PECB BEYOND RECOGNITION

Candidate Handbook

ISO/IEC 27032
LEAD CYBERSECURITY MANAGER

PECB

Table of Contents

SECTION I: INTRODUCTION

About PECB

PECB is a certification body which provides education[1] and certification in accordance with ISO/IEC 17024 for individuals on a wide range of disciplines.

We help professionals show commitment and competence by providing them with valuable evaluation and certification services against internationally recognized standards. Our mission is to provide services that inspire trust and continual improvement, demonstrate recognition, and benefit the society as a whole.

The key objectives of PECB are:

1. Establishing the minimum requirements necessary to certify professionals
2. Reviewing and verifying the qualifications of applicants to ensure they are eligible to apply for certification
3. Developing and maintaining reliable certification evaluations
4. Granting certifications to qualified candidates, maintaining records, and publishing a directory of the holders of a valid certification
5. Establishing requirements for the periodic renewal of certification and ensuring compliance with those requirements
6. Ensuring that candidates meet ethical standards in their professional practice
7. Representing its members, where appropriate, in matters of common interest
8. Promoting the benefits of certification to organizations, employers, public officials, practitioners in related fields, and the public

[1] Education refers to training courses developed by PECB that are offered globally through our network of partners.

The Value of PECB Certification

Why Choose PECB as Your Certification Body?

Global Recognition

Our certifications are internationally recognized and accredited by the International Accreditation Service (IAS); signatory of IAF Multilateral Recognition Arrangement (MLA) which ensures mutual recognition of accredited certification between signatories to the MLA and acceptance of accredited certification in many markets. Therefore, professionals who pursue a PECB certification credential will benefit from PECB's recognition in domestic and international markets.

Competent Personnel

The core team of PECB consists of competent individuals who have relevant sector-specific experience. All of our employees hold professional credentials and are constantly trained to provide more than satisfactory services to our clients.

Compliance with Standards

Our certifications are a demonstration of compliance with ISO/IEC 17024. They ensure that the standard requirements have been fulfilled and validated with the adequate consistency, professionalism, and impartiality.

Customer Service

We are a customer-centered company and we treat all our customers with value, importance, professionalism, and honesty. PECB has a team of experts dedicated to support customer requests, problems, concerns, needs, and opinions. We do our best to maintain a 24-hours maximum response time without compromising the quality of the service.

PECB Code of Ethics

PECB professionals will:

1. Conduct themselves professionally, with honesty, accuracy, fairness, responsibility, and independence
2. Act at all times solely in the best interest of their employer, their clients, the public, and the profession, by adhering to the professional standards and applicable techniques while offering professional services
3. Maintain competency in their respective fields and strive to constantly improve their professional capabilities
4. Offer only professional services for which they are qualified to perform, and adequately inform clients about the nature of the proposed services, including any relevant concerns or risks
5. Inform each employer or client of any business interests or affiliations that might influence their judgment or impair their fairness
6. Treat in a confidential and private manner the information acquired during professional and business dealings of any present or former employer or client
7. Comply with all laws and regulations of the jurisdictions where professional activities are conducted
8. Respect the intellectual property and contributions of others
9. Not, intentionally or otherwise, communicate false or falsified information that may compromise the integrity of the evaluation process of a candidate for a professional designation
10. Not act in any manner that could compromise the reputation of PECB or its certification programs
11. Fully cooperate on the inquiry following a claimed infringement of this Code of Ethics

The full version of the PECB Code of Ethics can be downloaded here.

Introduction to ISO/IEC 27032 Lead Cybersecurity Manager

ISO/IEC 27032 provides guidance for improving the state of cybersecurity of the organizations by helping them properly address common cybersecurity risks. ISO/IEC 27032 provides an overview of cybersecurity, and elaborates on the relationship between cybersecurity and other types of security, such as information security, network security, internet security, and critical information infrastructure protection. In addition, it provides guidance regarding the roles in cybersecurity, common cybersecurity issues, and a framework on resolving such issues.

The "ISO/IEC 27032 Lead Cybersecurity Manager" credential is a professional certification for individuals aiming to demonstrate that they possess the necessary competencies to establish and manage a cybersecurity program.

As the use of digital data has been continuously increasing, so did the number of cyberattacks. Consequently, the demand for cybersecurity professionals is on the rise, as organizations need skilled professionals to ensure protection against cyber threats. The "ISO/IEC 27032 Lead Cybersecurity Manager" is an internationally recognized certification which can help you exploit your career potential and reach your professional objectives.

It is important to note that PECB certifications are not a license or simply a membership. They represent peer recognition that an individual has demonstrated proficiency in, and comprehension of, a set of competences. PECB certifications are awarded to candidates that can demonstrate that they have the required experience and have passed a standardized exam in the certification area.

This candidate handbook specifies the PECB ISO/IEC 27032 Lead Cybersecurity Manager certification scheme in compliance with ISO/IEC 17024:2012. In addition, this document contains information about the process through which candidates may obtain and maintain their credentials. It is very important to read all the information included in this document before completing and submitting your application. If you have questions after reading it, please contact the PECB international office at certification@pecb.com.

SECTION II: PECB CERTIFICATION PROCESS AND EXAMINATION PREPARATION, RULES, AND POLICIES

Decide Which Certification Is Right for You

All PECB certifications have specific education and professional experience requirements. To determine the right credential for you, verify the eligibility criteria for various certifications and your professional needs.

Prepare and Schedule the Exam

All candidates are responsible for their own study and preparation for certification exams. No specific set of training courses or curriculum of study is required as part of the certification process. Nevertheless, attending a training course can significantly increase candidates' chances of successfully passing a PECB exam.

To schedule an exam, candidates have two options:

1. Contact one of our partners who provide training courses and exam sessions. To find a training course provider in a particular region, candidates should go to Active Partners. The PECB training course schedule is also available on Training Events.
2. Take a PECB exam remotely from their home or any location they desire through the PECB Exam application, which can be accessed here: Exam Events.

To learn more about exams, competency domains, and knowledge statements, please refer to **Section III** of this document.

Application Fees for Examination and Certification

PECB offers direct exams, where a candidate can sit for the exam without attending the training course. The applicable prices are as follows:

- Lead Exam: $1000
- Manager Exam: $700
- Foundation and Transition Exam: $500

The application fee for certification is $500.

For all candidates that have followed the training course and taken the exam with one of PECB's partners, the application fee includes the costs associated with examination, application for certification, and the first year of Annual Maintenance Fee (AMF) only.

Competency Domains

The objective of the "PECB ISO/IEC 27032 Cybersecurity Manager" exam is to ensure that the candidate has acquired the necessary expertise to support an organization in establishing and managing a cybersecurity program based on ISO/IEC 27032 and NIST Cybersecurity Framework.

The ISO/IEC 27032 Lead Cybersecurity Manager certification is intended for:

- Cybersecurity professionals
- Information security professionals
- Project managers who want to develop their competencies in cybersecurity management program
- Technical experts who deal with cybersecurity issues
- Individuals responsible for managing a cybersecurity program in an organization

The exam covers the following competency domains:

- **Domain 1:** Fundamental principles and concepts of cybersecurity
- **Domain 2:** Roles and responsibilities of stakeholders
- **Domain 3:** Cybersecurity risk management
- **Domain 4:** Attack mechanisms and cybersecurity controls
- **Domain 5:** Information sharing and coordination
- **Domain 6:** Integrating the cybersecurity program in business continuity management
- **Domain 7:** Cybersecurity incident management and performance measurement

PECB

Domain 1: Fundamental principles and concepts of cybersecurity **Main objective:** Ensure that the candidate understands and is able to interpret the principles and concepts of ISO/IEC 27032	
Competencies	**Knowledge statements**
1. Ability to understand and explain the main concepts of the ISO/IEC 27032 and NIST cybersecurity framework 2. Ability to understand, analyze, and utilize the guidance of ISO/IEC 27032 and other cybersecurity frameworks 3. Ability to understand and explain the main concepts of cybersecurity such as cyberspace, cybercrime, cybersecurity, information security 4. Ability to understand and explain the difference between information security and cybersecurity 5. Ability to categorize stakeholders in the cyberspace 6. Ability to identify assets in the cyberspace and define their life cycle 7. Ability to understand and explain the concepts of confidentiality, integrity, and availability 8. Ability to understand and explain the relationship between the concepts of vulnerability, threat, risk, and their impact 9. Ability to understand and explain the classification of security controls	1. Knowledge of ISO/IEC 27032 and NIST cybersecurity framework 2. Knowledge of the main cybersecurity frameworks 3. Knowledge of the main cybersecurity concepts and principles 4. Knowledge of the information security concepts 5. Knowledge of the role of stakeholders in the cyberspace 6. Knowledge of cyberspace assets 7. Knowledge of the concepts of confidentiality, integrity, and availability 8. Knowledge of information security vulnerabilities, threats, and risks 9. Knowledge of the difference between security controls classified by type, such as technical, legal, administrative, and managerial controls 10. Knowledge of the difference between security controls classified by function, such as preventive, corrective, and detective controls

Domain 2: Roles and responsibilities of stakeholders

Main objective: Ensure that the candidate understands and is able to interpret and explain the roles and responsibilities of stakeholders in cybersecurity

Competencies

1. Ability to assign and communicate the cybersecurity roles and responsibilities
2. Ability to explain the role of stakeholders in improving a cybersecurity program
3. Ability to understand and explain the roles and responsibilities of providers and consumers as the main stakeholders in cybersecurity
4. Ability to understand and explain the roles and responsibilities of the individuals, organizations, government, and law enforcement agencies, and their impact on cyberspace
5. Ability to understand and explain the role of information systems security program manager
6. Ability to determine the required resources for the cybersecurity program
7. Ability to understand and explain the different types of security policies
8. Ability to establish a cybersecurity policy

Knowledge statements

1. Knowledge of the cybersecurity organizational structure
2. Knowledge of the roles and responsibilities of key stakeholders and various parties, government, and law enforcement agencies and their impact on cyberspace
3. Knowledge of the roles and responsibilities of providers and consumers and their impact in cyberspace
4. Knowledge of the role of information systems security program manager
5. Knowledge of cybersecurity leadership and program approval
6. Knowledge of the resources needed for the cybersecurity program
7. Knowledge of cybersecurity policy establishment process

PECB

Domain 3: Cybersecurity risk management **Main objective:** Ensure that the candidate can implement and manage a cybersecurity risk management program	
Competencies	**Knowledge statements**
1. Ability to establish a risk management program based on ISO/IEC 27032, ISO/IEC 27005, and NIST cybersecurity framework 2. Ability to define the goals and objectives of a cybersecurity risk management program 3. Ability to identify assets, threats, existing controls, vulnerabilities, and consequences 4. Ability to assess the consequences and the likelihood of incidents 5. Ability to evaluate the levels of risk based on risk evaluation criteria 6. Ability to select and implement appropriate risk treatment options 7. Ability to evaluate and manage residual risks 8. Ability to ensure good communication and consultation between all relevant stakeholders	1. Knowledge of the concept of risk and its application in cybersecurity 2. Knowledge of the risk management frameworks 3. Knowledge of risk assessment approaches and methodologies 4. Knowledge of the risk identification process 5. Knowledge of cybersecurity assets and their importance 6. Knowledge of risk analysis process 7. Knowledge of risk evaluation process 8. Knowledge of risk treatment options and risk treatment plan 9. Knowledge of residual risk management process 10. Knowledge of the acceptable level of risk in cybersecurity 11. Knowledge of risk communication and consultation process

Domain 4: Attack mechanisms and cybersecurity controls

Main objective: Ensure that the candidate understands and is able to explain top cyber threats and their mitigation vectors, and implement key cybersecurity controls in accordance with the guidelines of ISO/IEC 27032

Competencies	Knowledge statements
1. Ability to understand and identify different types of attack mechanisms 2. Ability to identify and mitigate the attacks from inside and outside the private network 3. Ability to identify and respond to the most common types of cyberattacks such as malware, web-based and web-application attacks, phishing, denial-of-service, spam, botnets, data breaches, insider threat, theft, cryptojacking, and ransomware. 4. Ability to understand and explain the importance of the implementation of cybersecurity controls 5. Ability to implement key cybersecurity controls based on ISO/IEC 27032 such as application level controls, server protection, end-user controls, and controls against social engineering attacks	1. Knowledge of attack mechanisms such as malware, botnets, denial-of-service, phishing, spam, exploits kits, data breaches, identity theft, and ransomware. 2. Knowledge of the attacks from inside and outside the private network 3. Knowledge of application-level controls and their implementation 4. Knowledge of server protection controls and operation of secure servers 5. Knowledge of end-user controls and how they can protect the system against exploits and attacks 6. Knowledge of controls against social engineering attacks and their implementation 7. Knowledge of access control mechanisms 8. Knowledge of network monitoring and tools such as IDS and firewalls 9. Knowledge of cryptographic controls

PECB

Domain 5: Information sharing and coordination

Main objective: Ensure that the candidate is able to establish a framework for information sharing and coordination based on the ISO/IEC 27032

Competencies	Knowledge statements
1. Ability to understand and explain the importance and the benefits of a framework for information sharing and coordination in cybersecurity 2. Ability to determine and implement the required methods and processes for information sharing and coordination 3. Ability to understand and define the technical controls and standardization of information sharing and coordination 4. Ability to define and establish policies and procedures regarding information sharing and coordination 5. Ability to test and review systems periodically 6. Ability to prepare and conduct awareness and training workshops to prepare stakeholders for the establishment of an information sharing and coordination framework 7. Ability to determine competence needs and conduct training and awareness sessions 8. Ability to plan the competence development activities	1. Knowledge of an information sharing and coordination framework 2. Knowledge of techniques and best practices on writing policies, procedures, and other types of documents 3. Knowledge of the categorization and classification of information that is collected, kept safe, or distributed via information sharing and coordination framework 4. Knowledge of the development and implementation of methods and processes to ensure effectiveness, efficiency, and reliability of execution for the information sharing and coordination framework 5. Knowledge of operation of the information sharing and coordination framework 6. Knowledge of training and awareness program and their main objectives 7. Knowledge of the difference between training, awareness, and communication 8. Knowledge of evaluation methods for training programs

PECB

Domain 6: Integrating the cybersecurity program in business continuity management **Main objective:** Ensure that the candidate is able to integrate the cybersecurity program in the business continuity management plan of the organization	
Competencies	**Knowledge statements**
1. Ability to understand the role of business continuity in the context of cybersecurity 2. Ability to understand the objectives and benefits of integrating a cybersecurity program in business continuity management 3. Ability to define the principles and elements of ICT readiness for business continuity (IRBC) and determine its phases 4. Ability to define the format and structure of a cybersecurity continuity plan 5. Ability to understand and explain the concept of critical activities in the cybersecurity continuity context 6. Ability to understand and explain technical approaches for improving cybersecurity continuity	1. Knowledge of business continuity management 2. Knowledge of business continuity objectives 3. Knowledge of the benefits of integrating a cybersecurity program in business continuity management 4. Knowledge of the principles of business continuity as indicated in ISO/IEC 27031 5. Knowledge of the critical activities in cybersecurity continuity 6. Knowledge of a recovery plan and its objectives 7. Knowledge of technical approaches for improving cybersecurity continuity

PECB

Domain 7: Cybersecurity management and performance measurement

Main objective: Ensure that the candidate is able to identify and detect cybersecurity events and evaluate the effectiveness of the implemented processes and procedures within the cybersecurity program

Competencies

1. Ability to establish an incident management process based on best practices
2. Ability to reduce the possible impact of cybersecurity incidents on the operations of the organization
3. Ability to set cybersecurity incident management objectives
4. Ability to manage cybersecurity incidents by conducting several phases such as planning and preparation, detection and reporting, assessment and decision, response, and lessons learned
5. Ability to prepare and plan the operation of an effective and efficient cybersecurity incident management scheme
6. Ability to gather evidence during incidents based on a digital forensics policy
7. Ability to identify the lessons that can be learned from the occurrence of cybersecurity incidents and other incidents
8. Ability to perform testing on technical systems to ensure their reliability
9. Ability to determine the stages of testing, determine testing techniques, prepare the test and documentation, and conduct post-testing activities
10. Ability to measure the performance of the cybersecurity program, determine measurement objectives, define what needs to be monitored and measured, and establish performance indicators
11. Ability to continually improve the cybersecurity program

Knowledge statements

1. Knowledge of the principles, elements, and phases of the ICT readiness for business continuity (IRBC)
2. Knowledge of a cybersecurity incident management process
3. Knowledge of the cybersecurity incident prevention process
4. Knowledge of the ways to reduce the direct and indirect costs caused by cybersecurity incidents
5. Knowledge of the characteristics and main processes of a cybersecurity incident management scheme
6. Knowledge of the roles and responsibilities of the key actors during the implementation of a cybersecurity incident management scheme
7. Knowledge of digital forensics and their integration into cybersecurity incident response
8. Knowledge of the cybersecurity testing techniques
9. Knowledge of performance measurement methods
10. Knowledge of the monitoring, measuring, analyzing, and evaluating methods of the cybersecurity program
11. Knowledge of activities that continually improve the cybersecurity program

Based on the abovementioned domains and their relevance, 12 questions are included in the exam, as summarized in the table below:

			Level of understanding (Cognitive/Taxonomy) required					
		Points per question	Questions that measure comprehension, application, and analysis	Questions that measure evaluation	Number of questions per competency domain	% of the exam devoted to each competency domain	Number of points per competency domain	% of points per competency domain
Competency domains	Fundamental principles and concepts of cybersecurity	5	X		1	8.33	5	6.67
	Roles and responsibilities of stakeholders	5	X		1	8.33	5	6.67
	Cybersecurity risk management	5	X		2	16.67	15	20
		10		X				
	Attack mechanisms and cybersecurity controls	5	X		4	33.33	30	40
		5	X					
		10		X				
		10		X				
	Information sharing and coordination	5	X		1	8.33	5	6.67
	Integrating cybersecurity program in business continuity management	5	X		1	8.33	5	6.67
	Cybersecurity incident management and performance measurement	5		X	2	16.67	10	13.33
		5		X				
	Total points	75						
	Number of questions per level of understanding		7	5				
	% of the exam devoted to each level of understanding (cognitive/taxonomy)		58.33	41.67				

The passing score of the exam is 70%.

After successfully passing the exam, candidates will be able to apply for the "PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager" credential depending on their level of experience.

Taking the Exam

General Information on 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. **Paper-based:** 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.
2. **Online:** Exams are provided electronically via the PECB Exams application. The use of electronic devices, such as tablets and cell phones, is not allowed. The exam session is supervised remotely by a PECB Invigilator via the PECB Exams application and an external/integrated camera.

For more detailed information about the online format, please refer to the PECB Online Exam Guide.

PECB exams are available in two types:

1. Essay-type question exam
2. Multiple-choice question exam

This exam consists of 12 essay-type questions. They are used to determine whether a candidate has acquired the necessary competencies related to the defined competency domains. Additionally, problem-solving techniques and arguments that are supported with reasoning and evidence will also be evaluated.

The exam is open book and is not intended to measure memorizing or recalling information. It aims to evaluate candidates' comprehension, analytical skills, and applied knowledge. Therefore, candidates are required to provide logical and convincing answers and explanations in order to demonstrate that they have understood the content and the main concepts of the competency domains. You will find a sample of exam questions provided below.

Since the exam is "open book," candidates are allowed to use the following reference materials:

- A hard copy of ISO/IEC 27032 standard
- Training course materials (accessed through PECB Exams app and/or printed)
- Any personal notes taken during the training course (accessed through PECB Exams app and/or printed)
- A hard copy dictionary

Any attempt to copy, collude, or otherwise cheat during the exam session will lead to automatic failure.

PECB exams are available in English and other languages. To learn if the exam is available in a particular language, please contact examination@pecb.com.

Note: PECB will progressively transition to multiple-choice exams. They will also be open book and comprise scenario-based questions that will allow PECB to evaluate candidates' knowledge, abilities, and skills to use information in new situations (apply), draw connections among ideas (analyze), and justify a stand or decision (evaluate). All PECB multiple-choice exams have one question and three alternatives, of which only one is correct.

For specific information about exam types, languages available, and other details, visit the List of PECB Exams.

Sample Exam Questions

Question 1: Roles and responsibilities of the cybersecurity program team
Explain why service providers are considered as stakeholders?

Possible answer:
According to clause 10.3 of ISO/IEC 27032, service providers have similar roles and responsibilities with consumer organizations; however, they have additional responsibilities in maintaining or even improving the security of the cyberspace by:

- *offering safe and secure products and services*
- *providing safety and security guidance for end-users*
- *helping other providers and consumers with regard to the trends and observations of traffic in their networks and services*

If they provide information and services to the cyberspace and the cyberspace environment depends on them, they should be considered stakeholders. So, service providers are affected by the outcome of the cyberspace or the services in it.

Question 2: Cybersecurity controls
List at least two controls that clause 12.3 *Server protection* of ISO/IEC 27032 suggests to use in order to protect servers against unauthorized access and the hosting of malicious content on the servers.

Possible answer:
1. *Implement a system to test and deploy security updates, and ensure the server operating system and applications are kept up-to-date with the security updates are available*
2. *Conduct regular vulnerability assessments and security testing for the online sites and applications to ensure that their security is maintained appropriately*

Question 3: Awareness and training
What should organizations do to make their employees aware of the emerging cybersecurity risks? In addition, how should organization train their employees so they can effectively respond to cybersecurity risks?

Possible answer:
To achieve these objectives, organizations should:
- *Regularly inform employees on cybersecurity risk status and findings concerning the organization and the industry*
- *Design, organize, and deliver focused training sessions that simulate cyberattacks*
- *Conduct regular testing, with walkthroughs of relevant scenarios to ensure comprehensive understanding and ability to execute procedures and specific tools*

Receiving the Exam Results

Exam results will be communicated via email. The only possible results are *pass* and *fail*; no specific grade will be included.

- 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.

Candidates that disagree with the results may request a re-evaluation by writing to results@pecb.com within 30 days of receiving the results. Re-evaluation requests received after 30 days will not be processed. If candidates do not agree with the results of the reevaluation, they have 30 days from the date they received the reevaluated exam results to file a complaint through the PECB Ticketing System. Any complaint 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, s/he 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, because 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 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

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.

Reschedule the Exam

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

Apply for Certification

All candidates who successfully pass the exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credentials they were examined for. Specific educational and professional 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 online profile), including contact details of references who will be contacted to validate the candidate's professional experience. Candidates can submit their application in various languages. Candidates can choose to either pay online or be billed. For additional information, contact certification@pecb.com.

The online certification application process is very simple and takes only a few minutes, as follows:

- Register your account
- Check your email for the confirmation link
- Log in to apply for certification

For more information about the application process, follow the instructions on this manual Apply for Certification.

The application is approved as soon as the Certification Department validates that the candidate fulfills all the certification requirements regarding the respective credential. An email will be sent to the email address provided during the application process to communicate the application status. If approved, candidates will then be able to download the certification from their PECB Account.

PECB provides support in both English and French.

Renew your Certification

PECB certifications are valid for three years. To maintain them, candidates must demonstrate every year that they are still performing tasks that are related to the certification. PECB certified professionals must annually provide Continual Professional Development (CPD) credits and pay $100 as the Annual Maintenance Fee (AMF) to maintain the certification. For more information, please visit the Certification Maintenance page on the PECB website.

Closing a Case

If candidates do not apply for certification within three years, 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 and pay the required fee.

PECB

SECTION III: CERTIFICATION REQUIREMENTS

ISO/IEC 27032 Lead Cybersecurity Manager

The requirements for PECB ISO/IEC 27032 Lead Cybersecurity Manager certifications are:

Credential	Professional experience	Cybersecurity program experience	Other requirements	Credential
PECB Certified ISO/IEC 27032 Provisional Cybersecurity Manager	PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27032 Cybersecurity Manager	PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager exam or equivalent	Two years: One year of work experience in cybersecurity	At least 200 hours of cybersecurity activities	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager	PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager exam or equivalent	Five years: Two years of work experience in cybersecurity	At least 300 hours of cybersecurity activities	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27032 Senior Lead Cybersecurity Manager	PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager exam or equivalent	Ten years: Seven years of work experience in cybersecurity	At least 1,000 hours of cybersecurity activities	Signing the PECB Code of Ethics

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

1. Implementing and managing a cybersecurity program
2. Implementing and managing cybersecurity controls
3. Implementing a cybersecurity risk management program
4. Creating risk mitigation strategies
5. Implementing attack mitigation vectors
6. Establishing a framework for information sharing and coordination
7. Managing cybersecurity incident response plan

SECTION IV: CERTIFICATION RULES AND POLICIES

Professional References

For each application, two professional references are required. They must be from individuals who have worked with the candidate in a professional environment and can validate their cybersecurity program experience, as well as their current and previous work history. Professional references of persons who fall under the candidate's supervision or are their relatives are not valid.

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 résumé.

Cybersecurity Program Experience

The candidate's cybersecurity program 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 candidate's eligibility for certification. 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 can eventually lead to its downgrade to a lower credential.

Denial of Certification

PECB can deny certification if candidates:

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

For more detailed information, refer to "Complaint and Appeal" section.

The application payment for the certification is non-refundable.

Suspension of Certification

PECB can temporarily suspend certification if the candidate fails to satisfy the requirements. Other reasons for suspending certification include:

- PECB receives large amounts of or serious complaints by interested parties (Suspension will be applied until the investigation has been completed.).
- The logos of PECB or accreditation bodies are intentionally misused.
- The candidate fails to correct the misuse of a certification mark within the time frame determined by PECB.
- The certified individual has voluntarily requested a suspension.
- PECB deems appropriate other conditions for suspension of certification.

Revocation of Certification

PECB can revoke certification if the candidate fails to fulfill the PECB requirements. Candidates are then no longer allowed to represent themselves as PECB certified professionals. Other reasons for revoking certification can be if candidates:

- Violate the PECB Code of Ethics
- Misrepresent and provide false information of the scope of the certification
- Break any other PECB rules

Upgrade of Credentials

Professionals can apply to upgrade to a higher credential as soon as they can demonstrate that they fulfil the requirements.

In order to apply for an upgrade, candidates need to login in to their PECB Account, visit the “My Certifications” tab, and click on the “Upgrade” link. The upgrade application fee is $100.

Downgrade of Credentials

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

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

Note: PECB certified professionals who hold Lead Certifications and fail to provide evidence of certification maintenance requirements will have their credentials downgraded. On the other hand, the holders of Master Certifications who fail to submit CPDs and pay AMFs will have their certifications revoked.

Other Statuses

Besides being active, suspended, or revoked, a certification can be voluntarily withdrawn or designated as Emeritus. More information about these statuses and the permanent cessation status, and how to apply, please visit Certification Status Options.

SECTION V: PECB GENERAL POLICIES

PECB Code of Ethics

Adherence to the PECB Code of Ethics is a voluntary engagement. It is important that PECB certified professionals not only adhere to the principles of this Code, but also encourage and support the same from others. More information can be found here.

Other Exams and Certifications

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 27001 Lead Auditor certification).

Non-discrimination and Special Accommodations

All candidate applications will be evaluated objectively, regardless of the candidate's age, gender, race, religion, nationality, or marital status.

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations 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. Any information candidates provide regarding their disability/need will be treated with strict confidentiality.

Click here to download the Candidates with Disabilities Form.

Complaints and Appeals

Any complaints must be made no later than 30 days after receiving the certification decision. PECB will provide a written response to the candidate within 30 working days after receiving the complaint. If they do not find the response satisfactory, the candidate has the right to file an appeal. For more information about the complaints and appeal procedures, click here.

(1) 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.

(2) 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

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.

Emails:
Examination: examination@pecb.com
Certification: certification@pecb.com
Customer Service: customer@pecb.com