PECB

BEYOND RECOGNITION

ISO/IEC 27034 LEAD APPLICATION SECURITY IMPLEMENTER

Candidate Handbook

PECB

Table of Contents

SECTION I: INTRODUCTION

About PECB[1]

PECB is a leading certification body dedicated to fostering digital trust through comprehensive education, certification, and certificate programs across various disciplines. We empower professionals to develop and demonstrate their competence in digital security and other areas of expertise by providing world-class certification programs that adhere to internationally recognized standards.

Slogan:
Beyond Recognition

Vision:
As the global leader in digital trust education and certification, our vision is to empower and inspire professionals by enhancing their skills and fostering their professional success.

Mission:
Our mission is to empower professionals with the knowledge and skills to protect their digital assets and ensure business continuity. Through our comprehensive training programs, we aim to foster a secure digital ecosystem where innovation thrives and risks are managed effectively.

Values
Growth, Change, Harmony, Simplicity, Reliability and Quality

[1] **Notes:**

- The legal name of PECB is "PECB Group Inc."
- PECB is an acronym that stands for "Professional Evaluation and Certification Board."
- Education (used in the first sentence of this page) refers to training courses developed by PECB, and offered globally through its network of partners.
- Certification refers to certification services provided according to ISO/IEC 17024.
- Certificate Program refers to certificate program services provided according to ANSI/ASTM E2659.
- The term "certified" shall only be used for personnel certifications, based on ISO/IEC 17024 requirements. The term "certificate holder" shall only be used for certificate programs, based on ANSI/ASTM E2659 requirements. Certificate holders are not certified, licensed, accredited, or registered to engage in a specific occupation or profession.

The Value of PECB Certification/Certificate Program

Accreditation

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.

Our certifications are distinguished by prestigious global accreditations, affirming both their value and your expertise. PECB certifications are validated by top-tier bodies including the International Accreditation Service (IAS-PCB-111), the United Kingdom Accreditation Service (UKAS-No. 21923), the Korean Accreditation Board (KAB-PC-08), and Comité français d'accréditation (COFRAC N° 4-0637) under ISO/IEC 17024 – General requirements for bodies operating certification of persons. Additionally, our certificate programs are 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 also an esteemed associate member of The Independent Association of Accredited Registrars (IAAR), and 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, and CLUSIF. Furthermore, we hold an approved status as an Approved Publishing Partner (APP) by the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) for the Cybersecurity Maturity Model Certification standard (CMMC), and are authorized by Club EBIOS to offer the EBIOS Risk Manager Skills certification and by CNIL (Commission Nationale de l'Informatique et des Libertés) to offer the DPO's skills and knowledge 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. Our Customer Support team is available 24 hours a day, 7 days a week to address questions, requests and needs.

PECB Code of Ethics

The Code of Ethics are the values and ethics that PECB is committed to follow, and defines the responsibilities of PECB professionals including employees, trainers, examiners, invigilators, members of different committees, partners, distributors, certified individuals and certificate holders.

To read the complete version of PECB's Code of Ethics, go to Code of Ethics | PECB.

Introduction to ISO/IEC 27034 Lead Application Security Implementer

This document specifies the PECB ISO/IEC 27034 Lead Application Security Implementer 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 certification.team@pecb.com.

PECB

SECTION II: EXAMINATION PREPARATION, RULES, AND POLICIES

Preparing for and scheduling the exam

Candidates are responsible for their own studying and preparation for certification exams. No specific set of training courses or curriculum of study is required as part of the certification process.

To schedule the exam, candidates have two options:

1. **Online:** Through the PECB Exams application. To schedule a remote exam, please go to the following link: Exam Events.
2. **Paper-based:** By contacting the PECB authorized partner that provided the training course. The partner arranges the date, time, and the location where the candidate is going to attend the exam.

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.

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[2]
- Manager Exam: $700
- Foundation Exam: $500
- Transition Exam: $500

The application fee for certification are as follows:

- Master Certification: $100
- Foundation Certification: $200
- Transition Certification: $200
- All other Certifications: $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).

[2] All prices listed in this document are in US dollars.

Competency domains

The ISO/IEC 27034 Lead Application Security Implementer certification is intended for:

- Application security professionals responsible for managing and implementing security measures in the software development life cycle
- IT and information security managers who need to ensure secure application development within their organizations
- Compliance officers and risk managers focused on achieving regulatory compliance and reducing application-related security risks
- Software developers and architects who want to integrate security practices into the development and design processes
- Consultants seeking to broaden their expertise in application security and ISO/IEC 27034 implementation
- Individuals interested in advancing their careers in information security, with a focus on application security

The content of the exam is divided as follows:

- **Domain 1:** Fundamental principles and concepts of application security
- **Domain 2:** Application security planning
- **Domain 3:** Implementation of application security controls
- **Domain 4:** Application security incident management and response
- **Domain 5:** Verifying and monitoring application security
- **Domain 6:** Continual improvement and auditing of application security

Domain 1: Fundamental principles and concepts of application security

Main objective: Ensure that the candidate is able to interpret ISO/IEC 27034 principles and concepts.

Competencies	Knowledge statements
1. Ability to discuss the relationship between ISO/IEC 27034 and other standards and regulatory frameworks 2. Ability to interpret the scope and structure of ISO/IEC 27034, including its key components such as ONF, ASMP, and ASC 3. Ability to explain the fundamental concepts and principles of application security, including its types and the role of information assets 4. Ability to identify vulnerabilities, threats, and consequences within the context of application security 5. Ability to apply the CIA triad (confidentiality, integrity, and availability) and assess its importance in application security processes	1. Knowledge of the ISO/IEC 27000 family of standards and their interrelationship with ISO/IEC 27034 2. Knowledge of the scope and multi-part structure of ISO/IEC 27034 3. Knowledge of the advantages and benefits of adopting ISO/IEC 27034 4. Knowledge of application security concepts, types, and core principles 5. Knowledge of vulnerabilities, threats, consequences, and information security risks 6. Knowledge of the CIA triad and its role in securing information assets 7. Knowledge of information security risk assessment in the context of application security

Domain 2: Application security planning

Main objective: Ensure that the candidate is able to define the application security scope, understand organizational and application-level planning processes, and implement processes such as the ONF management process and application security management process in alignment with ISO/IEC 27034**.**

Competencies	Knowledge statements
1. Ability to analyze an organization's mission, objectives, values, and strategies	1. Knowledge of how an organization's mission, objectives, values, and strategies influence application security planning
2. Ability to define the scope of application security and differentiate it from the scope of the application itself	2. Knowledge of the differences between the application security scope and the application scope
3. Ability to analyze the business, regulatory, and technological contexts that impact application security	3. Knowledge of the regulatory, business, and technological contexts impacting application security and compliance
4. Ability to identify and analyze the interested parties	4. Knowledge of the roles of internal and external stakeholders in application security
5. Ability to identify critical identity management and permissions information	5. Knowledge of critical identity management, permissions information, and application specifications
6. Ability to assess which application specifications and information need protection	6. Knowledge of types of organizational planning
7. Ability to analyze and apply types of organizational planning, including strategic, tactical, operational, and contingency planning	7. Knowledge of ONF structure, establishment, and management
8. Ability to design and implement the Organization Normative Framework (ONF), including establishing the ONF committee	8. Knowledge of the roles, responsibilities, and qualifications repository within the ONF
9. Ability to implement and manage the ONF management process	9. Knowledge of the ONF management process
10. Ability to define the roles, responsibilities, and qualifications repository	10. Knowledge of the process for establishing an application security policy
11. Ability to establish and maintain an application security policy aligned with organizational objectives	11. Knowledge of the ASMP and its purpose in managing application security
12. Ability to describe the Application Security Management Process (ASMP) and its relationship with the ONF	12. Knowledge of the relationship of the ASMP with the ONF
13. Ability to identify application security requirements and assess environmental factors	13. Knowledge of how to identify application requirements and assess the application environment
14. Ability to develop and maintain the Application Normative Framework (ANF)	14. Knowledge of the development and maintenance of the ANF
15. Ability to verify and document the outcomes of application security verification activities	15. Knowledge of verification process for application security

Domain 3: Implementation of application security controls

Main objective: Ensure that the candidate is able to implement application security controls and security practices.

Competencies	Knowledge statements
1. Ability to identify and define the information requirements for implementing application security controls (ASCs) effectively 2. Ability to identify essential information for ASC 3. Ability to define the security objectives of ASC 4. Ability to plan and execute security activities and verification measurements for ASC 5. Ability to analyze and apply the principles of secure design 6. Ability to implement security practices for ensuring application security	1. Knowledge of the structure and components of ASCs 2. Knowledge of information requirements for implementing ASCs 3. Knowledge of best practices for establishing clear objectives for ASCs 4. Knowledge of methods for measuring security activities and verification metrics 5. Knowledge of the principles for secure design implementation 6. Knowledge of processes for implementing security as code 7. Knowledge of implementing least privilege across systems 8. Knowledge of the importance of separating duties to minimize risks 9. Knowledge of best practices for implementing and maintaining application security

Domain 4: Application security incident management and response

Main objective: Ensure that the candidate is able to implement advanced application security technologies develop training and awareness programs, and effectively manage and respond to security incidents.

Competencies	Knowledge statements
1. Ability to interpret the role of artificial intelligence and machine learning in enhancing security	1. Knowledge of the role of artificial intelligence and machine learning in strengthening security
2. Ability to analyze the principles behind zero trust architecture	2. Knowledge of the best practices on zero trust architecture
3. Ability to apply strategies for securing application programming interfaces (APIs)	3. Knowledge of strategies for securing application programming interfaces (APIs)
4. Ability to apply strategies for securing containers, including the use of specialized operating systems, segmentation, and specific security tools	4. Knowledge of key strategies for securing containers
5. Ability to apply identity and access management principles and practices	5. Knowledge of identity and access management (IAM) principles and implementation methods
6. Ability to interpret application security incident management	6. Knowledge of application security incident management
7. Ability to plan and prepare for application security incidents	7. Knowledge of planning and preparation for application security incidents
8. Ability to develop and implement an application security incident management policy	8. Knowledge of application security policies
9. Ability to develop an incident management plan	9. Knowledge of incident management plan
10. Ability to establish an incident response team	10. Knowledge of incident management reports
11. Ability to respond effectively to application security incidents	11. Knowledge of incident response teams establishment and integration
12. Ability to interpret the concepts of competence, training, and awareness	12. Knowledge of the necessary steps to respond to application security incidents
13. Ability to develop and implement awareness and competence development programs	13. Knowledge of designing and implementing awareness programs and activities
	14. Knowledge of competence development needs and programs
	15. Knowledge of competence development evaluation programs

Domain 5: Verifying and monitoring application security

Main objective: Ensure that the candidate is able to verify, test and monitor application security.

Competencies	Knowledge statements
1. Ability to interpret the key steps of the application security verification process	1. Knowledge of application security verification process
2. Ability to identify and validate ANF elements from the ONF	2. Knowledge of identifying and validating ANF elements from the ONF
3. Ability to assess security risks related to the application	3. Knowledge of application security risks identification and analysis
4. Ability to identify and validate application security requirements	4. Knowledge of procedures for reviewing and ensuring the accuracy of application security requirements
5. Ability to identify and validate the Target Level of Trust	5. Knowledge of identifying and validating the Target Level of Trust for applications
6. Ability to conduct verification measurements for ASCs and update the ANF	6. Knowledge of processes for conducting verification measurements of Application Security Controls (ASCs) and updating the ANF accordingly
7. Ability to monitor, review, and continually improve the ONF	7. Knowledge of roles and responsibilities involved for monitoring and reviewing the ONF
8. Ability to define roles and responsibilities for monitoring and reviewing the ONF	8. Knowledge of what needs to be monitored and measured
9. Ability to decide what needs to be monitored and measured	9. Knowledge of establishing performance indicators
10. Ability to establish key performance indicators	10. Knowledge of monitoring result reporting

Domain 6: Continual improvement and auditing of application security

Main objective: Ensure that the candidate is able to implement continual improvement processes for application security and support auditing activities.

Competencies	Knowledge statements
1. Ability to distinguish between different types of audits 2. Ability to interpret Prediction Application Security Rationale (PASR) 3. Ability to effectively plan and manage audit activities 4. Ability to manage the audit process and oversee the audit execution 5. Ability to continually monitor change factors 6. Ability to continually improve the application security	1. Knowledge of different types of audits 2. Knowledge of the PASR and its role in forecasting application security assurance 3. Knowledge of the initiation and preparation phases of the audit 4. Knowledge of the activities involved in conducting the audit 5. Knowledge of the completion phase of the audit 6. Knowledge of the treatment of nonconformities process 7. Knowledge of the audit follow-up activities 8. Knowledge of application security continual improvement 9. Knowledge of best practices for documenting improvements

Based on the above-mentioned domains and their relevance, the exam contains 80 multiple-choice questions, as summarized in the table below:

				Level of understanding (Cognitive/Taxonomy) required	
		Number of questions/points per competency domain	% of the exam devoted/points to/for each competency domain	Questions that measure comprehension, application, and analysis	Questions that measure evaluation
Competency domains	Fundamental principles and concepts of application security	10	12.5	X	
	Application security planning	20	25	X	
	Implementation of application security controls	20	25		X
	Application security incident management and response	10	12.5		X
	Verifying and monitoring application security	10	12.5	X	
	Continual improvement and auditing of application security	10	12.5		X
	Total	**80**	**100%**		
	Number of questions per level of understanding			**40**	**40**
	% of the exam devoted to each level of understanding (cognitive/taxonomy)			**50%**	**50%**

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

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) Online Exam: Exams are provided electronically via the PECB Exams application. The use of secondary electronic devices, such as tablets and phones, are not allowed during the exam. The exam session is supervised remotely by a PECB Invigilator via the PECB Exams application and an external/integrated camera.

PECB Exam Types:

a. Multiple-choice, closed-book, where the candidates are not allowed to use any reference materials. Usually, Foundation and Transition exams are of this type.

b. Essay-type, open-book, where candidates are allowed to use the following reference materials:

   - A hard copy of main standard
   - Training course materials (through KATE and/or printed)
   - Any personal notes taken during the training course (through KATE and/or printed)
   - A hard copy dictionary

c. Multiple-choice, open-book, where candidates are allowed to use the following reference materials:

   - A hard copy of main standard
   - Training course materials (through KATE and/or printed)
   - Any personal notes taken during the training course (through KATE and/or printed)
   - A hard copy dictionary

2) Paper Based: Exams are also available in a paper format. 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.

PECB Exam Types:

a. Multiple-choice, closed-book, where the candidates are not allowed to use any reference materials. Usually, Foundation and Transition exams are of this type.

b. Essay-type, open-book, where candidates are allowed to use the following reference materials:

- A hard copy of main standard
- Training course materials (printed)
- Any personal notes taken during the training course (printed)
- A hard copy dictionary

c. Multiple-choice, open-book, where candidates are allowed to use the following reference materials:

- A hard copy of main standard
- Training course materials (printed)
- Any personal notes taken during the training course (printed)
- A hard copy dictionary

For specific information about exam types, languages available, and other details, please contact support@pecb.com or go to the List of PECB Exams.

This exam comprises multiple-choice questions: The multiple-choice exam can be used to evaluate candidates' understanding on both simple and complex concepts. It comprises both stand-alone and scenario-based questions. Stand-alone questions stand independently within the exam and are not context-depended, whereas scenario-based questions are context-dependent, i.e., they are developed based on a scenario which a candidate is asked to read and is expected to provide answers to five questions related to that scenario. When answering stand-alone and scenario-based questions, candidates will have to apply various concepts and principles explained during the training course, analyze problems, identify and evaluate alternatives, combine several concepts or ideas, etc.

Each multiple-choice question has three options, of which one is the correct response option (keyed response) and two incorrect response options (distractors).

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

- A hard copy of the ISO/IEC 27034 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.

Sample exam questions

Nexora, an e-commerce company, provides secure and personalized online shopping experiences. With a growing global presence and increasing regulatory demands, *Nexora* decided to adopt ISO/IEC 27034 standards to integrate security into its application development processes and ensure alignment with its business goals.

Initially, the company defined the scope of application security by establishing security objectives, identifying key processes and activities, engaging relevant stakeholders, and outlining critical identity management and permissions requirements. Next, it analyzed the business, regulatory, and technological context, as well as specified the applications and information requiring protection.

As part of the Organization Normative Framework (ONF), *Nexora* ensured alignment of organizational processes with relevant laws and regulations. *Nexora* established the ONF committee, granting it the authority for internal communication and for maintaining and improving the ONF; however it did not appoint a candidate for each role. During the ONF design process, *Nexora* set application security goals and determined the scope for the current iteration. The company's priorities and strategies, as well as ONF elements deemed necessary for the iteration, were also defined and designed.

The committee established an application security policy as part of its ONF, ensuring it aligned with other organizational policies and the broader Information Security Management System (ISMS). This alignment guaranteed consistency across all security practices, promoting regulatory compliance and reducing the risk of security gaps. The security policy was incorporated into the business context of the ONF, serving as a key source of security requirements for application projects. These requirements were integrated into the Application Security Controls (ASCs), helping to mitigate potential risks associated with application development and operations. Additionally, the committee provided clear implementation guidance through the ONF, enabling employees and partners to understand and follow security protocols without needing to consult the full standard. By referencing the security policy, the company addressed compliance requirements and managed risks effectively, ensuring a consistent application of security measures across all business units.

During the establishment of the ONF, *Nexora* engaged in planning activities to assign specific tasks, organize processes, and establish policies to support the initiative's success. These daily activities were essential to ensure the tactical goals were executed effectively, aligning with the company's operational needs.

Based on this scenario, answer the following questions:

1. **In the last paragraph, what phase of organizational planning did *Nexora* engage in?**
   A. Contingency planning
   B. **Operational planning**
   C. Strategy planning

2. **From which source is *Nexora's* ONF influenced?**

A. **Regulatory context**
B. Customer context
C. Marketing context

3. **Did *Nexora* fully apply the requirements for establishing the ONF committee?**
   A. Yes, because *Nexora* granted authority to the committee for internal communication.
   B. **No, because Nexora did not define roles and responsibilities for committee members.**
   C. No, because *Nexora* should have grated the committee solely the authority to establish the ONF.

4. **Which step of the ONF design process did *Nexora* NOT follow?**
   A. Determining the scope for the current ONF iteration, essential for defining focus areas and guiding the design process
   B. Establishing an inventory of relevant information and categorizing it by security needs
   C. Defining goals for application security to ensure the ONF design aligns with organizational priorities

5. **Did *Nexora* establish the application security policy in accordance to ISO/IEC 27034-2?**
   A. **Yes, *Nexora* aligned its application security policy with the ONF and other organizational policies.**
   B. No, *Nexora's* policy did not address compliance requirements.
   C. No, *Nexora's* policy was not integrated with the ASCs.

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.

If candidates do not agree with the results, they have 30 days from the date of receiving the results to file a complaint through the PECB Ticketing System. Complaints received after 30 days will not be processed.

Exam Retake Policy

There is no limit 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 the 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.

Exam Security Policy

A significant component of a professional certification credential is maintaining the security and confidentiality of the exam. PECB relies upon the ethical behavior of certification holders and applicants to maintain the security and confidentiality of PECB exams. Any disclosure of information about the content of PECB exams is a direct violation of PECB's Code of Ethics. PECB will take action against any individuals that violate such rules and policies, including permanently banning individuals 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.

PECB

SECTION III: CERTIFICATION PROCESS AND REQUIREMENTS

PECB ISO/IEC 27034 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 27034 scheme have the following requirements:

Credential	Exam	Professional experience	MS project experience	Other requirements
PECB Certified ISO/IEC 27034 Provisional Application Security Implementer	PECB Certified ISO/IEC 27034 Lead Application Security Implementer exam	None	None	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27034 Application Security Implementer		Two years: One year of work experience in application security	Project activities: a total of 200 hours	
PECB Certified ISO/IEC 27034 Lead Application Security Implementer		Five years: Two years of work experience in application security	Project activities: a total of 300 hours	
PECB Certified ISO/IEC 27034 Senior Lead Application Security Implementer		Ten years: Seven years of work experience in application security	Project activities: a total of 1,000 hours	

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

1. Defining the application security scope
2. Planning security implementation at both organizational and application levels
3. Implementing and enforcing application security controls, policies, and best practices
4. Establishing a structured incident management process
5. Verifying, testing, and monitoring application security
6. Ensuring audit readiness by facilitating audit planning, supporting audits, addressing audit findings, and integrating improvements

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 professional experience 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. They can choose to either pay online or be billed. For additional information, please contact 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.

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 CV.

Professional references

For each application, two professional references are required. Professional references shall be individuals who have worked with you in a professional environment and can validate your expertise in the respective field, current, and previous work history. You cannot use as a reference the persons who fall under your supervision or are a relative of yours.

Application security project experience

The candidate's application security project log will be checked to ensure that the candidate has the required number of implementation hours.

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/Certificate Program

PECB can deny certification/certificate program if candidates:

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

Any concerns regarding the denial of certification/certificate program may file a complaint or appeal by following the complaint and appeal process (https://pecb.com/en/complaint-and-appeal-procedure).

The application payment for the certification/certificate program is nonrefundable. This is because of the process of verifying the application, the evidence submitted by the candidates, and the engagement of the relevant departments in this process.

Suspension of Certification

PECB can temporarily suspend certification if the candidate fails to satisfy the requirements of PECB. Additional reasons for suspension can be if:

- 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/certificate program.

Individuals whose certification has been suspended, are not authorized to further promote their certification while it is suspended.

A suspended certification can either be:

- Reinstated – if reasons for suspension are corrected within the given time frame by PECB
- Revoked – if reasons for suspension are not corrected within the given time frame by PECB

Suspended members must remediate their suspension within a maximum period of 6 months.

Note 1: *For ISO/IEC 27005:2022 Risk Manager/Lead Risk Manager, failure to submit the CPD and AMF payment during the cycle will result in a 12-month suspension period, during which you can address any outstanding AMFs and CPDs. If no action is taken during the suspension period, the certification will be revoked.*

Note 2: *For CNIL– DPO, failure to comply with the recertification requirements (work experience in data protection and passing the CNIL– DPO recertification exam) will result in a 12-month suspension period. If no action is taken during the suspension period, the certification will be revoked.*

Revocation of Certification

PECB can revoke (that is, to withdraw) certification if the candidate fails to satisfy the requirements of PECB. Candidates are then no longer allowed to represent themselves as PECB certified professionals. Additional reasons can be if candidates:

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

Individuals whose certification has been revoked, are not authorized to use any references to a certified status.

Individuals whose certification has been revoked may file a complaint or appeal by following the complaint and appeal process (https://pecb.com/en/complaint-and-appeal-procedure).

Note 1: *For ISO/IEC 27005:2022 Risk Manager/Lead Risk Manager, failure to submit the CPD and AMF payment during the cycle will result in a 12-month suspension period, during which you can address any outstanding AMFs and CPDs. If no action is taken during the suspension period, the certification will be revoked.*

Note 2: *For CNIL– DPO, failure to comply with the recertification requirements (work experience in data protection and passing the CNIL– DPO recertification exam) will result in a 12-month suspension period. If no action is taken during the suspension period, the certification will be revoked.*

Other Statuses

Besides being active, suspended, or revoked, a certification can be voluntary withdrawn, or designated as Emeritus.

Emeritus Status

Means that your certification is in good standing, but does not need to be maintained by fulfilling CPD nor AMF requirements.

To qualify and be eligible to apply for the Emeritus status, you must be over 60 years of age, have held a PECB certification for at least five years, and you must no longer practice job functions that are specific to the certification.

Optionally, Emeritus who would like to continue practicing job functions, such as audits and/or implementation projects, must report their CPDs on an annual basis, and fulfill a minimum annual requirement of 20 hours of work experience, implementation/auditing or consulting-related experience, training, private study, coaching, attendance at seminars and conferences, or other relevant activities. AMF is not required.

To apply for this status, please complete the form and send it to certification@pecb.com.

Important note: *In order to return to active certification status, you are required to retake the exam and apply for certification.*

Check the brochure for more information about the benefits of the Emeritus Certification Status.

Voluntary Withdrawal Status

Means that your certification is in good standing, but you decide you do not want to maintain your certification(s) anymore.

To apply for this status, please complete the form and send it to certification@pecb.com.
Individuals whose certification has been voluntarily withdrawn will no longer be allowed to present themselves as PECB Certified Professionals.

Important note: *In order to return to active certification status, you are required to retake the exam and apply for certification.*

Permanent Cessation Status

In the event that the certified individual passes away or becomes incapacitated (e.g., because of an accident), the legal representative is responsible for sending the required information to PECB (i.e., death certificate or medical certificate). Consequently, the name of the person will be removed from the contact list and the PECB account will be deleted.

Upgrade and downgrade of credentials

Upgrade of credentials
PECB Professionals can apply for a higher credential once they provide evidence that proves that they fulfill the requirements of the higher credential.

PECB Certifications can be upgraded online through your dashboard by logging here, clicking **My Certifications** and then the **Upgrade** button.

For more information about the upgrade fee, go to the Certification Maintenance page on the PECB website.

Note: *For downgraded certifications that need to be upgraded, an evaluation will be done to determine if an exam is required prior to obtain an upgraded certification.*

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

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

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. 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 and pay the required fee.

Complaint and Appeal Policy

Any complaint that a candidate has must be submitted in writing no later than 30 days after PECB's initial decision. Within 30 working days of receiving the complaint, PECB will provide a written response to the candidate, outlining the results of the review and any actions taken.

Candidates may request a re-evaluation of their exam results or certification decision within 30 days. If not satisfied, they can file an appeal through the PECB Ticketing System. For more detailed information, please refer to the Complaint and Appeal Policy | PECB

PECB

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 27034 Lead Application Security Implementer 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[3] 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[4]. 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.

[3] 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.

[4] 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

Certification:
certification.team@pecb.com

Customer Service:
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