

# ISO/IEC 27701 LEAD AUDITOR

## Candidate Handbook

## Table of Contents

---

<b>SECTION I: INTRODUCTION .....</b>	<b>3</b>
About PECB .....	3
The Value of PECB Certification.....	4
PECB Code of Ethics.....	5
Introduction to ISO/IEC 27701 Lead Auditor .....	6
<b>SECTION II: EXAMINATION PREPARATION, RULES, AND POLICIES .....</b>	<b>7</b>
Preparing for and scheduling the exam.....	7
Competency domains.....	8
Taking the exam.....	17
Exam Security Policy.....	21
Exam results.....	22
Exam Retake Policy.....	22
<b>SECTION III: CERTIFICATION PROCESS AND REQUIREMENTS .....</b>	<b>23</b>
PECB ISO/IEC 27701 credentials .....	23
Applying for certification .....	24
Professional experience .....	24
Professional references.....	24
PIMS audit experience .....	24
Evaluation of certification applications .....	25
<b>SECTION IV: CERTIFICATION POLICIES .....</b>	<b>26</b>
Denial of certification.....	26
Certification status options .....	26
Upgrade and downgrade of credentials .....	27
Renewing the certification .....	27
Closing a case .....	27
Complaint and Appeal Policy .....	27
<b>SECTION V: GENERAL POLICIES .....</b>	<b>28</b>
Exams and certifications from other accredited certification bodies .....	28
Non-discrimination and special accommodations .....	28
Behavior Policy.....	28
Refund Policy.....	28

## SECTION I: INTRODUCTION

---

### About PECB

PECB is a certification body that provides education<sup>1</sup>, certification, and certificate programs for individuals on a wide range of disciplines.

Through our presence in more than 150 countries, we help professionals demonstrate their competence in various areas of expertise by providing valuable evaluation, certification, and certificate programs against internationally recognized standards.

### Our key objectives are:

1. Establishing the minimum requirements necessary to certify professionals and to grant designations
2. Reviewing and verifying the qualifications of individuals to ensure they are eligible for certification
3. Maintaining and continually improving the evaluation process for certifying individuals
4. Certifying qualified individuals, granting designations and maintaining respective directories
5. Establishing requirements for the periodic renewal of certifications and ensuring that the certified individuals are complying with those requirements
6. Ascertaining that PECB professionals meet ethical standards in their professional practice
7. Representing our stakeholders in matters of common interest
8. Promoting the benefits of certification and certificate programs to professionals, businesses, governments, and the public

### Our mission

Provide our clients with comprehensive examination, certification, and certificate program services that inspire trust and benefit the society as a whole.

### Our vision

Become the global benchmark for the provision of professional certification services and certificate programs.

### Our values

Integrity, Professionalism, Fairness

---

<sup>1</sup> Education refers to training courses developed by PECB and offered globally through our partners.

## The Value of PECB Certification

### Global recognition

PECB credentials are internationally recognized and endorsed by many accreditation bodies, so professionals who pursue them will benefit from our recognition in domestic and international markets.

The value of PECB certifications is validated by the accreditation from the International Accreditation Service (IAS-PCB-111), the United Kingdom Accreditation Service (UKAS-No. 21923) and the Korean Accreditation Board (KAB-PC-08) under ISO/IEC 17024 – General requirements for bodies operating certification of persons. The value of PECB certificate programs is validated by the accreditation from the ANSI National Accreditation Board (ANAB-Accreditation ID 1003) under ANSI/ASTM E2659-18, Standard Practice for Certificate Programs.

PECB is an associate member of The Independent Association of Accredited Registrars (IAAR), a full member of the International Personnel Certification Association (IPC), a signatory member of IPC MLA, and a member of Club EBIOS, CPD Certification Service, CLUSIF, Credential Engine, and ITCC. In addition, PECB is an approved Licensed Partner Publisher (LPP) from the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) for the Cybersecurity Maturity Model Certification standard (CMMC), is approved by Club EBIOS to offer the EBIOS Risk Manager Skills certification, and is approved by CNIL (Commission Nationale de l'Informatique et des Libertés) to offer DPO certification. For more detailed information, click [here](#).

### High-quality products and services

We are proud to provide our clients with high-quality products and services that match their needs and demands. All of our products are carefully prepared by a team of experts and professionals based on the best practices and methodologies.

### Compliance with standards

Our certifications and certificate programs are a demonstration of compliance with ISO/IEC 17024 and ASTM E2659. They ensure that the standard requirements have been fulfilled and validated with adequate consistency, professionalism, and impartiality.

### Customer-oriented service

We are a customer-oriented company and treat all our clients with value, importance, professionalism, and honesty. PECB has a team of experts who are responsible for addressing requests, questions, and needs. We do our best to maintain a 24-hour maximum response time without compromising the quality of the services.

### Flexibility and convenience

Online learning opportunities make your professional journey more convenient as you can schedule your learning sessions according to your lifestyle. Such flexibility gives you more free time, offers more career advancement opportunities, and reduces costs.

## PECB Code of Ethics

The Code of Ethics represents the highest values and ethics that PECB is fully committed to follow, as it recognizes the importance of them when providing services and attracting clients.

The Compliance Division makes sure that PECB employees, trainers, examiners, invigilators, partners, distributors, members of different advisory boards and committees, certified individuals, and certificate holders (hereinafter “PECB professionals”) adhere to this Code of Ethics. In addition, the Compliance Division consistently emphasizes the need to behave professionally and with full responsibility, competence, and fairness in service provision with internal and external stakeholders, such as applicants, candidates, certified individuals, certificate holders, accreditation authorities, and government authorities.

It is PECB’s belief that to achieve organizational success, it has to fully understand the clients and stakeholders’ needs and expectations. To do this, PECB fosters a culture based on the highest levels of integrity, professionalism, and fairness, which are also its values. These values are integral to the organization, and have characterized the global presence and growth over the years and established the reputation that PECB enjoys today.

PECB believes that strong ethical values are essential in having healthy and strong relationships. Therefore, it is PECB’s primary responsibility to ensure that PECB professionals are displaying behavior that is in full compliance with PECB principles and values.

PECB professionals are responsible for:

1. Displaying professional behavior in service provision with honesty, accuracy, fairness, and independence
2. Acting at all times in their service provision solely in the best interest of their employer, clients, the public, and the profession in accordance with this Code of Ethics and other professional standards
3. Demonstrating and developing competence in their respective fields and striving to continually improve their skills and knowledge
4. Providing services only for those that they are qualified and competent and adequately informing clients and customers about the nature of proposed services, including any relevant concerns or risks
5. Informing their employer or client of any business interests or affiliations which might influence or impair their judgment
6. Preserving the confidentiality of information of any present or former employer or client during service provision
7. Complying with all the applicable laws and regulations of the jurisdictions in the country where the service provisions were conducted
8. Respecting the intellectual property and contributions of others
9. Not communicating intentionally false or falsified information that may compromise the integrity of the evaluation process of a candidate for a PECB certification or a PECB certificate program
10. Not falsely or wrongly presenting themselves as PECB representatives without a proper license or misusing PECB logo, certifications or certificates
11. Not acting in ways that could damage PECB’s reputation, certifications or certificate programs
12. Cooperating in a full manner on the inquiry following a claimed infringement of this Code of Ethics

To read the complete version of PECB’s Code of Ethics, go to [Code of Ethics | PECB](#).

## **Introduction to ISO/IEC 27701 Lead Auditor**

ISO/IEC 27701 defines the requirements for establishing, implementing, maintaining, and continually improving the privacy information management system (PIMS). The protection of personally identifiable information has become a societal need since, almost everyone who has an internet connection, has their PII exposed. The standard defines the requirements and provides guidance for protecting PII on an ongoing, ever evolving basis. In the dynamic world of technology, it is evident that organizations need guidance to securely handle PII and properly implement the PIMS.

Training courses delivered by PECB help participants enhance their competence to effectively plan and perform audits in conformance with the certification process of ISO/IEC 27701, apply audit techniques and practices, and manage (or be part of) audit teams and audit programs.

Considering that auditing is one of the most in-demand professions, an internationally recognized certification can help you achieve your professional goals. The “ISO/IEC 27701 Lead Auditor” credential is a professional certification for individuals aiming to demonstrate the competence to audit the 27701 management system and lead an audit team.

PECB certifications are not a license or simply a membership. They attest the candidates’ knowledge and skills gained through our training courses and are issued to candidates that have the required experience and have passed the exam.

This document specifies the PECB ISO/IEC 27701 Lead Auditor certification scheme in compliance with ISO/IEC 17024:2012. It also outlines the steps that candidates should take to obtain and maintain their credentials. As such, it is very important to carefully read all the information included in this document before completing and submitting your application. If you have questions or need further information after reading it, please contact the PECB international office at [certification.team@pecb.com](mailto:certification.team@pecb.com).

## SECTION II: EXAMINATION PREPARATION, RULES, AND POLICIES

---

### Preparing for and scheduling the exam

All candidates are responsible for their own study and preparation for certification exams. Although candidates are not required to attend the training course to be eligible for taking the exam, attending it can significantly increase their chances of successfully passing the exam.

To schedule the exam, candidates have two options:

1. Contact one of our authorized partners. To find an authorized partner in your region, please go to [Active Partners](#). The training course schedule is also available online and can be accessed on [Training Events](#).
2. Take a PECB exam remotely through the [PECB Exams application](#). To schedule a remote exam, please go to the following link: [Exam Events](#).

To learn more about exams, competency domains, and knowledge statements, please refer to *Section III* of this document.

### Rescheduling the exam

For any changes with regard to the exam date, time, location, or other details, please contact [online.exams@pecb.com](mailto:online.exams@pecb.com).

### Application fees for examination and certification

Candidates may take the exam without attending the training course. The applicable prices are as follows:

- Lead Exam: \$1000<sup>2</sup>
- Manager Exam: \$700
- Foundation Exam: \$500
- Transition Exam: \$500

The application fee for certification is \$500.

For the candidates that have attended the training course via one of PECB's partners, the application fee covers the costs of the exam (first attempt and first retake), the application for certification, and the first year of Annual Maintenance Fee (AMF).

---

<sup>2</sup> All prices listed in this document are in US dollars.

## Competency domains

The “ISO/IEC 27701 Lead Auditor” credential is a professional certification for individuals aiming to demonstrate the competence to audit the privacy information management system and lead an audit team.

The most important skills required in the market are the ability to effectively plan and perform audits in conformity to the certification process, apply audit techniques and practices, and manage (or be part of) audit teams and audit programs.

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

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

The content of the exam is divided as follows:

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



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

**Main objective:** Ensure that the candidate is able to explain and apply ISO/IEC 27701 principles and concepts.

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

## Domain 2: Privacy information management system (PIMS)

**Main objective:** Ensure that the candidate is able to identify and explain the requirements for a privacy information management system based on ISO/IEC 27701.

Competencies	Knowledge statements
<ol style="list-style-type: none"> <li>1. Ability to identify, understand, classify, and explain the requirements of ISO/IEC 27701</li> <li>2. Ability to distinguish and illustrate the information security and privacy requirements and best practices by using concrete examples</li> <li>3. Ability to understand, explain, and illustrate the main steps to establish, implement, monitor, review, maintain, and improve an organization's PIMS</li> <li>4. Ability to analyze, evaluate, and validate action plans to implement a specific control or process</li> </ol>	<ol style="list-style-type: none"> <li>1. Knowledge of ISO/IEC 27701 requirements</li> <li>2. Knowledge of the best practices in information security and privacy management</li> <li>3. Knowledge of the establishment, implementation, and maintenance of information security and privacy management procedures</li> <li>4. Knowledge of the implementation and management of action plans to support PIMS</li> </ol>

## Domain 3: Fundamental audit concepts and principles

**Main objective:** Ensure that the candidate is able to interpret and apply the main concepts and principles related to a PIMS audit.

Competencies	Knowledge statements
<ol style="list-style-type: none"> <li>1. Ability to understand, explain, and apply the principles of auditing based on ISO 19011</li> <li>2. Ability to identify and judge situations that would discredit the professionalism of the auditor and PECB code of ethics</li> <li>3. Ability to identify and evaluate exceptions to the confidentiality principle required by law and authorized interested parties</li> <li>4. Ability to explain, illustrate, and apply the evidence-based and risk-based auditing approach in the context of an ISO/IEC 27701 audit</li> <li>5. Ability to explain and compare the types and characteristics of audit evidence</li> <li>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</li> <li>7. Ability to judge the appropriate level of reasonable assurance in the context of an ISO/IEC 27701 audit</li> </ol>	<ol style="list-style-type: none"> <li>1. Knowledge of the main audit concepts and terminology based on ISO 19011</li> <li>2. Knowledge of types of audits such as first party audit (internal audit), second party audit, and third party audit</li> <li>3. Knowledge of audit objectives and audit criteria</li> <li>4. Knowledge of principles of auditing such as integrity, fair presentation, due professional care, confidentiality, independence, evidence-based approach, and risk-based approach</li> <li>5. Knowledge of professional responsibilities of an auditor and the PECB code of ethics</li> <li>6. Knowledge of the types of audit evidence such as physical, mathematical, confirmative, technical, analytical, documentary, and verbal</li> <li>7. Knowledge of the quality and reliability of audit evidence</li> <li>8. Knowledge of the audit approach based on risk</li> <li>9. Knowledge of the concepts of materiality and reasonable assurance and their applicability in an audit</li> </ol>

## Domain 4: Preparing an ISO/IEC 27701 audit

**Main objective:** Ensure that the candidate is able to prepare a PIMS management system audit.

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

## Domain 5: Conducting an ISO/IEC 27701 audit

**Main objective:** Ensure that the candidate is able to conduct a PIMS audit.

Competencies	Knowledge statements
1. Ability to conduct a stage 1 audit	1. Knowledge of the objectives and steps of the stage 1 audit
2. Ability to prepare and conduct on-site activities	2. Knowledge of the points to validate during the stage 1 audit
3. Ability to plan the stage 2 audit and assign work to the audit team	3. Knowledge of types of documented information to be audited
4. Ability to prepare audit test plans and the documented information for stage 2 audit	4. Knowledge of the verification of internal audit documents
5. Ability to conduct a stage 2 audit	5. Knowledge of audit planning steps and how to prepare audit test plans
6. Ability to organize and conduct an opening meeting	6. Knowledge of the principles of maintaining audit working documents
7. Ability to conduct audit tests	7. Knowledge of the objectives and the content of the opening meeting of an audit
8. Ability to explain, illustrate, and apply evidence collection procedures	8. Knowledge of the audit tests
9. Ability to explain, illustrate, and apply evidence analysis procedures	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 an ISO/IEC 27701 audit

**Main objective:** Ensure that the candidate is able to conclude a PIMS audit and conduct audit follow-up activities.

Competencies	Knowledge statements
<ol style="list-style-type: none"> <li>1. Ability to determine audit finding, draft nonconformities, and conduct quality review</li> <li>2. Ability to draft a nonconformity report</li> <li>3. Ability to determine, agree, and draft the audit conclusions</li> <li>4. Ability to conduct the closing meeting</li> <li>5. Ability to prepare and distribute the audit report</li> <li>6. Ability to make the certification decision and give recommendations for improvement</li> <li>7. Ability to evaluate action plans by the auditor</li> <li>8. Ability to conduct audit follow-up activities and conduct surveillance activities</li> <li>9. Ability to plan and conduct recertification audit</li> </ol>	<ol style="list-style-type: none"> <li>1. Knowledge of audit findings, nonconformities, observations, and anomalies</li> <li>2. Knowledge of the differences between major nonconformity, minor nonconformity, observation, and anomaly</li> <li>3. Knowledge of documenting the audit findings and drafting a nonconformity report</li> <li>4. Knowledge of the best practices to draft nonconformity report</li> <li>5. Knowledge of the evaluation process of evidences to determine, agree, and draft the audit conclusions</li> <li>6. Knowledge of the guidelines and best practices to present audit findings and audit conclusion to the auditee</li> <li>7. Knowledge of the organization and content of the closing meeting</li> <li>8. Knowledge of content and distribution of the audit report</li> <li>9. Knowledge of content and evaluation of action plans</li> <li>10. Knowledge of audit follow-up activities and surveillance activities</li> <li>11. Knowledge of the certification cycle and conditions for extension, suspension or withdrawal, and transfer of the certification</li> </ol>

## Domain 7: Managing an ISO/IEC 27701 audit program

**Main objective:** Ensure that the candidate is able to establish and manage a PIMS audit program.

Competencies	Knowledge statements
<ol style="list-style-type: none"> <li>1. Ability to understand and explain the audit program and the use of PDCA model</li> <li>2. Ability to understand and explain the implementation of ISO/IEC 27701 audit program</li> <li>3. Ability to understand and explain the responsibilities to protect the integrity, availability, and confidentiality of the audit records</li> <li>4. Ability to achieve independence, objectivity, and impartiality of the audit function</li> <li>5. Ability to evaluate the efficiency of the audit program by monitoring, reviewing, and improving the audit program</li> </ol>	<ol style="list-style-type: none"> <li>1. Knowledge of the use of PDCA model in the management of an audit program</li> <li>2. Knowledge of the audit program resources and records</li> <li>3. Knowledge of the differences between the internal and external audits</li> <li>4. Knowledge of the structure of the audit charter</li> <li>5. Knowledge of the main internal audit services and activities</li> <li>6. Knowledge of the continual internal audit program</li> <li>7. Knowledge of the monitoring, evaluating, reviewing, and improving an audit program</li> </ol>

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

		Level of understanding (Cognitive/Taxonomy) required		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
		Points per question	Questions that measure comprehension, application, and analysis				
Competency domains	Fundamental principles and concepts of a 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 an ISO/IEC 27701 audit	5	X	2	16.67	15	20
		10	X				
	Conducting an ISO/IE 27701 audit	5	X	3	25	15	20
		5	X				
		5	X				
	Closing an ISO/IE 27701 audit	10	X	2	16.67	20	26.66
		10	X				
	Managing an ISO/IE 27701 audit program	5	X	1	8.33	5	6.67
Total points		75					
Number of questions per level of understanding			8	4			
% of the exam devoted to each level of understanding (cognitive/taxonomy)			66.7	33.3			

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

After successfully passing the exam, candidates will be able to apply for obtaining the “PECB Certified ISO/IEC 27701 Lead Auditor” credential.



## Taking the exam

### General information about 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 Partner 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 information about online exams, go 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.** Essay-type questions 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 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.

This is an open-book exam. The candidate is allowed to use the following reference materials:

- A hard copy of the ISO/IEC 27701 standard
- Training course materials (accessed through the PECB Exams app and/or printed)
- Any personal notes taken during the training course (accessed through the PECB Exams app and/or printed)
- A hard copy dictionary

A sample of exam questions will be provided below.

**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).

For specific information about exam types, languages available, and other details, please contact [examination.team@pecb.com](mailto:examination.team@pecb.com) or go to the [List of PECB Exams](#).

## Sample exam questions

### 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*
  - *Observation 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.

### Possible answer:

AUDIT TEST PLAN	
<b>Audit criteria:</b> <i>The organization should notify the customer of any legally binding requests for disclosure of PII.</i>	
<b>Observation</b>	<i>The audit team should observe how the organization notifies its customers in case of any legally binding requests for disclosure of PII.</i>
<b>Documented information review</b>	<i>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.</i>

<b>Interview</b>	<i>The audit team should interview personnel responsible for the implementation of procedures on how to notify the customer for disclosure of PII.</i>
<b>Technical verification</b>	<i>N/A</i>
<b>Analysis</b>	<i>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.</i>

## Exam Security Policy

PECB is committed to protect the integrity of its exams and the overall examination process, and relies upon the ethical behavior of applicants, potential applicants, candidates and partners to maintain the confidentiality of PECB exams. This Policy aims to address unacceptable behavior and ensure fair treatment of all candidates.

Any disclosure of information about the content of PECB exams is a direct violation of this Policy and PECB's Code of Ethics. Consequently, candidates taking a PECB exam are required to sign an Exam Confidentiality and Non-Disclosure Agreement and must comply with the following:

1. The questions and answers of the exam materials are the exclusive and confidential property of PECB. Once candidates complete the submission of the exam to PECB, they will no longer have any access to the original exam or a copy of it.
2. Candidates are prohibited from revealing any information regarding the questions and answers of the exam or discuss such details with any other candidate or person.
3. Candidates are not allowed to take with themselves any materials related to the exam, out of the exam room.
4. Candidates are not allowed to copy or attempt to make copies (whether written, photocopied, or otherwise) of any exam materials, including, without limitation, any questions, answers, or screen images.
5. Candidates must not participate nor promote fraudulent exam-taking activities, such as:
  - Looking at another candidate's exam material or answer sheet
  - Giving or receiving any assistance from the invigilator, candidate, or anyone else
  - Using unauthorized reference guides, manuals, tools, etc., including using "brain dump" sites as they are not authorized by PECB

Once a candidate becomes aware or is already aware of the irregularities or violations of the points mentioned above, they are responsible for complying with those, otherwise if such irregularities were to happen, candidates will be reported directly to PECB or if they see such irregularities, they should immediately report to PECB.

Candidates are solely responsible for understanding and complying with PECB Exam Rules and Policies, Confidentiality and Non-Disclosure Agreement and Code of Ethics. Therefore, should a breach of one or more rules be identified, candidates will not receive any refunds. In addition, PECB has the right to deny the right to enter a PECB exam or to invite candidates for an exam retake if irregularities are identified during and after the grading process, depending on the severity of the case.

Any violation of the points mentioned above will cause PECB irreparable damage for which no monetary remedy can make up. Therefore, PECB can take the appropriate actions to remedy or prevent any unauthorized disclosure or misuse of exam materials, including obtaining an immediate injunction. PECB will take action against individuals that violate the rules and policies, including permanently banning them from pursuing PECB credentials and revoking any previous ones. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

## Exam results

Exam results will be communicated via email.

- 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 a re-evaluation by writing to [examination.team@pecb.com](mailto:examination.team@pecb.com) within 30 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 days from the date they received the reevaluated exam results to file a complaint through the [PECB Ticketing System](#). Any complaint received after 30 days will not be processed.

## Exam Retake Policy

There is no limit to the number of times a candidate can retake an exam. However, there are certain limitations in terms of the time span between exam retakes.

If a candidate does not pass the exam on the 1st attempt, they must wait 15 days after the initial date of the exam for the next attempt (1st retake).

**Note:** Candidates who have completed the training course with one of our partners, and failed the first exam attempt, are eligible to retake for free the exam within a 12-month period from the date the coupon code is received (the fee paid for the training course, includes a first exam attempt and one retake). Otherwise, retake fees apply.

For candidates that fail the exam retake, PECB recommends they attend a training course in order to be better prepared for the exam.

To arrange exam retakes, based on exam format, candidates that have completed a training course, must follow the steps below:

1. Online Exam: when scheduling the exam retake, use initial coupon code to waive the fee
2. Paper-Based Exam: candidates need to contact the PECB Partner/Distributor who has initially organized the session for exam retake arrangement (date, time, place, costs).

Candidates that have not completed a training course with a partner, but sat for the online exam directly with PECB, do not fall under this Policy. The process to schedule the exam retake is the same as for the initial exam.

## SECTION III: CERTIFICATION PROCESS AND REQUIREMENTS

### PECB ISO/IEC 27701 credentials

All PECB certifications have specific requirements regarding education and professional experience. To determine which credential is right for you, take into account your professional needs and analyze the criteria for the certifications.

The credentials in the PECB ISO/IEC 27701 scheme have the following requirements:

Credential	Education	Exam	Professional experience	MS audit/assessment experience	Other requirements
PECB Certified ISO/IEC 27701 Provisional Auditor	At least secondary education	PECB Certified ISO/IEC 27701 Lead Auditor exam or equivalent	None	None	<a href="#">Signing the PECB Code of Ethics</a>
PECB Certified ISO/IEC 27701 Auditor			Two years: One year of work experience in privacy information management	Audit activities: a total of 200 hours	
PECB Certified ISO/IEC 27701 Lead Auditor			Five years: Two years of work experience in privacy information management	Audit activities: a total of 300 hours	
PECB Certified ISO/IEC 27701 Senior Lead Auditor			Ten years: Seven years of work experience in privacy information management	Audit activities: a total of 1,000 hours	

To be considered valid, the audit activities should follow best audit practices and include the following:

1. Planning an audit
2. Managing an audit program
3. Drafting audit reports
4. Drafting nonconformity reports
5. Drafting audit working documents
6. Reviewing and managing documented information related to the audit
7. Conducting on-site audits
8. Following up on nonconformities
9. Leading an audit team

## Applying for certification

All candidates who successfully pass the exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credential they were assessed for. Specific educational and professional requirements need to be fulfilled in order to obtain a PECB certification. Candidates are required to fill out the online certification application form (that can be accessed via their PECB account), including contact details of individuals who will be contacted to validate the candidates' professional experience. Candidates can submit their application in English, French, German, Spanish or Korean languages. They can choose to either pay online or be billed. For additional information, please contact [certification.team@pecb.com](mailto:certification.team@pecb.com).

The online certification application process is very simple and takes only a few minutes:

- [Register](#) your account
- Check your email for the confirmation link
- [Log in](#) to apply for certification

For more information on how to apply for certification, click [here](#).

The Certification Department validates that the candidate fulfills all the certification requirements regarding the respective credential. The candidate will receive an email about the application status, including the certification decision.

Following the approval of the application by the Certification Department, the candidate will be able to download the certificate and claim the corresponding Digital Badge. For more information about downloading the certificate, click [here](#), and for more information about claiming the Digital Badge, click [here](#).

PECB provides support both in English and French.

## Professional experience

Candidates must provide complete and correct information regarding their professional experience, including job title(s), start and end date(s), job description(s), and more. Candidates are advised to summarize their previous or current assignments, providing sufficient details to describe the nature of the responsibilities for each job. More detailed information can be included in the résumé.

## Professional references

For each application, two professional references are required. They must be from individuals who have worked with the candidate in a professional environment and can validate their privacy information management experience, as well as their current and previous work history. Professional references of persons who fall under the candidate's supervision or are their relatives are not valid.

## PIMS audit experience

The candidate's audit log will be checked to ensure that they have completed the required number of audit hours. The following audit types constitute valid audit experience: pre-audit, internal audits, second party audits, or third party audits.



## **Evaluation of certification applications**

The Certification Department will evaluate each application to validate the candidates' eligibility for certification or certificate program. A candidate whose application is being reviewed will be notified in writing and, if necessary, given a reasonable time frame to provide any additional documentation. If a candidate does not respond by the deadline or does not provide the required documentation within the given time frame, the Certification Department will validate the application based on the initial information provided, which may lead to the candidates' credential downgrade.

## SECTION IV: CERTIFICATION POLICIES

---

### Denial of certification

PECB can deny certification/certificate program if candidates:

- Falsify the application
- Violate the exam procedures
- Violate the PECB Code of Ethics

Candidates whose certification/certificate program has been denied can file a complaint through the complaints and appeals procedure. For more detailed information, refer to [Complaint and Appeal Policy](#) section.

The application payment for the certification/certificate program is nonrefundable.

### Certification status options

#### Active

Means that your certification is in good standing and valid, and it is being maintained by fulfilling the PECB requirements regarding the CPD and AMF.

#### Suspended

PECB can temporarily suspend candidates' certification if they fail to meet the requirements. Other reasons for suspending certification include:

- PECB receives excessive or serious complaints by interested parties (suspension will be applied until the investigation has been completed.)
- The logos of PECB or accreditation bodies are willfully misused.
- The candidate fails to correct the misuse of a certification mark within the determined time by PECB.
- The certified individual has voluntarily requested a suspension.
- PECB deems appropriate other conditions for suspension of certification.

#### Revoked

PECB can revoke (that is, to withdraw) the certification if the candidate fails to satisfy its requirements. In such cases, candidates are no longer allowed to represent themselves as PECB Certified Professionals.

Additional reasons for revoking certification can be if the candidates:

- Violate the PECB Code of Ethics
- Misrepresent and provide false information of the scope of certification
- Break any other PECB rules
- Any other reasons that PECB deems appropriate

Candidates whose certification has been revoked can file a complaint through the complaints and appeals procedure. For more detailed information, refer to [Complaint and Appeal Policy](#) section.

## Other statuses

Besides being active, suspended, or revoked, a certification can be voluntarily withdrawn or designated as Emeritus. To learn more about these statuses and the permanent cessation status, go to [Certification Status Options](#).

## Upgrade and downgrade of credentials

### Upgrade of credentials

Professionals can upgrade their credentials as soon as they can demonstrate that they fulfill the requirements.

To apply for an upgrade, candidates need to log into their PECB account, visit the “My Certifications” tab, and click on “Upgrade.” The upgrade application fee is \$100.

### Downgrade of credentials

A PECB Certification can be downgraded to a lower credential due to the following reasons:

- The AMF has not been paid.
- The CPD hours have not been submitted.
- Insufficient CPD hours have been submitted.
- Evidence on CPD hours has not been submitted upon request.

**Note:** *PECB certified professionals who hold Lead certifications and fail to provide evidence of certification maintenance requirements will have their credentials downgraded. The holders of Master Certifications who fail to submit CPDs and pay AMFs will have their certifications revoked.*

## Renewing the certification

PECB certifications are valid for three years. To maintain them, PECB certified professionals must meet the requirements related to the designated credential, e.g., they must fulfill the required number of continual professional development (CPD) hours. In addition, they need to pay the annual maintenance fee (\$120). For more information, go to the [Certification Maintenance](#) page on the PECB website.

## Closing a case

If candidates do not apply for certification within one year, 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 to [certification.team@pecb.com](mailto:certification.team@pecb.com) and pay the required fee.

## Complaint and Appeal Policy

Any complaints must be made no later than 30 days after receiving the certification decision. PECB will provide a written response to the candidate within 30 working days after receiving the complaint. If candidates do not find the response satisfactory, they have the right to file an appeal.

For more information about the Complaint and Appeal Policy, click [here](#).

## SECTION V: GENERAL POLICIES

---

### Exams and certifications from other accredited certification bodies

PECB accepts certifications and exams from other recognized accredited certification bodies. PECB will evaluate the requests through its equivalence process to decide whether the respective certification(s) or exam(s) can be accepted as equivalent to the respective PECB certification (e.g., ISO/IEC 27701 Lead Auditor certification).

### Non-discrimination and special accommodations

All candidate applications will be evaluated objectively, regardless of the candidates' age, gender, race, religion, nationality, or marital status.

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations<sup>3</sup> for candidates, when appropriate. If candidates need special accommodations because of a disability or a specific physical condition, they should inform the partner/distributor in order for them to make proper arrangements<sup>4</sup>. Any information that candidates provide regarding their disability/special needs will be treated with confidentiality. To download the Candidates with Disabilities Form, click [here](#).

### Behavior Policy

PECB aims to provide top-quality, consistent, and accessible services for the benefit of its external stakeholders: distributors, partners, trainers, invigilators, examiners, members of different committees and advisory boards, and clients (trainees, examinees, certified individuals, and certificate holders), as well as creating and maintaining a positive work environment which ensures safety and well-being of its staff, and holds the dignity, respect and human rights of its staff in high regard.

The purpose of this Policy is to ensure that PECB is managing unacceptable behavior of external stakeholders towards PECB staff in an impartial, confidential, fair, and timely manner. To read the Behavior Policy, click [here](#).

### Refund Policy

PECB will refund your payment, if the requirements of the Refund Policy are met. To read the Refund Policy, click [here](#).

---

<sup>3</sup> According to ADA, the term "reasonable accommodation" may include: (A) making existing facilities used by employees readily accessible to and usable by individuals with disabilities; and (B) job restructuring, part-time or modified work schedules, reassignment to a vacant position, acquisition or modification of equipment or devices, appropriate adjustment or modifications of examinations, training materials or policies, the provision of qualified readers or interpreters, and other similar accommodations for individuals with disabilities.

<sup>4</sup> ADA Amendments Act of 2008 (P.L. 110–325) Sec. 12189. Examinations and courses. [Section 309]: Any person that offers examinations or courses related to applications, licensing, certification, or credentialing for secondary or post-secondary education, professional, or trade purposes shall offer such examinations or courses in a place and manner accessible to persons with disabilities or offer alternative accessible arrangements for such individuals.

**Address:**

Headquarters  
6683 Jean Talon E,  
Suite 336 Montreal,  
H1S 0A5, QC,  
CANADA

**Tel./Fax:**

T: +1-844-426-7322  
F: +1-844-329-7322

**Emails:****Examination:**

[examination.team@pecb.com](mailto:examination.team@pecb.com)

**Certification:**

[certification.team@pecb.com](mailto:certification.team@pecb.com)

**Customer Service:**

[support@pecb.com](mailto:support@pecb.com)

**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.

[www.pecb.com](http://www.pecb.com)