When Recognition Matters

EXAM PREPARATION GUIDE

PECB Certified Lead Privacy Implementer

The objective of the “PECB Certified Privacy Lead Implementer” examination is to ensure that the candidate has the knowledge to support an organization in managing Privacy framework and for understanding best practices used to implement concepts of Privacy framework.

The target population for this examination is:

- Compliance Project Implementer
- Privacy Services Implementer
- Project Regulatory Compliance IT Professional
- Safety and Privacy Project Specialist
- Information Security Officer
- Head of Governance Risk and Compliance

The exam content covers the following domains:

- Domain 1: Fundamental principles and concepts in Privacy Implementation
- Domain 2: Privacy Implementation Best Practices based on ISO 29100
- Domain 3: Designing and Developing an Organizational Privacy Implementation Framework based on ISO 29100
- Domain 4: Implementing a Privacy Framework
- Domain 5: Designing and Implementing Privacy Controls
- Domain 6: Performance Monitoring and Measuring
- Domain 7: Improving the Privacy Implementation Process

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts in Privacy Implementation

Main objective: To ensure that the Certified Lead Privacy Implementer candidate can understand, interpret and illustrate the main Privacy Implementation concepts related to published standards including ISO 29100

Competencies	Knowledge statements
1. Understand and explain the operations of the ISO organization and the development of Privacy Implementation Standards 2. Ability to identify, analyze and evaluate the Privacy Implementation compliance requirements for an organization 3. Ability to explain and illustrate the main concepts in Privacy Implementation and Information Security Privacy risk management 4. Understanding of the differences in Privacy across differing territories 5. Understand the issues related to privacy from the use of specific applications and technologies covering Cloud Computing, Outsourcing, Offshoring, Mobile Applications and Smart Devices 6. Understanding of the relevant legal, regulatory and contractual issues related to Privacy Implementation 7. Ability to understand the concept of and identify Personal Identifiable Information (PII)	1. Knowledge of the application of the eight ISO management principles to Privacy Implementation 2. Knowledge of the main standards in Privacy Implementation 3. Knowledge of the different sources of Privacy Implementation requirement for an organization: laws, regulations, international and industry standards, contracts, market practices, internal policies 4. Knowledge of the main Privacy Implementation concepts and terminology as described in ISO 29100 5. Knowledge of the concept of privacy risk and its application in Privacy Implementation 6. Knowledge of the differing technologies and technology management techniques which can have a direct impact on privacy 7. Knowledge of the strategies and approaches to develop and implement an effective Privacy Implementation Framework

Domain 2: Privacy Implementation Best Practices based on ISO 29100

Main objective: To ensure that the Certified Lead Privacy Implementer candidate can understand, interpret and provide guidance on how to implement and manage Privacy Implementation requirements based on best practices of ISO 29100

Competencies	Knowledge statements
1. Ability to identify, understand, classify and explain the clauses with requirements from ISO 29100 2. Ability to detail and illustrate the requirements and best practices by concrete examples 3. Ability to compare possible solutions to Privacy Implementation issues of an organization and identify/analyze the strength and weakness of each solution 4. Ability to select and demonstrate the best Privacy Implementation solution in order to address Privacy Implementation objectives stated by the organization 5. Ability to create and justify an action plan to implement a Privacy Implementation Framework by identifying the stages and key components 6. Ability to prepare a credible Privacy Implementation Framework can be incorporated into an operating environment.	1. Knowledge of operational planning and control 2. Knowledge of business impact analysis and privacy risk assessment 3. Knowledge of Privacy Implementation strategy 4. Knowledge of establishing and implementing Privacy Implementation procedures 5. Knowledge of establishing Privacy Response Procedures 6. Knowledge of exercising and testing 7. Knowledge of Privacy Implementation Controls Best Practices 8. Knowledge of Privacy Implementation Best Practices

Domain 3: Designing and Developing an Organizational Privacy Implementation Framework based on ISO 29100

Main objective: To ensure that the Certified Lead Privacy Implementer candidate can plan the implementation of an effective Privacy Implementation Process

Competencies

1. Ability to manage a project to develop an effective Privacy Implementation Framework following project management best practices
2. Ability to gather, analyze and interpret the necessary information to plan the implementation of a Privacy Implementation Framework
3. Ability to observe, analyze and interpret the external and internal environment of an organization
4. Ability to gather the necessary information to contribute to the design of an effective and aligned Privacy Implementation Framework
5. Ability to state and justify a Privacy Implementation scope, response strategies and times adapted to the security objectives of a specific organization
6. Ability to select and justify the selected approach and methodology adapted to the needs of the organization
7. Ability to design a Privacy Implementation Framework which can integrate with other common management system standards such as ISO/IEC 27001

Knowledge statements

1. Knowledge of the main project management concepts, terminology, process and best practice as described in ISO 10006
2. Knowledge of the principal approaches and methodology frameworks to implement a Privacy Implementation Framework
3. Knowledge of the main concepts and terminology related to organizations
4. Knowledge of an organization's external and internal environment
5. Knowledge of the main interested parties related to an organization and their characteristics
6. Knowledge of techniques to gather information necessary to design the Privacy Implementation Framework
7. Knowledge of the characteristics of the Privacy Implementation Scope, response strategies and timeframes
8. Knowledge of the key legislation and regulatory requirements which influence the design of the Privacy Implementation Framework

Domain 4: Implementing a Privacy Framework

Main objective: To ensure that the Certified Lead Privacy Implementer candidate can implement the Privacy Implementation process and associated security controls required for an effective Privacy Implementation process

Competencies

1. Ability to understand, analyze needs and provide guidance on the attribution of roles and responsibilities in the context of the implementation and management of an Privacy Implementation Process
2. Ability to define the document and record management processes needed to support the implementation and the operations of an Privacy Implementation Process
3. Ability to define and design security controls & processes which support Privacy Implementation and document them
4. Ability the define and writing an Privacy Implementation policy and Privacy Implementation policies & procedures
5. Ability to implement the required processes and security controls of a Privacy Implementation Framework
6. Ability to define and implement appropriate Privacy Implementation training, awareness and communication plans
7. Ability to define and implement a Privacy Implementation Framework based on Privacy Implementation best practices
8. Ability to transfer a Privacy Implementation project to operations and manage the change management process

Knowledge statements

1. Knowledge of the roles and responsibilities of the key actors during the implementation of a Privacy Implementation Process and in its operation after the end of the implementation project
2. Knowledge of the main organizational structures applicable for an organization to effectively manage Privacy
3. Knowledge of the best practices on document and record management processes and the document management life cycle
4. Knowledge of the characteristics and the differences between the different documents related to a Privacy Implementation Framework: policy, procedure, guideline, standard, baseline, worksheet, etc.
5. Knowledge of model-building controls, process techniques and best practices
6. Knowledge of controls and processes deployment techniques and best practices
7. Knowledge of techniques and best practices to write Privacy Implementation policies, procedures and others types of documents included in a Privacy Implementation Framework
8. Knowledge of the characteristics and the best practices to implement Privacy Implementation training, awareness and communication plans
9. Knowledge of the characteristics and main processes of information management related to the Privacy Implementation Framework based on best practices
10. Knowledge of change management techniques best practices

Domain 5: Designing and Implementing Privacy Controls

Main objective: To ensure that Certified Lead Privacy Implementer Candidate can effectively operate a Privacy Implementation Framework

Competencies	Knowledge statements
1. Ability to identify where elements of a Privacy Framework should be applied within an organization. 2. Ability to conduct a Privacy Impact Assessment and associated Privacy risk Assessment. 3. Ability to respond a potential Privacy breach or allegation of such a breach. 4. Ability to assess the supply chain and identify Privacy risks posed by the supply chain. 5. Ability to apply Privacy principles to a variety of business scenarios.	1. Knowledge of data and PII and the circumstances when Privacy should be considered 2. Knowledge of the Privacy Impact Process and associated Privacy risk Assessment Processes 3. Knowledge of Incident Response and the methods to respond to Data Breaches involving PII 4. Knowledge of the privacy risks posed by Outsourcing, Cloud Computing and Offshoring and how to effectively manage these risks 5. Knowledge of privacy principles and their effect on Business decisions.

Domain 6: Performance Monitoring and Measuring

Main objective: To ensure that the Certified Lead Privacy Implementer candidate can evaluate, monitor and measure the performance of a Privacy Implementation Framework

Competencies	Knowledge statements
1. Ability to monitor and evaluate the effectiveness of a Privacy Implementation Framework 2. Ability to verify the extent to which identified Privacy requirements are being met. 3. Ability to monitor trends and patterns related to Privacy and identify root causes of any failures 4. Ability to analyze the handling of events which may have compromised Privacy 5. Ability to perform regular and methodical reviews regarding the suitability, adequacy, effectiveness and efficiency of an Privacy Implementation Framework with policies and objectives of an organization 6. Ability to define and implement an internal audit process for Privacy.	1. Knowledge of the techniques and best practices to monitor the effectiveness of a Privacy Implementation Framework 2. Knowledge of the main concepts and components related to a Privacy Implementation Measurement Program: measures, attributes, indicators, dashboard, etc. 3. Knowledge of the characteristics and the differences between an operational, tactical and strategic Privacy Implementation indicators and dashboards 4. Knowledge of the techniques and methods to define and document adequate and reliable indicators 5. Knowledge of how to identify trends and the root cause of Privacy breaches.

Domain 7: Improving the Privacy Implementation Process

Main objective: To ensure that the Certified Lead Privacy Implementer candidate can provide guidance on the Continual improvement of a Privacy Implementation Framework

Competencies	Knowledge statements
1. Ability to understand the principle and concepts related to continual improvement 2. Ability to counsel an organization on how to continually improve the effectiveness and the efficiency of a Privacy Implementation Framework 3. Ability to implement a Privacy Implementation Framework continual improvement processes in an organization 4. Ability to determine the appropriate business improvement tools to support continual improvement processes of a specific organization 5. Ability to identify, analyze the root-causes of negative findings 6. Ability to identify, analyze the root-cause of potential problems and proposed action plans to treat them	1. Knowledge of the main concepts related to continual improvement 2. Knowledge of the characteristics and the difference between the concept of effectiveness and the efficiency 3. Knowledge of the concept and techniques to perform a benchmarking 4. Knowledge of the main processes, tools and techniques used by professionals to identify the root-causes of negative findings 5. Knowledge of the characteristics and the difference between corrective actions and preventive actions 6. Knowledge of the main processes, tools and techniques used by professionals to develop effective corrective and preventative action plans

Based on these 7 domains and their relevance, 12 questions are included in the exam, as summarized in the following table:

				Level of Understanding (Cognitive/Taxonomy) Required					
		Question Number	Points per Question	Questions that measure Comprehension, Application and Analysis	Question that measure Synthesis and Evaluation	Number of Questions per competency domain	% of test devoted to each competency domain	Number of points per competency domain	% of points per competency domain
Competency Domains	Fundamental principles and concepts in Privacy Implementation	1	5	x		2	16.67	20	26.67
		2	5	x					
	Privacy Implementation Best Practices based on ISO 29100	4	10	x		3	25.00	15	20.00
		3	5	x					
		6	10	x					
	Designing and Developing an Organizational Privacy Implementation Framework based on ISO 29100	11	5		x	1	8.33	5	6.67
	Implementing a Privacy Framework	8	5		x	3	25.00	10	13.33
		12	5		x				
		7	5		x				
	Designing and Implementing Privacy Controls	10	10		x	1	8.33	15	20.00
	Performance Monitoring and Measuring	9	5		x	1	8.33	5	6.67
	Improving the Privacy Implementation Process	5	5		x	1	8.33	5	6.67
Total Points			75						
Number of Questions per level of understanding				5	7				
% of Test Devoted to each level of understanding (Cognitive/Taxonomy)				41.67	58.33				

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

After successfully passing the exam, candidates will be able to apply for the credentials of PECB Certified Lead Privacy Implementer, depending on their level of experience.

TAKE A CERTIFICATION EXAM

Candidates will be required to arrive at least thirty (30) minutes before the beginning of the certification exam. Candidates arriving late will not be given additional time to compensate for the late arrival and may be denied entry to the exam room (if they arrive more than 5 minutes after the beginning of the exam scheduled time).

All candidates will need to present a valid identity card with a picture such as a driver's license or a government ID to the proctor and the exam confirmation letter.

The exam duration is three (3) hours.

The questions are essay type questions. This type of format was chosen because the intent is to determine whether an examinee can write a clear coherent answer/argument and to assess problem solving techniques. Because of this particularity, the exam is set to be "open book" and does not measure the recall of data or information. The examination evaluates, instead, comprehension, application, analysis, synthesis and evaluation, which mean that even if the answer is in the course material, candidates will have to justify and give explanations, to show they really understood the concepts. At the end of this document, you will find sample exam questions and their possible answers.

As the exams are "open book"; the candidates are authorized to use the following reference materials:

- A copy of the 29100:2011standard,
- Course notes from the Participant Handout,
- Any personal notes made by the student during the course and
- A hard copy dictionary.

The use of electronic devices, such as laptops, cell phones, etc., is not allowed.

All attempt to copy, collude or otherwise cheat during the exam will automatically lead to the exam's failure.

PECB exams are available in English. For availability of the exam in a language other than English, please contact examination@pecb.com

RECEIVE YOUR EXAM RESULTS

Results will be communicated by email in a period of 6 to 8 weeks, after taking the exam. The results will not include the exact grade of the candidate, only a mention of pass or fail.

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

In the case of a failure, the results will be accompanied with the list of domains in which the candidate had a low grade, to provide guidance for exams' retake preparation.

Candidates who disagree with the exam results may file a complaint. For more information, please refer to www.pecb.com

EXAM RETAKE POLICY

There is no limitation on how many times a candidate can retake the same exam. However, there are some limitations in terms of allowed time-frame in between exams.

When candidates fail the examination, they are only allowed to retake the examination once within 12 months after the first attempt. If second examination is unsuccessful, candidates will be allowed to retake the exam only after 1 year (12 months). Retake fee applies.

Only candidates, who have completed a full PECB training but fail the written exam, are eligible to retake the exam for free, under one condition:

"A candidate can only retake the exam once and this retake must occur within 12 months from the initial exam's date."

When candidates fail the same examination for the second time, their file is automatically closed for 1 year.

CLOSING FILES

Closing a file is equivalent to rejecting a candidate's application. As a result, when candidates request that their file be reopened, PECB will no longer be bound by the conditions, standards, policies, candidate handbook or exam preparation guide that were in effect before their file was closed.

Candidates who want to request that their file be reopened must do so in writing, and pay the required fees.

EXAMINATION SECURITY

A significant component of a successful and respected professional certification credential is maintaining the security and confidentiality of the examination. PECB relies upon the ethical behaviour of certificate holders and applicants to maintain the security and confidentiality of

PECB examinations. When someone who holds PECB credentials reveals information about PECB examination content, they violate the PECB Code of Ethics. PECB will take action against individuals who violate PECB Policies and the Code of Ethics. Actions taken may include permanently barring individuals from pursuing PECB credentials and revoking certifications from those who have been awarded the credential. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

SAMPLE EXAM QUESTIONS AND POSSIBLE ANSWERS

1. Interpretation of ISO clauses

For each of the following clauses of the Privacy framework standard (ISO 29100), please provide an action plan with at least two concrete actions that would be acceptable to ensure conformity to the clause and fulfill control objectives.

Example: 4.5 Privacy safeguarding requirements

Make sure to involve very specific restrictions on the processing of Personally Identifiable Information (PII) with defined roles and responsibilities respective to privacy framework, Mandate the implementation of specific privacy controls and record the high-level privacy principles by meeting the requirements to privacy according to safeguarding checklist tailored to tasks.

2. Development of metrics

For each of the following clauses of the Privacy framework standard (ISO 29100), please provide two examples of metrics that would be acceptable to measure the conformity to the clause.

Example: 4.6 Privacy policies

- Approved privacy policy from Board of Directors
- Communicated the implementation within the organization in a visible document for employees

3. Recommendations

The management of the organization would like to receive recommendations from you to improve the processes in place to comply with the requirements of Privacy framework (ISO 29100) on control of documents

Possible answers:

1. Document and implement a procedure for control of documents
2. Maintain a log for documents changes with records of the approvals
3. Communicating the new process and organize training session.