



PECB

Candidate Handbook

LEAD SOC 2
MANAGER

Contents

SECTION I: INTRODUCTION.....	3
About PECB	3
Accreditations and Affiliations	3
PECB Code of Ethics.....	3
Introduction to SOC 2 Lead Manager Certification	4
SECTION II: EXAM PROCESS, RULES AND POLICIES	5
Preparing For and Scheduling the Exam.....	5
Special Accommodations.....	5
Taking the Exam.....	5
Exam Results.....	6
Exam Retake Policy.....	6
Exam Security Policy	6
Exam Competency Domains	7
Sample Exam Questions.....	13
SECTION III: CERTIFICATION PROCESS, RULES AND POLICIES	15
PECB SOC 2 Credentials	15
Applying for Certification	15
Professional Experience	16
Professional References	16
Project Experience	16
Evaluation of Certification Applications.....	16
SECTION IV: CERTIFICATION MAINTENANCE POLICY	17
Renewing the Certification	17
Upgrade Credentials	17
Suspension of Certification	17
Revocation of Certification	17
Other Statuses	17
SECTION V: OTHER POLICIES	18
Application Fees for Examination and Certification	18
Complaint and Appeal Policy	18
Exams from Other Accredited Certification Bodies.....	18
Refund Policy	18

SECTION I: INTRODUCTION

About PECB¹

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.

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 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

Accreditations and Affiliations

At PECB, we are driven and culturally powered by a systemic process of continual improvement and professional development. As a testament to our high standards and commitment to providing quality services to our clients, PECB is accredited by a number of bodies and is a member of many professional organizations.

For detailed information on our accreditations and affiliations, click [here](#).

PECB Code of Ethics

The Code of Ethics is the set of values that PECB is committed to following, 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 PECB's Code of Ethics, click [here](#).

¹ Notes:

- The legal name of PECB is "PECB Group Pte. Ltd."
- 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.
- "Certified" refers to ISO/IEC 17024 certifications' requirements and "Certificate holder" refers to ASTM E2659 certificate programs' requirements. Certificate holders are not certified, licensed, accredited, or registered to engage in a specific occupation or profession.

Introduction to SOC 2 Lead Manager Certification

This document specifies the PECB SOC 2 Lead Manager certification scheme in compliance with ISO/IEC 17024. 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 certification application.

If you have questions or need further information after reading it, please contact support@pecb.com.

SECTION II: EXAM PROCESS, RULES AND POLICIES

For detailed and most up-to-date information, you are advised to refer to the online **Exam Rules and Policies** by clicking [here](#).

Preparing For and Scheduling the Exam

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 location where the candidate is going to attend the exam.

For any changes with regard to the exam date, time, location, or other details, please contact support@pecb.com.

Special Accommodations

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations for candidates, when appropriate. If candidates need special accommodations because of special needs (dyslexia, dyspraxia, ADHD, vision impairment, but not limited to) and temporary conditions (pregnancy, surgery, postoperative recovery, but not limited to), they can apply for such arrangements through the [myPECB](#) dashboard/ Enroll for an Exam. Any information that candidates provide regarding their special needs will be treated with confidentiality.

Taking the Exam

Candidates are required to arrive/be present at least 30 minutes before the exam starts. Candidates who arrive late will not receive additional time to make up for the delay and may not be allowed to sit for the exam.

Candidates are required to bring a valid identity card (national ID card, driver's license, or passport) and show it to the invigilator.

Online Exam Rules	Paper-Based Exam Rules
- Exams are provided electronically via the PECB Exams application. - The use of secondary electronic devices, such as tablets and phones, is 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. - If requested on the day of the exam, 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	- Exams are provided on paper, where candidates are not allowed to use anything but the exam paper and a pen. - The use of electronic devices, such as laptops, tablets, or phones, is not allowed. - The exam session is supervised by a PECB approved Invigilator at the location where the Partner has organized the training course. - If requested on the day of the exam, 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

For specific information on exam types, languages available, and other details, please check the [List of PECB Exams](#).

Exam Results

Exam results will be communicated via email.

- The time span for the communication of exam results 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 disagree with the evaluation, they may request a re-evaluation of their exam results within 30 days from the date they receive their exam results. If still not satisfied, they can file an appeal through the [PECB Ticketing System](#) within 30 days from the date they receive the re-evaluation decision. Appeals received after 30 days will not be processed. For more detailed information, please refer to [Complaint and Appeal Policy](#).

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. For more information, please visit this link: [Exam Rules and Policies - PECB](#).

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 who violate such rules and policies, including permanently banning individuals from pursuing PECB credentials and revoking/invalidating any previous ones. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

Exam Competency Domains

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts of SOC 2 Framework

Main objective: Ensure that the candidate can interpret the core principles, objectives, structure, and governance model of the SOC 2 framework and its relationship with major security standards and regulations.

Competencies	Knowledge statements
1. Ability to explain the foundational concepts, terminology, and purpose of the SOC 2 framework 2. Ability to articulate the interplay between SOC 2 and key information security standards and regulatory requirements (ISO/IEC 27001, NIST CSF, GDPR, PCI DSS, CSA, CIS Controls, etc.) 3. Ability to contextualize SOC 2 within organizational governance, risk, and compliance architectures 4. Ability to explain SOC 2 objectives, report types, and the structure of SOC reporting 5. Ability to interpret how SOC 2 mapping supports alignment with other frameworks and compliance obligations	1. Knowledge of regulatory expectations, contractual obligations, industry standards, and internal policies that influence SOC 2 compliance 2. Knowledge of SOC 2 terminology, Trust Services Categories, and key reporting constructs 3. Knowledge of how SOC 2 maps to other industry frameworks such as ISO/IEC 27001, NIST CSF, and NIST SP 800-53 4. Knowledge of common SOC reporting mechanisms 5. Knowledge of SOC 2 objectives and the intended use of SOC 2 reports for customers and stakeholders 6. Knowledge of the compliance impact and assurance value of SOC 2 within cloud and service provider environments 7. Knowledge of SOC 2 background, including the origin, applicability, and role of the AICPA in defining the framework

Domain 2: SOC 2 criteria

Main objective: Ensure that the candidate can identify, interpret, and analyze the Trust Services Criteria (TSC), their points of focus, and their operational implications.

Competencies	Knowledge statements
1. Ability to explain the structure, components, and intent of the Trust Services Criteria 2. Ability to interpret, analyze, and apply the TSC across security, availability, processing integrity, confidentiality, and privacy 3. Ability to evaluate and tailor SOC 2 controls to align with organizational processes and risk posture 4. Ability to support the development, operation, review, improvement, and governance of SOC 2 control environments 5. Ability to analyze the relationship between the TSC and COSO principles and components 6. Ability to interpret and apply supplemental and additional criteria associated with each Trust Services Category	1. Knowledge of the TSC Common Criteria and specific criteria for each Trust Services Category 2. Knowledge of points of focus and their role in guiding control design and evaluation 3. Knowledge of the key steps needed to establish SOC 2 control objectives, control activities, and supporting documentation 4. Knowledge of continual-improvement concepts and how they apply to a dynamic SOC 2 control environment 5. Knowledge of risk-driven control scoping and alignment techniques 6. Knowledge of integration opportunities between SOC 2 controls and broader organizational security frameworks 7. Knowledge of the 2017 TSC structure and its alignment with COSO principles 8. Knowledge of supplemental criteria, including logical and physical access controls, system operations, change management, and risk mitigation 9. Knowledge of additional criteria for availability, confidentiality, processing integrity, and privacy

Domain 3: Planning of SOC 2 requirements implementation

Main objective: Ensure the candidate can plan the implementation of SOC 2 controls and compliance activities.

Competencies	Knowledge statements
1. Ability to collect, analyze, and interpret the information required to plan a SOC 2 compliance program	1. Knowledge of project management principles, terminology, and best practices relevant to SOC 2 deployment
2. Ability to define SOC 2 objectives, control priorities, and stakeholder expectations	2. Knowledge of common SOC 2 implementation methodologies and approaches
3. Ability to identify SOC 2-relevant risks and assess their operational impact	3. Knowledge of typical SOC 2 objectives and the methods used to achieve them
4. Ability to analyze the internal and external environment to inform SOC 2 scoping decisions	4. Knowledge of organizational context factors and their impact on SOC 2 scope
5. Ability to identify key processes, activities, and interested parties relevant to SOC 2 requirements	5. Knowledge of techniques for gathering information and performing SOC 2 self-assessments and gap analyses
6. Ability to determine the resource, budget, and capability requirements for SOC 2 implementation	6. Knowledge of data gathering and analysis techniques used in SOC 2 gap assessments
7. Ability to define stakeholder roles and responsibilities across the SOC 2 lifecycle	7. Knowledge of SOC 2 project-plan structures, deliverables, and team operating models
8. Ability to draft and maintain a SOC 2 implementation roadmap	8. Knowledge of resource allocation for SOC 2 programs
9. Ability to perform gap analyses and establish maturity targets	9. Knowledge of organizational models supporting SOC 2 governance
10. Ability to define and justify an appropriate SOC 2 scope based on services, systems, boundaries, and requirements	10. Knowledge of scope definition processes and boundaries for SOC 2 systems
11. Ability to develop SOC 2-aligned policies and supporting governance artifacts	11. Knowledge of best practices for developing SOC 2 policies, standards, and procedures
12. Ability to execute and document risk assessment activities aligned with SOC 2 expectations	12. Knowledge of risk assessment methodologies aligned with SOC 2 expectations
13. Ability to account for third-party and vendor-related SOC 2 requirements in planning activities	13. Knowledge of SOC 2 third-party requirements and how vendor dependencies influence compliance planning

Domain 4: Implementation of SOC 2 requirements

Main objective: Ensure that the candidate can implement SOC 2 controls and operational processes required for SOC 2 readiness and certification.

Competencies	Knowledge statements
1. Ability to identify, analyze, and evaluate control-related risks and opportunities 2. Ability to support organizational capacity-building to enable effective SOC 2 control execution 3. Ability to operationalize SOC 2 controls and properly document their design and execution 4. Ability to manage organizational knowledge relevant to SOC 2 operations 5. Ability to design and implement SOC 2-aligned training, awareness, and communication programs 6. Ability to create communication channels that support control adoption, readiness, and alignment across stakeholders 7. Ability to implement supplemental and additional TSC criteria, including logical and physical access, system operations, change management, and risk mitigation 8. Ability to implement security incident management, business continuity, and disaster-recovery practices aligned with SOC 2 expectations 9. Ability to evaluate competence needs and support ongoing competence development related to SOC 2 control execution	1. Knowledge of processes used to identify, analyze, and evaluate SOC 2-related risks and opportunities 2. Knowledge of best practices for delivering SOC 2-specific training and awareness programs 3. Knowledge of communication mechanisms that drive stakeholder alignment, engagement, and readiness 4. Knowledge of the implementation of TSC control categories: security, availability, processing integrity, confidentiality, and privacy 5. Knowledge of the implementation of COSO-aligned criteria: control environment, information and communication, risk assessment, monitoring activities, and control activities 6. Knowledge of supplemental criteria implementation, including logical/physical access, system operations, change management, and risk mitigation 7. Knowledge of additional criteria for availability, processing integrity, confidentiality, and privacy 8. Knowledge of security incident management, incident monitoring, documentation, and reporting requirements 9. Knowledge of business continuity and disaster recovery implementation practices 10. Knowledge of competence development, awareness sessions, and training-outcome evaluation methods

Domain 5: Monitoring of security measures and preparing for SOC 2 certification audit

Main objective: Ensure that the candidate can evaluate, monitor, and measure the performance of SOC 2 controls and support end-to-end audit readiness.

Competencies	Knowledge statements
1. Ability to monitor and evaluate the effectiveness of SOC 2 controls and security measures 2. Ability to verify the achievement of SOC 2 objectives and control outcomes 3. Ability to support internal readiness assessments and ongoing compliance reviews 4. Ability to conduct recurring evaluations to validate suitability, adequacy, and effectiveness of SOC 2 controls 5. Ability to facilitate management review activities to ensure continued alignment 6. Ability to support corrective and improvement actions based on audit findings 7. Ability to establish measurement objectives, performance indicators, and reporting mechanisms relevant to SOC 2 compliance 8. Ability to track change factors and ensure continual updates to SOC 2 documentation and improvements	1. Knowledge of techniques and best practices for monitoring and evaluating SOC 2 control effectiveness 2. Knowledge of performance-measurement concepts, methods, metrics, and KPIs relevant to SOC 2 3. Knowledge of internal audit and readiness-assessment processes aligned with SOC 2 expectations 4. Knowledge of major vs. minor nonconformities and their operational impact 5. Knowledge of guidelines and templates for documenting audit findings and nonconformity reports 6. Knowledge of management-review processes and ongoing improvement methodologies 7. Knowledge of how to set measurement objectives and establish performance indicators for SOC 2 monitoring 8. Knowledge of continual monitoring of change factors and how they influence SOC 2 maintenance activities 9. Knowledge of continual improvement practices, including documentation of improvements and updates to SOC 2 evidence

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 the SOC 2 Framework	11	13.75	X	
	SOC 2 criteria (Trust Services Criteria)	12	15	X	
	Planning the implementation of SOC 2 requirements	25	31.25		X
	Implementation of SOC 2 requirements	22	27.5	X	
	Monitoring of security measures and preparing for the SOC 2 certification audit	10	12.5		X
Total		80	100%		
Number of questions per level of understanding				45	35
% of the exam devoted to each level of understanding (cognitive/taxonomy)				56.25%	43.75%

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

This exam comprises multiple-choice questions: The multiple-choice exam can be used to evaluate candidates' understanding of 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-dependent, whereas scenario-based questions are context-dependent, i.e., they are developed based on a scenario that 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 copy of the main standard (accessed through the PECB Exams app and/or printed)
- 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 sample of exam questions will be provided below.

Sample Exam Questions

CloudStrideSol, headquartered in Austin, Texas, delivers a cloud-based workforce analytics platform to customers across multiple regions. As the client base grew and security expectations intensified, the organization launched a SOC 2 readiness program to reinforce the reliability and protection of its operational environment.

During an early-stage assessment, Emma, the SOC 2 manager, identified that sensitive system dashboards lacked strong access restrictions, data in transit between internal applications was not consistently protected, and monitoring coverage did not adequately capture suspicious activity. These weaknesses created exposure to unauthorized access attempts and increased the likelihood of data misuse. To address these gaps, leadership introduced targeted safeguards to restrict access to authorized individuals, secure data transmission, and enhance detection of anomalous events across the environment.

As the program advanced, the compliance team, supported by Emma, recognized that unclear system boundaries and inconsistencies across business units were creating challenges in defining what fell under the SOC 2 evaluation. To streamline the process, they conducted a structured review of operational processes, system components, and data flows to determine which applications, environments, and services would be included. This exercise allowed the organization to outline clear boundaries, identify critical systems, and ensure that all stakeholders were aligned on the specific elements subject to SOC 2 oversight.

The expansion of *CloudStrideSol*'s analytics platform introduced new concerns regarding the exposure of sensitive information during development and operational activities. Engineers were regularly accessing production-level datasets that exposed unnecessary sensitive fields. Internal reviews further revealed inconsistent identity verification and limited logging of access attempts. To mitigate these exposure points, Emma coordinated efforts to obscure sensitive fields within non-production data, reinforce authentication requirements for administrative access, and strengthen monitoring of access activity.

CloudStrideSol expanded its SOC 2 risk assessment by reviewing events that recently disrupted operations. A severe storm caused outages at the secondary data center, exposing weaknesses in environmental resilience. Shortly after, an internal administrator misconfigured access settings, unintentionally exposing a non-critical tool to the public. These incidents prompted the security team to classify the underlying threat sources and reinforce associated risk-mitigation strategies.

In the documentation phase, Emma worked with the compliance team to create a structured record of the organization's controls. Each control was linked to the relevant Trust Services Criteria, assigned a unique identifier, and accompanied by a clear description of its purpose and the individual responsible for operating it. This catalog served as the foundation for ongoing evaluation and governance of *CloudStrideSol*'s SOC 2 control environment.

Based on the scenario above, answer the following question.

1. Which Trust Services Criteria category did *CloudStrideSol* primarily strengthen through the safeguards introduced?
 - A. **Security**
 - B. Availability
 - C. Processing Integrity

2. Which implementation activity did *CloudStrideSol* complete during this phase of the SOC 2 initiative?
 - A. **Scope assessment**
 - B. Training and awareness
 - C. Readiness assessment
3. Which measure did *CloudStrideSol* apply to reduce unnecessary exposure of sensitive information within its engineering workflows?
 - A. Physical security controls
 - B. **Data masking and anonymization**
 - C. Audit logging
4. Which threat source category covers the incident that resulted in outages at the secondary data center?
 - a. Unintentional acts
 - b. Vendors and business partners
 - c. **Environmental events**
5. Which SOC 2 compliance document did *CloudStrideSol* focus on when cataloging controls, assigning owners, and aligning each activity with the Trust Services Criteria?
 - A. Management assertion
 - B. System description
 - C. **Control matrix**

SECTION III: CERTIFICATION PROCESS, RULES AND POLICIES

PECB SOC 2 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 SOC 2 scheme have the following requirements:

Credential	Exam	Professional experience	MS project experience	Other requirements
PECB Certified SOC 2 Provisional Manager	PECB Certified Lead SOC 2 Manager	None	None	Signing the PECB Code of Ethics
PECB Certified SOC 2 Manager		Two years: One year of work experience in information security	Project activities: a total of 200 hours	
PECB Certified Lead SOC 2 Manager		Five years: Two years of work experience in information security	Project activities: a total of 300 hours	
PECB Certified Senior Lead SOC 2 Manager		Ten years: Seven years of work experience in information 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. Conducting a gap analysis on a SOC 2 program
2. Developing an information security policy
3. Assessing and treating information security risks
4. Implementing SOC 2 controls
5. Measuring and reporting SOC 2 performance metrics

For detailed and most up-to-date information, you are advised to refer to the online **Certification Process** by clicking [here](#).

Applying for Certification

All participants who successfully pass their certification exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credentials they were examined for. Specific professional requirements will need to be fulfilled to be PECB certified.

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

- [Create](#) your account
- Check your email for the confirmation link
- [Log in](#) and click on Apply for Certificate

The approval of the application occurs when the Certification Department validates that you fulfil all the certification requirements regarding the credential you have applied for. An email will be sent to the address you provided during your application to update you on your application status. If approved, you will then be able to download your certificate and digital badge from your member account.

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.

Project Experience

The candidate's 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.

PECB can deny certification/certificate program if candidates:

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

If applicants have any concerns regarding the denial of certification/certificate program, they may file an appeal by following the complaint and appeal process [Complaint and Appeal Policy](#).

The application payment for the certification/certificate program is nonrefundable. This is due to the application verification process, the evidence submitted by the candidates, and the involvement of the relevant departments.

If candidates pass the exam, they can apply for the certificate within 12 months from the course completion date for instructor-led training, or within 12 months from the purchase date for self-study and eLearning formats. 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.

SECTION IV: CERTIFICATION MAINTENANCE POLICY

For detailed and most up-to-date information, you are advised to refer to the online **Certification Maintenance Policy** by clicking [here](#).

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 continuing professional development (CPD) hours. In addition, they need to pay the annual maintenance fee.

Upgrade Credentials

PECB Certifications can be upgraded online through your dashboard by logging in [here](#), clicking **View Certificate**, and then clicking the **Upgrade** button. For more information on the upgrade requirements and fees, go to the [Certification Maintenance](#) page on the PECB website.

Suspension of Certification

Failure to submit the CPD and AMF payment during the certification cycle will result in a 12-month suspension period, during which you can address any outstanding AMFs and CPDs. In addition to these, the certification may be suspended for other reasons listed in the **Certification Maintenance Policy**. Individuals whose certification has been suspended are not authorized to further promote their certification while it is suspended.

Suspended members must remediate their suspension within a maximum period of 12 months.

Revocation of Certification

PECB can revoke (that is, withdraw) certification if the candidate fails to address the outstanding AMFs and CPDs during the 12-month suspension period. In addition to these, certification may be revoked for other reasons listed in the **Certification Maintenance Policy**. Individuals whose certification has been revoked are not authorized to use any references to a certified status.

If candidates disagree with any certification decision (certification level, suspension, or revocation) they may request a re-evaluation within 30 days from the date they receive their certification decision. If still not satisfied, they can file an appeal through the [PECB Ticketing System](#) within 30 days from the date they receive the re-evaluation decision. Appeals received after 30 days will not be processed. For more detailed information, please refer to [Complaint and Appeal Policy](#).

Other Statuses

Besides being active, suspended, or revoked, a certification can be voluntary withdrawn, or designated as Emeritus. For more information, go to the [Certification Maintenance](#) page on the PECB website.

SECTION V: OTHER POLICIES

Application Fees for Examination and Certification

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

- Lead Exam: \$1000²
- Manager Exam: \$700
- Foundation Exam: \$500
- Transition Exam: \$500

The application fee for certification is as follows:

- Master Certification: \$100
- Foundation Certification: \$200
- Transition Certification: \$200
- All other Certifications: \$500

For candidates who complete a training, eLearning, or self-study course delivered by a PECB Partner, the training fee includes the first exam attempt, one free retake, the certification application fee, and the first year of the Annual Maintenance Fee (AMF). This cycle must be completed within 12 months from the course completion date for instructor-led training, or within 12 months from the purchase date for self-study and eLearning formats.

Complaint and Appeal Policy

A person wishing to file a complaint or an appeal can do so by submitting a [service ticket](#) and selecting the corresponding category in the topic dropdown menu: “file a complaint” or “file a certification/certificate program appeal”. Before filing a complaint or an appeal, make sure to follow the [complaint and appeal policy](#).

Exams from Other Accredited Certification Bodies

PECB accepts exams from other recognized accredited certification bodies. PECB will evaluate the requests through its equivalence process to decide whether the respective exam(s) can be accepted as equivalent to the respective PECB certification.

Refund Policy

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

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



Contact PECB Support at
support@pecb.com



Telephone number
+1-844-426-7322



Visit our [Help Center](#) to access manuals, FAQs, and quick guides, or reach us directly via Live Chat or by submitting a ticket [here](#).

Follow us on:



www.pecb.com