PECB

BEYOND RECOGNITION

ISO/IEC 27400 LEAD MANAGER

Candidate Handbook

PECB

Table of Contents

SECTION I: INTRODUCTION

About PECB[1]

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

Slogan:
Beyond Recognition

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

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

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

[1] **Notes:**

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

The Value of PECB Certification/Certificate Program

Accreditation

PECB credentials are internationally recognized and endorsed by many accreditation bodies, so professionals who pursue them will benefit from our recognition in domestic and international markets.

Our certifications are distinguished by prestigious global accreditations, affirming both their value and your expertise. PECB certifications are validated by top-tier bodies including the International Accreditation Service (IAS-PCB-111), the United Kingdom Accreditation Service (UKAS-No. 21923), the Korean Accreditation Board (KAB-PC-08), and Comité français d'accréditation (COFRAC N° 4-0637) under ISO/IEC 17024 – General requirements for bodies operating certification of persons. Additionally, our certificate programs are validated by the accreditation from the ANSI National Accreditation Board (ANAB-Accreditation ID 1003) under ANSI/ASTM E2659-18, Standard Practice for Certificate Programs.

PECB is also an esteemed associate member of The Independent Association of Accredited Registrars (IAAR), and a full member of the International Personnel Certification Association (IPC), a signatory member of IPC MLA, and a member of Club EBIOS, CPD Certification Service, and CLUSIF. Furthermore, we hold an approved status as an Approved Publishing Partner (APP) by the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) for the Cybersecurity Maturity Model Certification standard (CMMC), and are authorized by Club EBIOS to offer the EBIOS Risk Manager Skills certification and by CNIL (Commission Nationale de l'Informatique et des Libertés) to offer the DPO's skills and knowledge certification. For more detailed information, click here.

High-quality products and services

We are proud to provide our clients with high-quality products and services that match their needs and demands. All of our products are carefully prepared by a team of experts and professionals based on the best practices and methodologies.

Compliance with standards

Our certifications and certificate programs are a demonstration of compliance with ISO/IEC 17024 and ASTM E2659. They ensure that the standard requirements have been fulfilled and validated with adequate consistency, professionalism, and impartiality.

Customer-oriented service

We are a customer-oriented company and treat all our clients with value, importance, professionalism, and honesty. Our Customer Support team is available 24 hours a day, 7 days a week to address questions, requests and needs.

PECB Code of Ethics

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

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

Introduction to ISO/IEC 27400 Lead Manager Certification

The ISO/IEC 27400 Lead Manager training course provides participants with a comprehensive understanding of the principles, strategies, and best practices of cybersecurity for the Internet of Things (IoT). It covers the key security risks, requirements, and controls outlined in ISO/IEC 27400, equipping professionals with the knowledge needed to establish, implement, manage, and continually improve IoT security measures within an organization.

The "ISO/IEC 27400 Lead Manager" credential is a professional certification for individuals aiming to demonstrate competence in implementing and managing IoT security and privacy management systems, including compliance documentation, risk management, and monitoring aligned with ISO/IEC 27400.

Considering that IoT security and privacy management is among the most critical and quickly progressing fields, obtaining an internationally recognized certification such as ISO/IEC 27400 Lead Manager can significantly enhance your career potential and help achieve your professional objectives.

This document specifies the PECB ISO/IEC 27400 Lead Manager certification scheme in compliance with ISO/IEC 17024:2012. It also outlines the steps that candidates should take to obtain and maintain their credentials. As such, it is very important to carefully read all the information included in this document before completing and submitting your application. If you have questions or need further information after reading it, please contact certification.team@pecb.com.

PECB

SECTION II: EXAMINATION PREPARATION, RULES, AND POLICIES

Preparing for and scheduling the exam

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

To schedule the exam, candidates have two options:

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

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

Rescheduling the exam

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

Application fees for examination and certification

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

- Lead Exam: $1000[2]
- Manager Exam: $700
- Foundation Exam: $500
- Transition Exam: $500

The application fee for certification are as follows:

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

For the candidates that have attended the training course via one of PECB's partners, the application fee covers the costs of the exam (first attempt and first retake), the application for certification, and the first year of Annual Maintenance Fee (AMF).

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

Competency domains

The ISO/IEC 27400 Lead Manager certification is intended for:

- Individuals seeking to gain a thorough understanding of IoT security and privacy principles and best practices
- Professionals responsible for ensuring security, privacy, and compliance in IoT environments
- Managers overseeing IoT infrastructure and managing risks associated with IoT deployments
- Consultants advising organizations on IoT security, privacy, and risk management
- Individuals looking to advance their careers in the fast development of the IoT security industry
- IoT service providers, IoT service developers, and IoT users who are involved in defining security and privacy requirements or implementing controls throughout the IoT systems life cycle, as described in ISO/IEC 30141 and ISO/IEC 27400

The content of the exam is divided as follows:

- **Domain 1:** Fundamental principles and concepts of IoT security
- **Domain 2:** IoT security roles and responsibilities and governance
- **Domain 3:** IoT risk management
- **Domain 4:** Selection of privacy and security controls in IoT
- **Domain 5:** Awareness, training, and IoT security monitoring
- **Domain 6:** IoT incident management
- **Domain 7:** IoT security audits, performance measurement, and continual improvement

Domain 1: Fundamental principles and concepts of IoT security

Main objective: Ensure that the candidate is able to interpret and apply the fundamental principles, concepts, and regulatory frameworks related to IoT security and privacy.

Competencies	Knowledge statements
1. Ability to explain the main concepts and objectives of IoT security and privacy	1. Knowledge of the structure, scope, and objectives of ISO/IEC 27400
2. Ability to identify and describe key international standards and regulatory frameworks related to IoT	2. Knowledge of global standards and regulatory frameworks applicable to IoT (e.g., ISO/IEC 30141, NIST SP 800-183, ETSI EN 303 645)
3. Ability to compare the structure and purpose of ISO/IEC 27400 with other relevant standards (e.g., ISO/IEC 30141, NIST SP 800-183, ETSI EN 303 645)	3. Knowledge of the components and characteristics of IoT ecosystems (e.g., devices, platforms, and communication models)
4. Ability to interpret principles such as confidentiality, integrity, availability, risk management, and security control in the context of IoT	4. Knowledge of the principles of information security, including confidentiality, integrity, and availability
	5. Knowledge of vulnerabilities, threats, impacts, and risks in the IoT environment
	6. Knowledge of key terminology and foundational concepts from ISO/IEC 27400

Domain 2: IoT security roles and responsibilities and governance

Main objective: Ensure that the candidate is able to analyze the organizational context and define appropriate IoT security roles and responsibilities, objectives, and structures to support governance in IoT environments.

Competencies	Knowledge statements
1. Ability to identify and evaluate an organization's mission, objectives, values, and strategies in relation to IoT security	1. Knowledge of the elements defining an organization's mission, objectives, values, and strategies related to IoT
2. Ability to assess internal and external environments to determine their impact on IoT security objectives	2. Knowledge of the influence of internal and external environments on IoT security governance
3. Ability to define key IoT security processes, perform gap analysis, and establish maturity targets	3. Knowledge of key processes and activities required for implementing IoT security
4. Ability to identify and categorize types of security-related policies applicable in IoT environments	4. Knowledge of gap analysis methods and key steps for defining and assessing maturity targets
5. Ability to define the organizational structure and assign roles and responsibilities for IoT security	5. Knowledge of types of policies relevant to IoT security and risk management
6. Ability to apply the RASCI model to assign responsibilities and ensure effective role distribution	6. Knowledge of roles and responsibilities of IoT service providers and developers
7. Ability to establish and structure an effective IoT security team	7. Knowledge of the RASCI model and its application to IoT environments
	8. Knowledge of the process of establishing and organizing an IoT security team

Domain 3: IoT risk management

Main objective: Ensure that the candidate is able to apply IoT life cycle processes, asset management practices, and risk management frameworks to effectively support secure IoT system implementation.

Competencies	Knowledge statements
1. Ability to describe the stages and characteristics of IoT device and service life cycles	1. Knowledge of IoT device and service life cycles and associated security implications
2. Ability to apply life cycle-based planning for provisioning, monitoring, updating, and decommissioning IoT systems	2. Knowledge of life cycle planning and quality assurance processes for secure IoT service delivery
3. Ability to integrate security and privacy considerations throughout the IoT life cycle	3. Knowledge of roles and responsibilities of developers and providers in the IoT life cycle
4. Ability to identify and classify assets, including primary, supporting, and those located outside secured areas	4. Knowledge of asset identification techniques and IT asset life cycle stages
5. Ability to implement IoT asset management programs and IT asset management (ITAM) systems	5. Knowledge of ITAM systems and IoT asset management programs
6. Ability to explain the IoT risk management process, including identification, analysis, evaluation, and risk treatment	6. Knowledge of challenges related to managing assets outside physically secure areas
7. Ability to apply structured risk management approaches in the context of IoT-specific threats and vulnerabilities	7. Knowledge of IoT risk sources and system vulnerabilities
	8. Knowledge of structured IoT risk management frameworks and their components
	9. Knowledge of techniques for risk identification, risk analysis, risk evaluation, and risk treatment in IoT environments

Domain 4: Selection of privacy and security controls in IoT

Main objective: Ensure that the candidate is able to evaluate and apply appropriate privacy and security controls, including the use of blockchain technology, to enhance the protection and transparency of IoT systems.

Competencies	Knowledge statements
1. Ability to identify and apply security controls for IoT service developers, service providers, and users as defined in ISO/IEC 27400	1. Knowledge of security control categories and requirements for IoT stakeholders based on ISO/IEC 27400
2. Ability to select and implement privacy controls to protect personal and sensitive data in IoT environments	2. Knowledge of privacy control principles and implementation practices in IoT environments
3. Ability to distinguish between responsibilities for privacy and security among developers, providers, and users	3. Knowledge of the differences in privacy and security responsibilities among developers, providers, and users
4. Ability to explain the role of blockchain technology in enhancing IoT security and transparency	4. Knowledge of blockchain fundamentals, including architecture and components
5. Ability to describe the components and architecture of blockchain and its relevance to IoT systems	5. Knowledge of the benefits and limitations of using blockchain for IoT system security
6. Ability to evaluate the applicability of Hyperledger Fabric and other blockchain frameworks for securing IoT environments	6. Knowledge of blockchain integration scenarios such as smart home security and supply chain transparency
	7. Knowledge of Hyperledger Fabric and its modular architecture for supporting secure IoT ecosystems

Domain 5: Awareness, training, and IoT security monitoring

Main objective: Ensure that the candidate is able to develop and evaluate awareness, training, and monitoring programs to enhance organizational IoT security and privacy performance.

Competencies	Knowledge statements
1. Ability to differentiate between competence, training, awareness, and communication	1. Knowledge of the distinctions between competence, training, awareness, and communication in the context of IoT security
2. Ability to design and implement effective awareness and training programs tailored to IoT security needs	2. Knowledge of awareness programs and training development practices
3. Ability to assess competence development needs and plan related activities	3. Knowledge of identification and planning of competence development needs, programs, and activities
4. Ability to evaluate the effectiveness of competence development initiatives	4. Knowledge of competence evaluation methods
5. Ability to define and establish IoT security monitoring and performance measurement objectives	5. Knowledge of measurement objectives and performance monitoring principles
6. Ability to identify what aspects of an IoT security program must be monitored and measured	6. Knowledge of aspects of IoT security programs that require monitoring and ways to define them
7. Ability to develop performance indicators for IoT security programs	7. Knowledge of performance indicators and their applicability to IoT security effectiveness
8. Ability to select appropriate monitoring methods and reporting practices	8. Knowledge of monitoring methods, frequencies, and reporting strategies for IoT security programs

Domain 6: IoT incident management

Main objective: Ensure that the candidate is able to manage the full life cycle of IoT incidents, from preparation and detection to response and post-incident evaluation.

Competencies	Knowledge statements
1. Ability to define IoT incident management objectives aligned with organizational policies 2. Ability to plan and prepare incident management procedures and assign responsibilities 3. Ability to detect, classify, and report IoT-related incidents 4. Ability to assess incidents and make decisions regarding containment and escalation 5. Ability to respond effectively to IoT security incidents 6. Ability to evaluate incident response effectiveness and apply lessons learned for continual improvement	1. Knowledge of IoT incident management objectives and planning principles 2. Knowledge of procedures for preparing and equipping teams for incident response 3. Knowledge of detection methods and incident reporting protocols 4. Knowledge of assessment and decision-making processes during incidents 5. Knowledge of effective response strategies for IoT-specific incidents 6. Knowledge of post-incident activities, including evaluation, documentation, and learning opportunities

Domain 7: IoT security audits, performance measurement, and continual improvement

Main objective: Ensure that the candidate is able to conduct internal audits, evaluate performance, and implement continual improvements for IoT security and privacy programs.

Competencies	Knowledge statements
1. Ability to describe the purpose and types of audits and distinguish between internal and external audits 2. Ability to plan and implement an IoT audit program, including roles, responsibilities, and resource allocation 3. Ability to apply appropriate audit methods and techniques 4. Ability to identify, document, and follow up on nonconformities 5. Ability to initiate and manage corrective actions and maintain the audit program 6. Ability to monitor change factors that affect the IoT security program 7. Ability to update documented information and maintain improvement records 8. Ability to apply continual improvement principles to enhance the effectiveness of the IoT security program	1. Knowledge of audit objectives, types of audits, and principles of independence and access 2. Knowledge of designing, managing, and maintaining an audit program 3. Knowledge of auditor roles, audit planning, and execution methods 4. Knowledge of nonconformity identification and corrective action procedures 5. Knowledge of change factors influencing IoT security performance 6. Knowledge of maintaining and improving the IoT security program through continual monitoring 7. Knowledge of methods for updating and documenting improvements in IoT programs

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 IoT security	10	12.5	X	
	IoT security roles and responsibilities and governance	15	18.75	X	
	IoT risk management	15	18.75	X	
	Selection of privacy and security controls in IoT	15	18.75		X
	Awareness, training, and IoT security monitoring	5	6.25	X	
	IoT incident management	12	15	X	
	IoT security audits, performance measurement, and continual improvement	8	10	X	
	Total	**80**	**100%**		
	Number of questions per level of understanding			**65**	**15**
	% of the exam devoted to each level of understanding (cognitive/taxonomy)			**81.25%**	**18.75%**

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

Taking the exam

General information about the exam
Candidates are required to arrive/be present at least 30 minutes before the exam starts.

Candidates who arrive late will not be given additional time to compensate for the late arrival and may not be allowed to sit for the exam.

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

If requested on the day of the exam (paper-based exams), additional time can be provided to candidates taking the exam in a non-native language, as follows:

- 10 additional minutes for Foundation exams
- 20 additional minutes for Manager exams
- 30 additional minutes for Lead exams

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

a. Multiple-choice, closed-book, where the candidates are not allowed to use any reference materials. Usually, Foundation and Transition exams are of this type.
b. Essay-type, open-book, where candidates are allowed to use the following reference materials:
    - A hard copy of main standard
    - Training course materials (through KATE and/or printed)
    - Any personal notes taken during the training course (through KATE and/or printed)
    - A hard copy dictionary
c. Multiple-choice, open-book, where candidates are allowed to use the following reference materials:
    - A hard copy of main standard
    - Training course materials (through KATE and/or printed)
    - Any personal notes taken during the training course (through KATE and/or printed)
    - A hard copy dictionary

2) Paper Based: Exams are also available in a paper format. The use of electronic devices, such as laptops, tablets, or phones, is not allowed. The exam session is supervised by a PECB approved Invigilator at the location where the Partner has organized the training course.
PECB Exam Types:

a. Multiple-choice, closed-book, where the candidates are not allowed to use any reference materials. Usually, Foundation and Transition exams are of this type.
b. Essay-type, open-book, where candidates are allowed to use the following reference materials:
    - A hard copy of main standard
    - Training course materials (printed)
    - Any personal notes taken during the training course (printed)

- A hard copy dictionary

c. Multiple-choice, open-book, where candidates are allowed to use the following reference materials:
   - A hard copy of main standard
   - Training course materials (printed)
   - Any personal notes taken during the training course (printed)
   - A hard copy dictionary

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

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

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

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

- A hard copy of the **ISO/IEC 27400** standard
- Training course materials (accessed through the PECB Exams app and/or printed)
- Any personal notes taken during the training course (accessed through the PECB Exams app and/or printed)
- A hard copy dictionary

A sample of exam questions will be provided below.

Sample exam questions

WestFin is a global financial technology company based in Dublin, Ireland, offering digital banking and investment services. The company has expanded into several international markets, supported by regional tech hubs in Europe, North America, and Southeast Asia. As *WestFin*'s Internet of Things (IoT) ecosystem grows, the company is focusing on improving its security and privacy measures. To support this effort, it began by assessing its business environment to understand market pressures and competition. The findings helped shape its IoT security strategy and highlight key risks and opportunities.

The company has started rolling out standardized IoT security processes across various departments. Although procedures are being followed more consistently, they still depend heavily on the individual experience of those implementing them. No formal training or communication has been provided yet, and the lack of consistency shows that these efforts are still in the early stages of becoming fully established across the organization.

To support the rollout of IoT security measures, *WestFin*'s IT Department developed an official IoT security policy. The policy sets clear requirements for device configuration, access control, and network segmentation across the company's IoT systems. It was formally approved by executive management, published, and communicated to involved personnel and parties through awareness sessions and team briefings to ensure consistent understanding and adoption across relevant business units. The policy also outlines specific roles and responsibilities to support its implementation and ongoing effectiveness. These include responsibilities for risk management activities; designing security measures for IoT systems, devices, and services; implementing and operating these measures during development and operations; managing supplier relationships; delivering awareness, education, and training programs; and supporting the incident management program.

As part of its IoT security strategy for digital banking services, *WestFin* ensures that device settings support user security by controlling software versions, open ports, and access to sensitive functions. Devices requiring passwords must use unique, securely shared credentials. These requirements are defined in the company's IoT security policy to protect users and support consistent security across its digital platforms.

Based on the scenario above, please answer the following questions.

1. **At which maturity level is *WestFin* currently operating based on its IoT security process implementation?**
   A. **Managed**
   B. Defined
   C. Optimized

2. **Does *WestFin* fully align with ISO/IEC 27400 Control-01 regarding the publication and communication of its IoT security policy?**
   A. No, the company failed to ensure the policy was accessible to external stakeholders, which is recommended under Control-01.
   B. **Yes, the company ensured that the IoT security policy was approved by management, published, formally communicated through training and awareness sessions, and distributed to all relevant parties.**
   C. No, communication efforts related to the policy were limited to high-level management, and frontline employees were not involved in the dissemination process.

3. **Does *WestFin* meet the guidelines of ISO/IEC 27400 Control-02 regarding roles and responsibilities for security of IoT?**
   A. No, the company failed to document the roles and responsibilities related to IoT security.
   B. No, the company did not define responsibilities for implementing IoT security measures.
   C. **Yes, the company meets the guidelines, as it has defined and documented all roles and responsibilities.**

4. **Which ISO/IEC 27400 control is reflected in the company's actions described in the last paragraph of the scenario?**
   A. **Control 15**
   B. Control 19
   C. Control 23

Exam results

Exam results will be communicated via email.

- The time span for the communication starts from the exam date and lasts three to eight weeks for essay type exams and two to four weeks for multiple-choice paper-based exams.
- For online multiple-choice exams, candidates receive their results instantly.

Candidates who successfully complete the exam will be able to apply for one of the credentials of the respective certification scheme.

For candidates who fail the exam, a list of the domains where they have performed poorly will be added to the email to help them prepare better for a retake.

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

Exam Retake Policy

There is no limit to the number of times a candidate can retake an exam. However, there are certain limitations in terms of the time span between exam retakes.

If a candidate does not pass the exam on the 1st attempt, they must wait 15 days after the initial date of the exam for the next attempt (1st retake).

Note: Candidates who have completed the training course with one of our partners, and failed the first exam attempt, are eligible to retake for free the exam within a 12-month period from the date the coupon code is received (the fee paid for the training course, includes a first exam attempt and one retake). Otherwise, retake fees apply.

For candidates that fail the exam retake, PECB recommends they attend a training course in order to be better prepared for the exam.

To arrange exam retakes, based on exam format, candidates that have completed a training course, must follow the steps below:

1. **Online Exam:** when scheduling the exam retake, use the initial coupon code to waive the fee
2. **Paper-Based Exam:** candidates need to contact the PECB Partner/Distributor who has initially organized the session for exam retake arrangement (date, time, place, costs).

Candidates that have not completed a training course with a partner, but sat for the online exam directly with PECB, do not fall under this Policy. The process to schedule the exam retake is the same as for the initial exam.

Exam Security Policy

A significant component of a professional certification credential is maintaining the security and confidentiality of the exam. PECB relies upon the ethical behavior of certification holders and applicants to maintain the security and confidentiality of PECB exams. Any disclosure of information about the content of PECB exams is a direct violation of PECB's Code of Ethics. PECB will take action against any individuals that violate such rules and policies, including permanently banning individuals from pursuing PECB credentials and revoking any previous ones. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

SECTION III: CERTIFICATION PROCESS AND REQUIREMENTS

PECB ISO/IEC 27400 credentials

All PECB certifications have specific requirements regarding education and professional experience. To determine which credential is right for you, take into account your professional needs and analyze the criteria for the certifications.

The credentials in the PECB ISO/IEC 27400 scheme have the following requirements:

Credential	Exam	Professional experience	MS project experience	Other requirements
PECB Certified ISO/IEC 27400 Provisional Manager	PECB Certified ISO/IEC 27400 Lead Manager exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27400 Manager		Two years: One year of work experience in IoT security management	Project activities: a total of 200 hours	
PECB Certified ISO/IEC 27400 Lead Manager		Five years: Two years of work experience in IoT security management	Project activities: a total of 300 hours	
PECB Certified ISO/IEC 27400 Senior Lead Manager		Ten years: Seven years of work experience in IoT security management	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. Planning and managing IoT device and service life cycles
2. Integrating security and privacy into each life cycle phase
3. Identifying and classifying IoT assets
4. Implementing asset management practices and ITAM systems
5. Applying IoT risk management processes
6. Treating and monitoring risks throughout the system life cycle

Applying for certification

All candidates who successfully pass the exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credential they were assessed for. Specific professional experience requirements need to be fulfilled in order to obtain a PECB certification. Candidates are required to fill out the online certification application form (that can be accessed via their PECB account), including contact details of individuals who will be contacted to validate the candidates' professional experience. They can choose to either pay online or be billed. For additional information, please contact certification.team@pecb.com.

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

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

For more information on how to apply for certification, click here.

The Certification Department validates that the candidate fulfills all the certification requirements regarding the respective credential. The candidate will receive an email about the application status, including the certification decision.

Following the approval of the application by the Certification Department, the candidate will be able to download the certificate and claim the corresponding Digital Badge. For more information about downloading the certificate, click here, and for more information about claiming the Digital Badge, click here.

Professional experience

Candidates must provide complete and correct information regarding their professional experience, including job title(s), start and end date(s), job description(s), and more. Candidates are advised to summarize their previous or current assignments, providing sufficient details to describe the nature of the responsibilities for each job. More detailed information can be included in the CV.

Professional references

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

IoT security and privacy management project experience

The candidate's IoT security and privacy management log will be checked to ensure that the candidate has the required number of implementation hours.

Evaluation of certification applications

The Certification Department will evaluate each application to validate the candidates' eligibility for certification or certificate program. A candidate whose application is being reviewed will be notified in writing and, if necessary, given a reasonable time frame to provide any additional documentation. If a candidate does not respond by the deadline or does not provide the required documentation within the given time frame, the Certification Department will validate the application based on the initial information provided, which may lead to the candidates' credential downgrade.

SECTION IV: CERTIFICATION POLICIES

Denial of Certification/Certificate Program

PECB can deny certification/certificate program if candidates:

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

Any concerns regarding the denial of certification/certificate program may file a complaint or appeal by following the complaint and appeal process (Complaint and Appeal Policy - PECB).

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

Suspension of Certification

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

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

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

A suspended certification can either be:

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

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

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

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

Revocation of Certification

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

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

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

Individuals whose certification has been revoked may file a complaint or appeal by following the complaint and appeal process (Complaint and Appeal Policy - PECB).

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

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

Other Statuses

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

Emeritus Status

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

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

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

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

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

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

Voluntary Withdrawal Status

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

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

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

Permanent Cessation Status

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

Upgrade and downgrade of credentials

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

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

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

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

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

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

Renewing the certification

PECB certifications are valid for three years. To maintain them, PECB certified professionals must meet the requirements related to the designated credential, e.g., they must fulfill the required number of continual

professional development (CPD) hours. In addition, they need to pay the annual maintenance fee. For more information, go to the Certification Maintenance page on the PECB website.

Closing a case

If candidates do not apply for certification within one year, their case will be closed. Even though the certification period expires, candidates have the right to reopen their case. However, PECB will no longer be responsible for any changes regarding the conditions, standards, policies, and candidate handbook that were applicable before the case was closed. A candidate requesting their case to reopen must do so in writing to certification.team@pecb.com and pay the required fee.

Complaint and Appeal Policy

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

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

SECTION V: GENERAL POLICIES

Exams and certifications from other accredited certification bodies

PECB accepts certifications and exams from other recognized accredited certification bodies. PECB will evaluate the requests through its equivalence process to decide whether the respective certification(s) or exam(s) can be accepted as equivalent to the respective PECB certification (e.g., ISO/IEC 27400 Lead Manager certification).

Non-discrimination and special accommodations

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

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations[3] for candidates, when appropriate. If candidates need special accommodations because of a disability or a specific physical condition, they should inform the partner/distributor in order for them to make proper arrangements[4]. Any information that candidates provide regarding their disability/special needs will be treated with confidentiality. To download the Candidates with Disabilities Form, click here.

Behavior Policy

PECB aims to provide top-quality, consistent, and accessible services for the benefit of its external stakeholders: distributors, partners, trainers, invigilators, examiners, members of different committees and advisory boards, and clients (trainees, examinees, certified individuals, and certificate holders), as well as creating and maintaining a positive work environment which ensures safety and well-being of its staff, and holds the dignity, respect and human rights of its staff in high regard.

The purpose of this Policy is to ensure that PECB is managing unacceptable behavior of external stakeholders towards PECB staff in an impartial, confidential, fair, and timely manner. To read the Behavior Policy, click here.

Refund Policy

PECB will refund your payment, if the requirements of the Refund Policy are met. To read the Refund Policy, click here.

[3] According to ADA, the term "reasonable accommodation" may include: (A) making existing facilities used by employees readily accessible to and usable by individuals with disabilities; and (B) job restructuring, part-time or modified work schedules, reassignment to a vacant position, acquisition or modification of equipment or devices, appropriate adjustment or modifications of examinations, training materials or policies, the provision of qualified readers or interpreters, and other similar accommodations for individuals with disabilities.

[4] ADA Amendments Act of 2008 (P.L. 110–325) Sec. 12189. Examinations and courses. [Section 309]: Any person that offers examinations or courses related to applications, licensing, certification, or credentialing for secondary or post-secondary education, professional, or trade purposes shall offer such examinations or courses in a place and manner accessible to persons with disabilities or offer alternative accessible arrangements for such individuals.

Address:

Headquarters
6683 Jean Talon E,
Suite 336 Montreal,
H1S 0A5, QC,
CANADA

Tel./Fax:

T: +1-844-426-7322
F: +1-844-329-7322

Emails:

Examination:
examination.team@pecb.com

Certification:
certification.team@pecb.com

Customer Service:
support@pecb.com

PECB Help Center

Visit our Help Center to browse Frequently Asked Questions (FAQ), view manuals for using PECB website and applications, read documents related to PECB processes, or to contact us via Support Center's online tracking system.

www.pecb.com