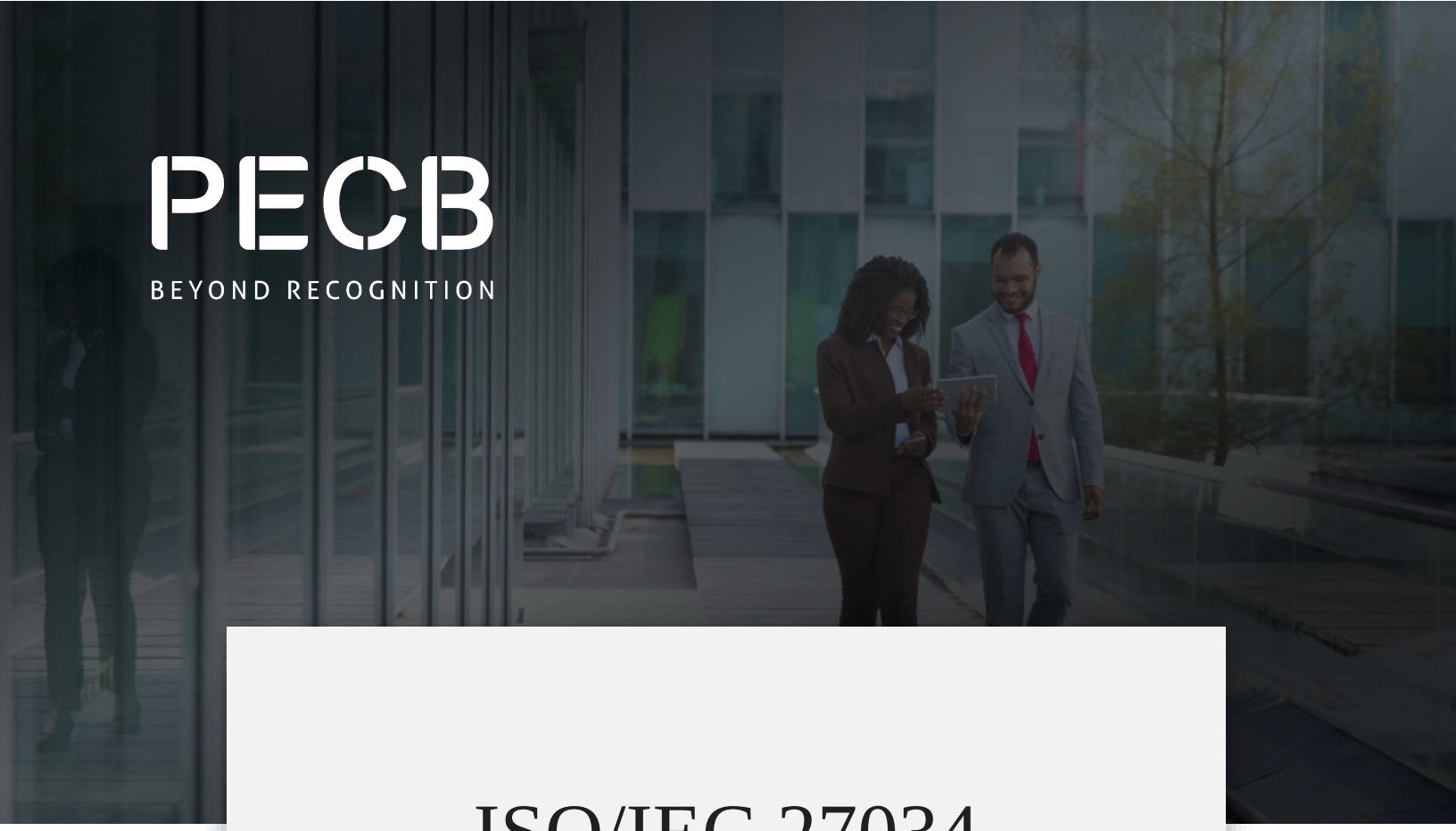
PECB

BEYOND RECOGNITION



ISO/IEC 27034 LEAD APPLICATION SECURITY AUDITOR

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 Auditor Certification

This document specifies the PECB ISO/IEC 27034 Lead Application Security 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 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 Auditor certification is intended for:

- Auditors seeking to conduct and lead audits of ISO/IEC 27034 application security processes
- Information security and IT professionals responsible for application security governance
- Consultants and managers involved in application security compliance assessments
- Members of audit teams and individuals preparing for ISO/IEC 27034 application security audit

The content of the exam is divided as follows:

- **Domain 1:** Fundamental principles and concepts of application security
- **Domain 2:** Application security audit concepts and principles
- **Domain 3:** Initiating an application security audit
- **Domain 4:** Preparing an application security audit
- **Domain 5:** Conducting an application security audit
- **Domain 6:** Audit closure and follow-up for application security

Domain 1: Fundamental principles and concepts of application security

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

Competencies	Knowledge statements
1. Ability to describe the fundamental concepts and principles of application security	1. Knowledge of the fundamental concepts and principles of application security
2. Ability to discuss the structure and scope of each part of the ISO/IEC 27034 series and relation to each other	2. Knowledge of the main objectives and structure of ISO standards related to application security
3. Ability to identify standards related to ISO/IEC 27034 family of standards	3. Knowledge of main concepts and types of application security
4. Ability to discuss the advantages derived from integrating ISO/IEC 27034	4. Knowledge of application's threats and vulnerabilities
5. Ability to identify the main requirements and guidelines of ISO/IEC 27034	5. Knowledge of common types of malicious software and how they affect an organization
6. Ability to explain the overall processes of ISO/IEC 27034	6. Knowledge of Organization Normative Framework (ONF) and its components
	7. Knowledge of Application Security Management Process (ASMP)

Domain 2: Application security audit concepts and principles

Main objective: Ensure that the candidate is able to explain the fundamental concepts and principles of application security audits and identify the key characteristics of the Targeted and Actual Levels of Trust.

Competencies	Knowledge statements
1. Ability to identify Targeted and Actual Levels of Trust to applications based on organizational risk management practices	1. Knowledge of the Application Security Control Library and how it supports Level of Trust definitions
2. Ability to explain the fundamental audit concepts and principles	2. Knowledge of how Levels of Trust function within the application security framework
3. Ability to differentiate between audit activities during the provisioning stages and the operation stages	3. Knowledge of the main audit concepts and principles
4. Ability to interpret audit best practices based on ISO 19011 and ISO/IEC 17021-1	4. Knowledge of audit best practices based on ISO 19011 and ISO/IEC 17021-1
5. Ability to interpret and differentiate audit activities across an application's life cycle	5. Knowledge of different types of audits
6. Ability to recognize the involved parties during the audit process	6. Knowledge of involved parties' competencies and responsibilities during the audit process
	7. Knowledge of evidence-based approach and risk-based approach to audit planning

Domain 3: Initiating an application security audit

Main objective: Ensure that the candidate is able to initiate an application security audit and plan activities accordingly.

Competencies	Knowledge statements
1. Ability to describe the audit initiation process 2. Ability to identify key factors for selecting an effective audit team 3. Ability to recognize the importance of prioritizing audit activities when developing an audit schedule 4. Ability to determine the feasibility of an audit by evaluating the availability of necessary information 5. Ability to adapt to the audit approach to the context of small organizations, considering simplified documentation, limited segregation of duties, and the central role of the owner or manager	1. Knowledge of audit's information, objectives, scope, methods, and audit team 2. Knowledge of the audit offer and its elements 3. Knowledge of valid reasons for which an auditee can reject an auditor for conducting the audit 4. Knowledge of how audit objectives, scope, and criteria are defined and aligned with the overall audit program and how they influence the planning, execution, and potential modification of individual audits 5. Knowledge of the feasibility of an audit by evaluating the availability of information, auditee cooperation, and sufficient time and resources to achieve audit objectives 6. Knowledge of the requirements for handling, retaining, and disclosing audit-related information, including confidentiality obligations, legal exceptions, and the importance of mutual agreement between audit participants

Domain 4: Preparing an application security audit

Main objective: Ensure that the candidate is able to effectively plan and organize an application security audit.

Competencies	Knowledge statements
1. Ability to prepare for an audit by conducting document reviews, assessing risks related to the auditee's context, evaluating prior audit findings, and contributing to the development of the audit plan	1. Knowledge of the procedures involved in audit preparation, including document review, risk assessment, audit planning, evaluation of prior findings, and the development of methods for assessing controls and identifying residual risks
2. Ability to identify and plan audits for specific ONF elements based on audit objectives and integration needs	2. Knowledge of ONF audit program requirements as defined in ISO/IEC 27034
3. Ability to recognize the responsibilities of the involved parties in the auditing of the ONF	3. Knowledge of alignment strategies between ONF audits and existing ISMS or organizational audit frameworks
4. Ability to evaluate audit outcomes including root causes, implemented solutions, and audit process improvements	4. Knowledge of responsibilities and accountability models, such as RACI charts, and their role in verifying ONF effectiveness
5. Ability to assess and apply relevant security controls by considering organizational, technical, environmental, and regulatory factors, ensuring effective and context-appropriate information system protection	5. Knowledge of the role of ONF and ANF in supporting application audit activities
6. Ability to distinguish between techniques for conducting detailed application risk analysis	6. Knowledge of audit evidence required to confirm application security compliance
	7. Knowledge of application security controls (ASCs) and their purpose
	8. Knowledge of ASMP audit components, including trust verification and feedback mechanisms

Domain 5: Conducting an application security audit

Main objective: Ensure that the candidate is able to conduct an application security audit.

Competencies	Knowledge statements
1. Ability to organize and conduct an opening meeting	1. Knowledge of the purpose and required components of an opening meeting
2. Ability to assign responsibilities for specific areas, taking into consideration the auditor's impartiality, objectivity, competence, and resource efficiency	2. Knowledge of the responsibilities of each audit team member, including guides and observers
3. Ability to solve and handle conflicts within the audit team and auditee	3. Knowledge of effective communication practices during an audit, including the role of regular team meetings, issue prioritization, inclusive discussion, and conflict resolution
4. Ability to engage with the managers and ONF committee regarding crucial aspects of ASCs and their implementation within the organization	4. Knowledge of evidence collection and verification procedures in application security audits
5. Ability to collect and verify audit evidence through appropriate sampling techniques	5. Knowledge of drafting audit conclusions based on verified evidence, audit criteria, and discussions
6. Ability to plan the agenda and effectively lead a closing meeting	6. Knowledge of the purpose and required components of a closing meeting
7. Ability to prepare and distribute a professional audit report	7. Knowledge of the required structure and content of an audit report, including all key elements
8. Ability to generate audit findings by comparing the audit evidence against the audit criteria, clearly documenting conformity or nonconformities	8. Knowledge of the principles and practices for determining, categorizing, and recording audit findings, including the evaluation of objective evidence, conformity and nonconformity documentation, follow-up on previous audits, and handling findings related to multiple audit criteria

Domain 6: Audit closure and follow-up for application security

Main objective: Ensure that the candidate is able to conclude an application security audit and conduct audit follow-up activities.

Competencies	Knowledge statements
1. Ability to conclude the audit in alignment with the audit plan or documented client agreement 2. Ability to ensure confidentiality and appropriate distribution of audit reports and audit findings 3. Ability to compile and deliver clear, accurate, and complete audit reports 4. Ability to identify lessons learned and communicate audit risks, opportunities, and follow-up needs 5. Ability to evaluate action plans, verify the status and effectiveness of corrective actions, and ensure that improvement objectives are realistic and tailored to the auditee's specific context 6. Ability to conduct follow-up audits by reviewing action plans, verifying the implementation and effectiveness of corrective measures, and determining the adequacy of responses to prior audit findings 7. Ability to document and retain evidence such as audit plans, findings, nonconformities, corrective actions, and follow-up reports 8. Ability to define, implement, and oversee archival processes that ensure long-term accessibility, integrity, and proper disposal of audit records	1. Knowledge of audit completion criteria and procedures 2. Knowledge of confidentiality principle and disclosure restrictions related to audit documentation 3. Knowledge of audit program documentation requirements, including audit plans, reports, evidence, and follow-up actions 4. Knowledge of required elements of a compliant audit report, including audit scope, audit findings, and audit conclusions 5. Knowledge of audit follow-up processes, including verification of corrective actions and status reporting 6. Knowledge of assessing the effectiveness of actions taken by the auditee and closing a nonconformity 7. Knowledge of data retention, record access, archival control, and disposal practices defined by ASLCRM

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	15	18.75	X	
	Application security audit concepts and principles	10	12.5	X	
	Initiating an application security audit	17	21.25		X
	Preparing an application security audit	15	18.75	X	
	Conducting an application security audit	15	18.75		X
	Audit closure and follow-up for application security	8	10		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:

- Hard copies of the ISO/IEC 27034 family of 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

SecureApp Innovations, a technology company, has recently developed a new customer relationship management (CRM) application to enhance customer interactions and streamline business operations. To ensure the security and regulatory compliance of the application, *SecureApp Innovations* implemented an application security management process (ASMP) based on ISO/IEC 27034.

During the development phase, *SecureApp Innovations* conducted a risk assessment to identify potential threats, including software flaws, user errors, and weak access controls. This assessment was crucial for understanding the business, regulatory, and technological contexts in which the CRM application would operate. By incorporating these contextual elements, *SecureApp Innovations* was able to identify and specify complete and measurable application security requirements that address risks to the confidentiality, integrity, and availability of the application's data.

To align the CRM application's security practices with industry standards, *SecureApp Innovations* established a tailored application normative framework (ANF) for the CRM system's security requirements. The ONF Committee, responsible for the overall application security management, played a key role in overseeing the ASMP's implementation. The committee was responsible for integrating security measures across the entire CRM application life cycle. The application owner was responsible for ensuring that the ASMP was applied correctly, and the project manager was responsible for its implementation during the development phase.

After identifying the risks, the company proceeded with the risk analysis process. Each identified risk was evaluated based on its potential impact on the security of the CRM application. The risks were then categorized as low, medium, or high to determine the mitigation priority. This structured approach helped *SecureApp Innovations* allocate its resources to address the highest-priority risks first and reduce the most critical ones.

To ensure that the CRM application complied with all applicable laws, *SecureApp Innovations* maintained a comprehensive documented inventory of those laws. This inventory covered the jurisdictions in which the application would be deployed to ensure that all associated business activities met legal requirements. The inventory helped mitigate the risk of noncompliance during the development and deployment phases.

Throughout the development process, *SecureApp Innovations* conducted regular audits to verify that security controls were being followed and to evaluate how security incidents were managed. After each audit, the company identified and implemented corrective actions. The company also conducted follow-up audits to verify the effectiveness of these corrective actions, ensuring continuous improvement in the security posture of the CRM application.

Based on this scenario, answer the following questions.

1. **Did *SecureApp Innovations* take the correct approach to application security requirements engineering?**
   A. No, because the company failed to conduct a formal analysis to identify the security needs.
   B. **Yes, because the company analyzed its operational context and potential risks to define appropriate safeguards.**
   C. Yes, but the company relied exclusively on predefined technical controls instead of assessing specific risks.

2. **Did *SecureApp Innovations* ensure the proper implementation of the ASMP for the CRM application?**
   A. **Yes, the ONF Committee oversaw the ASMP, and the application owner and project manager fulfilled their roles in applying it.**
   B. No, the application owner was not involved in ensuring that the ASMP was applied to the project.
   C. No, only the project manager is responsible for applying the ASMP, with no oversight from the ONF Committee.

3. **Which ONF component is addressed in the fifth paragraph of the scenario?**
   A. Application specifications repository
   B. Operational processes
   C. **Regulatory context**

4. **According to the scenario, which step of the application security risk assessment process did *SecureApp Innovations* perform when categorizing risks?**
   A. Risk analysis
   B. **Risk evaluation**
   C. Risk identification

5. **Based on the last paragraph of the scenario, which of the following best describes the structured approach that *SecureApp Innovations* used to audit and improve the CRM application?**
   A. Security testing life cycle
   B. **A typical audit life cycle**
   C. Incident response process

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 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	Application security audit experience	Other requirements
PECB Certified ISO/IEC 27034 Provisional Application Security Auditor	PECB Certified ISO/IEC 27034 Lead Application Security Auditor exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27034 Application Security Auditor		Two years: One year of work experience in application security	Audit activities: a total of 200 hours	
PECB Certified ISO/IEC 27034 Lead Application Security Auditor		Five years: Two years of work experience in application security	Audit activities: a total of 300 hours	
PECB Certified ISO/IEC 27034 Senior Lead Application Security Auditor		Ten years: Seven years of work experience in application security	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 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 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/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

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 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[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