total points	75	6	6				
	Number of questions per level of understanding							
	% of the exam devoted to each level of understanding (cognitive/taxonomy)		50	50				

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 Implementer" 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 session
- A hard copy dictionary

The use of electronic devices, such as laptops, smartphones, etc., is 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 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.

EXAMINATION 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: For each of the following clauses of ISO/IEC 27701, provide at least two types of evidence that would provide reasonable assurance that the control measures have been successfully implemented.

1. Clause 6.2.1.1 *Policies for information security*

2. Clause 6.3.2.1 *Mobile device policy*

Example: *Clause 6.5.3.2 Disposal of media*

- *Use of shredding, overwriting, degaussing, and destruction*
- *Perform risk assessment to determine the disposal method (physically destroyed, repair, or discarded)*

Possible answer:

1. **Clause 6.2.1.1 Policies for information security**
   - *Documented information regarding the review of the privacy policies to validate the content*
   - *Verification that applicable legislations and regulations have been considered during the development and maintenance of information security and privacy policies*

2. **Clause 6.3.2.1 Mobile device policy**
   - *Documented information regarding the review of the mobile device policy and its requirements for the physical protection and restriction of software installation*
   - *Checking if the PII stored in mobile devices is de-identified*

Question 2: In ISO/IEC 27701, clause 7.2.3 *Determine when and how consent is to be obtained*, states that: "The organization should determine and document a process by which it can demonstrate if, when and how consent for the processing of PII was obtained from PII principals." As such, provide at least five actions that would ensure conformity to this clause.

Possible answer:

I*n order to comply with the requirements of ISO/IEC 27701, clause 7.2.3, organizations should:*

- *Document the requirements for obtaining consent and provide details on how these requirements have been met*
- *Obtain consent when installing apps on other individuals' devices, for online tracking methods, website cookies, marketing calls or messages, etc.*
- *Include information on what the organization will do with the collected PII in the consent*

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