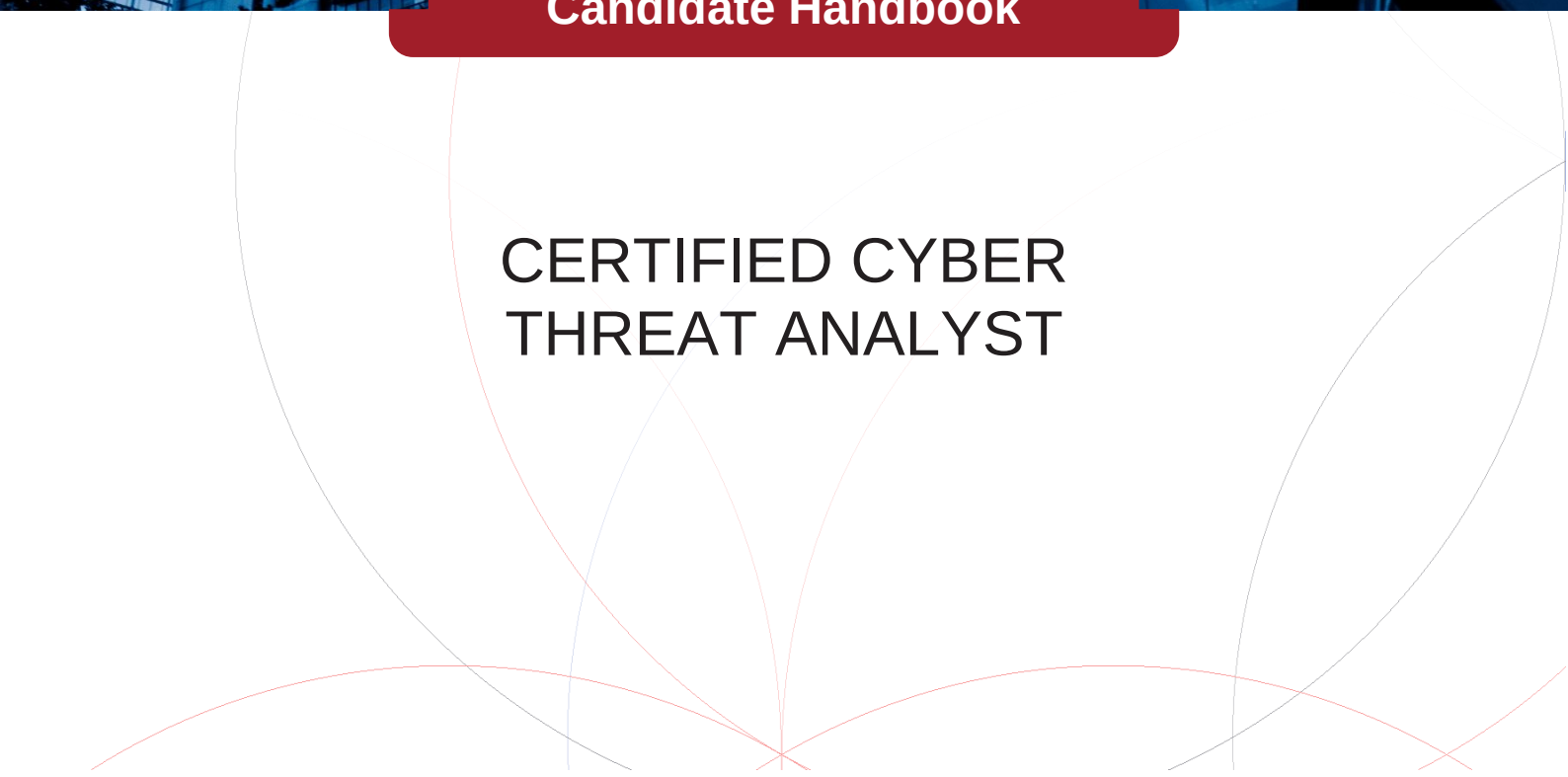




PECB

Candidate Handbook

**CERTIFIED CYBER
THREAT ANALYST**



Contents

SECTION I: INTRODUCTION.....	3
About PECB	3
Accreditations and Affiliations	3
PECB Code of Ethics	3
Introduction to Certified Cyber Threat Analyst 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 Certified Cyber Threat Analyst Credentials	15
Applying for Certification	15
Professional Experience	15
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 Certified Cyber Threat Analyst Certification

This document specifies the PECB Certified Cyber Threat Analyst 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: Threat intelligence and malware analysis

Main objective: Ensure that the candidate is able to interpret cyber threat intelligence, apply threat hunting frameworks and maturity models, and analyze malware and adversary indicators to support proactive threat hunting activities.

Competencies	Knowledge statements
1. Ability to explain the fundamental concepts of information security, including the confidentiality, integrity, and availability triad	1. Knowledge of the core principles of information security, including confidentiality, integrity, and availability
2. Ability to distinguish between a vulnerability, a threat, and a risk	2. Knowledge of the difference between a vulnerability, a threat, and a risk
3. Ability to identify common cyber threats and social engineering techniques	3. Knowledge of common cyber threats, malware types, and social engineering attack techniques
4. Ability to apply the Diamond Model of Intrusion Analysis to examine adversary activity	4. Knowledge of the Diamond Model of Intrusion Analysis and its core features
5. Ability to differentiate between indicators of compromise (IoCs) and indicators of attack (IoAs)	5. Knowledge of indicators of compromise (IoCs) and indicators of attack (IoAs) and their relative persistence
6. Ability to apply the Hunting Maturity Model (HMM) to assess an organization's threat hunting capability	6. Knowledge of the levels and characteristics of the Hunting Maturity Model (HMM)
7. Ability to apply the Sqrri threat hunting framework to structure a threat hunt	7. Knowledge of the stages of the Sqrri threat hunting framework
8. Ability to define the scope and boundaries of a threat hunting engagement	8. Knowledge of the elements involved in defining the scope of a threat hunt
9. Ability to classify types of malware and forms of cyber threat intelligence	9. Knowledge of qualitative, quantitative, and semi-quantitative risk analysis techniques
10. Ability to use threat intelligence platforms and tools to collect, correlate, and share indicators	10. Knowledge of threat intelligence platforms and tools such as MISP and VirusTotal

Domain 2: Network forensics

Main objective: Ensure that the candidate is able to identify and explain the network forensics tools, data sources, and analytical techniques used to investigate suspicious network activity and support the threat hunting process.

Competencies	Knowledge statements
1. Ability to explain the role of network forensics within the threat hunting process	1. Knowledge of the activities involved in assembling tools and data for an investigation plan
2. Ability to assemble the tools and data sources required for a network-based investigation	2. Knowledge of the elements of the data analysis phase, including correlation and root cause analysis
3. Ability to formulate, prioritize, and validate threat hunting hypotheses	3. Knowledge of the reporting requirements for communicating findings to varied stakeholders
4. Ability to apply behavioral analysis techniques to detect anomalous network activity	4. Knowledge of the communication channels used to share threat hunting findings with stakeholders
5. Ability to use packet capture and analysis tools to examine network traffic	5. Knowledge of behavioral analysis as a threat detection method
6. Ability to distinguish between the common types of security logs	6. Knowledge of network forensics tools such as Zeek, Suricata, and Wireshark
7. Ability to apply log parsing and normalization techniques across heterogeneous data sources	7. Knowledge of intrusion detection and prevention system capabilities
8. Ability to use SIEM platforms and correlation engines to identify security events	8. Knowledge of common log types and log data formats, including JSON
9. Ability to communicate threat hunting findings to technical and nontechnical stakeholders	9. Knowledge of the stages of the log management process, including parsing and normalization
10. Ability to develop detection signatures and rules following a threat hunt	10. Knowledge of SIEM capabilities, including security information management and security event management

Domain 3: Endpoint forensics

Main objective: Ensure that the candidate is able to identify and explain the endpoint forensics techniques and data preservation practices used to investigate suspicious host-level activity and support threat hunting and incident response.

Competencies	Knowledge statements
1. Ability to explain the objectives and process of endpoint forensics	1. Knowledge of the types of logs reviewed during an endpoint forensic investigation
2. Ability to review audit, system, and application logs to reconstruct user and system activity	2. Knowledge of the data preservation practices required to support reliable analysis
3. Ability to identify process execution metadata relevant to an endpoint investigation	3. Knowledge of adversary tactics, including collection, discovery, and exfiltration
4. Ability to apply data preservation practices to maintain the integrity of collected evidence	4. Knowledge of the common causes of insider threats
5. Ability to maintain chain of custody documentation throughout an investigation	5. Knowledge of threats arising from identity theft and credential misuse
6. Ability to recognize adversary tactics, such as collection and exfiltration on an endpoint	6. Knowledge of the process execution metadata collected from an endpoint
7. Ability to identify indicators of insider threats and credential misuse	7. Knowledge of the information typically recorded in application logs
8. Ability to establish a baseline of normal endpoint and network behavior	8. Knowledge of the risks arising from the physical theft, damage, or loss of devices
9. Ability to assess risks arising from the loss, theft, or damage of devices	9. Knowledge of the methods used to establish a baseline of normal system behavior
10. Ability to align risk mitigation strategies with an organization's prioritized critical systems	10. Knowledge of the purpose of documentation and chain of custody for collected data

Domain 4: Privilege escalation mechanisms

Main objective: Ensure that the candidate is able to identify and explain the tactics, techniques, and mechanisms that adversaries use to escalate privileges and move within an environment and how the MITRE ATT&CK framework supports their detection.

Competencies	Knowledge statements
1. Ability to explain the structure and purpose of the MITRE ATT&CK framework	1. Knowledge of the components of the MITRE ATT&CK framework, including tactics, techniques, and procedures
2. Ability to map observed adversary activity to ATT&CK tactics and techniques	2. Knowledge of the real-world observations on which the MITRE ATT&CK knowledge base is built
3. Ability to identify execution activity performed through shell interpreters and scripts	3. Knowledge of common means through which attacks propagate
4. Ability to recognize attempts to bypass multi-factor authentication and escalate privileges	4. Knowledge of the methods used to identify vulnerabilities, including vulnerability scanning
5. Ability to identify discovery activity used by adversaries to map an environment	5. Knowledge of the actions that indicate an adversary is pursuing privilege escalation
6. Ability to distinguish normal administrative activity from suspicious privilege escalation attempts	6. Knowledge of the execution tactic and its association with shell interpreters and scripts
7. Ability to build and interpret an ATT&CK coverage map	7. Knowledge of the discovery tactic and its use in mapping an internal environment
8. Ability to reconstruct an intrusion using the cyber kill chain	8. Knowledge of the stages of the cyber kill chain
9. Ability to identify common means through which attacks propagate	9. Knowledge of the purpose and benefits of an ATT&CK coverage map
10. Ability to apply vulnerability scanning techniques to identify exploitable weaknesses	10. Knowledge of the indicators used to distinguish routine administrative activity from suspicious activity

Domain 5: Security monitoring and log analysis

Main objective: Ensure that the candidate is able to identify and explain the log sources, monitoring techniques, and network traffic analysis methods used to detect and investigate malicious activity across an organization's environment.

Competencies	Knowledge statements
1. Ability to explain the role of security monitoring in detecting malicious network activity	1. Knowledge of the network data sources used to identify externally resolved hosts, such as DNS logs
2. Ability to distinguish between internal and external threats	2. Knowledge of the tactic represented by an adversary's lateral movement between network segments
3. Ability to identify real-time and non-real-time network traffic types	3. Knowledge of the characteristics of a botnet and command-and-control infrastructure
4. Ability to differentiate between north-south and east-west network traffic	4. Knowledge of phishing, spam, and other threats delivered through electronic messages
5. Ability to analyze DNS logs to identify hosts contacted by compromised systems	5. Knowledge of information leakage resulting from insecure application configurations
6. Ability to recognize indicators of botnet activity and command-and-control communications	6. Knowledge of the situations that represent internal versus external threats
7. Ability to identify phishing, spam, and web-based attack techniques	7. Knowledge of real-time traffic types, such as voice over internet protocol
8. Ability to use deep packet inspection to identify malware communication and data exfiltration	8. Knowledge of the distinction between north-south and east-west network traffic
9. Ability to recognize information leakage resulting from application misconfigurations	9. Knowledge of what deep packet inspection with tools such as Wireshark can help identify
10. Ability to identify lateral movement activity within a monitored network	10. Knowledge of reasons adversaries use legitimate network protocols for command-and-control communications

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

		Number of questions/points per competency domain	% of the exam devoted/points to/for each competency domain	Level of understanding (Cognitive/Taxonomy) required	
				Questions that measure comprehension, application, and analysis	Questions that measure evaluation
Competency domains	Threat intelligence and malware analysis	26	32,5	X	
	Network forensics	20	25		X
	Endpoint forensics	12	15		X
	Privilege escalation mechanisms	10	12.5	X	
	Security monitoring and log analysis	12	15		X
Total		80	100%		
Number of questions per level of understanding				36	44
% of the exam devoted to each level of understanding (cognitive/taxonomy)				45%	55%

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:

- 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

NovaMeridian Logistics operates regional freight and warehousing services from a single headquarters in Rotterdam, the Netherlands. The company employs around 600 people and relies on a small internal IT team supported by a managed security provider. After noticing unusual login attempts on its freight-tracking application, the IT manager asked the security provider's analyst, Daniela Voss, to investigate.

Daniela began by writing down what she expected to find, based on the pattern of failed logins, before running any searches in the company's log management platform. She then reviewed authentication logs, network traffic logs, and endpoint logs from the affected servers. The investigation revealed that a warehouse employee had clicked a link in an email that appeared to come from a shipping partner, which led to malware being installed on the employee's workstation. The malware had then attempted to log in to the freight-tracking application using credentials stored in the browser.

Daniela documented her findings in a short report highlighting the affected systems, the method of compromise, and recommended containment steps. She then shared the report with both the IT manager and company leadership in a brief meeting. *NovaMeridian's* IT team later updated its email filtering rules and created a new detection rule to flag similar login patterns in the future.

Based on the scenario above, answer the following questions.

1. **Before running any searches in the log management platform, Daniela documented what she expected to find based on the pattern of failed logins. Which stage of the threat hunting process does this describe?**
 - A. Investigating using tools and techniques
 - B. **Creating a hypothesis**
 - C. Informing and enriching analytics
2. **A warehouse employee clicked a link in an email that appeared to come from a shipping partner, which led to malware being installed on the workstation. Which threat does this email represent?**
 - A. Spam
 - B. Identity theft
 - C. **Phishing**
3. **Daniela reviewed authentication logs, network traffic logs, and endpoint logs from the affected servers to reconstruct the incident. Which activity of the threat hunting process does this represent?**
 - A. Scoping the hunt
 - B. **Data collection and analysis**
 - C. Reporting the findings
4. **Daniela shared a short report highlighting the affected systems, method of compromise, and recommended containment steps with the IT manager and company leadership in a brief meeting. Which reporting practice does this reflect?**
 - A. **Communicating findings clearly to both technical and nontechnical stakeholders**
 - B. Preserving the chain of custody for collected evidence
 - C. Defining the scope of the investigation

5. After the hunt concluded, *NovaMeridian's* IT team created a new detection rule to flag similar login patterns in the future. Which stage of the threat hunting process does this action represent?
- A. Creating a hypothesis
 - B. Investigating using tools and techniques
 - C. **Informing and enriching analytics**

SECTION III: CERTIFICATION PROCESS, RULES AND POLICIES

PECB Certified Cyber Threat Analyst 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 Certified Cyber Threat Analyst scheme have the following requirements:

Credential	Exam	Professional experience	Project experience	Other requirements
PECB Certified Provisional Cyber Threat Analyst	PECB Certified Cyber Threat Analyst exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified Cyber Threat Analyst		Five years: two years of work experience in threat hunting, threat analysis, and cybersecurity	Project activities: a total of 300 hours	

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

1. Identifying and analyzing indicators of compromise (IoCs)
2. Investigating suspicious network traffic and system behavior
3. Collaborating with threat intelligence teams to refine hunting techniques
4. Developing and refining detection rules based on hunt findings
5. Documenting hunt results and sharing them with relevant teams
6. Automating detection processes to prevent repetitive threats
7. Reviewing and enhancing the threat-hunting framework regularly

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