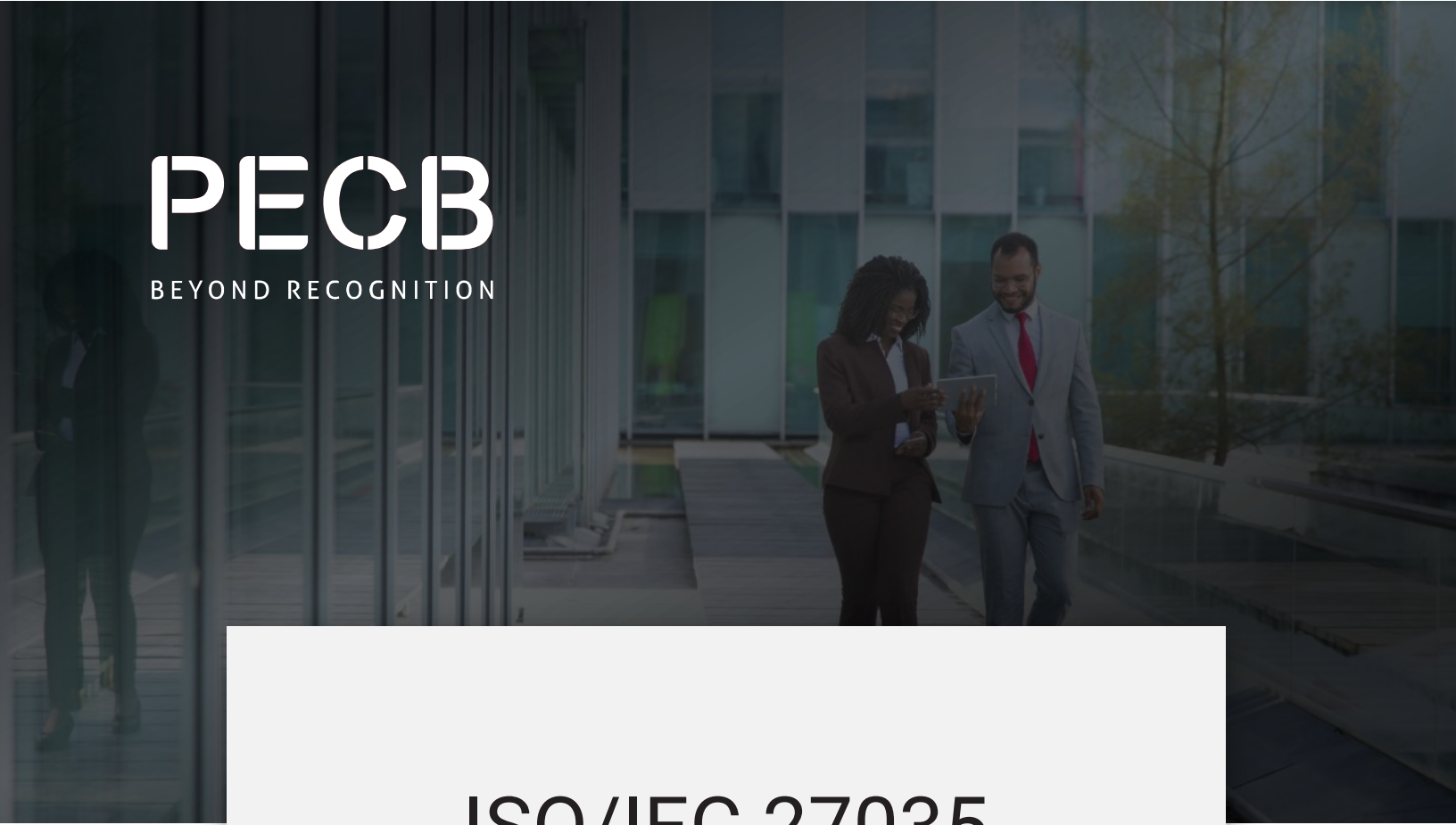


The logo for PECB, featuring the letters 'PECB' in a bold, white, sans-serif font. The letters are slightly spaced out, and the 'E' and 'C' have a unique, modern design with cutouts.

**PECB**

BEYOND RECOGNITION

A background image showing a modern office environment with large glass windows. In the foreground, a woman in a dark suit and a man in a light suit are walking and looking at a tablet together. The scene is dimly lit, suggesting an evening or indoor lighting.

# ISO/IEC 27035 LEAD INCIDENT MANAGER

## **Candidate Handbook**

## Table of Contents

---

<b>SECTION I: INTRODUCTION .....</b>	<b>3</b>
About PECB .....	3
The Value of PECB Certification.....	4
PECB Code of Ethics.....	5
Introduction to ISO/IEC 27035 Lead Incident Manager.....	6
<b>SECTION II: EXAMINATION PREPARATION, RULES, AND POLICIES .....</b>	<b>7</b>
Preparing for and scheduling the exam.....	7
Competency domains.....	8
Taking the exam.....	16
Exam Security Policy.....	20
Exam results.....	21
Exam Retake Policy.....	21
<b>SECTION III: CERTIFICATION PROCESS AND REQUIREMENTS .....</b>	<b>22</b>
PECB ISO/IEC 27035 credentials .....	22
Applying for certification .....	23
Professional experience .....	23
Professional references .....	23
ISIM project experience .....	23
Evaluation of certification applications .....	24
<b>SECTION IV: CERTIFICATION POLICIES .....</b>	<b>25</b>
Denial of certification.....	25
Certification status options .....	25
Upgrade and downgrade of credentials .....	26
Renewing the certification.....	26
Closing a case .....	26
Complaint and Appeal Policy .....	26
<b>SECTION V: GENERAL POLICIES .....</b>	<b>27</b>
Exams and certifications from other accredited certification bodies .....	27
Non-discrimination and special accommodations .....	27
Behavior Policy.....	27
Refund Policy .....	27

## SECTION I: INTRODUCTION

---

### **About PECB**

PECB is a certification body that provides education<sup>1</sup>, certification, and certificate programs for individuals on a wide range of disciplines.

Through our presence in more than 150 countries, we help professionals demonstrate their competence in various areas of expertise by providing valuable evaluation, certification, and certificate programs against internationally recognized standards.

### **Our key objectives are:**

1. Establishing the minimum requirements necessary to certify professionals and to grant designations
2. Reviewing and verifying the qualifications of individuals to ensure they are eligible for certification
3. Maintaining and continually improving the evaluation process for certifying individuals
4. Certifying qualified individuals, granting designations and maintaining respective directories
5. Establishing requirements for the periodic renewal of certifications and ensuring that the certified individuals are complying with those requirements
6. Ascertaining that PECB professionals meet ethical standards in their professional practice
7. Representing our stakeholders in matters of common interest
8. Promoting the benefits of certification and certificate programs to professionals, businesses, governments, and the public

### **Our mission**

Provide our clients with comprehensive examination, certification, and certificate program services that inspire trust and benefit the society as a whole.

### **Our vision**

Become the global benchmark for the provision of professional certification services and certificate programs.

### **Our values**

Integrity, Professionalism, Fairness

---

<sup>1</sup> Education refers to training courses developed by PECB and offered globally through our partners.

## The Value of PECB Certification

### Global recognition

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.

The value of PECB certifications is validated by the accreditation from the International Accreditation Service (IAS-PCB-111), the United Kingdom Accreditation Service (UKAS-No. 21923) and the Korean Accreditation Board (KAB-PC-08) under ISO/IEC 17024 – General requirements for bodies operating certification of persons. The value of PECB certificate programs is 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 an associate member of The Independent Association of Accredited Registrars (IAAR), 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, CLUSIF, Credential Engine, and ITCC. In addition, PECB is an approved Licensed Partner Publisher (LPP) from the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) for the Cybersecurity Maturity Model Certification standard (CMMC), is approved by Club EBIOS to offer the EBIOS Risk Manager Skills certification, and is approved by CNIL (Commission Nationale de l'Informatique et des Libertés) to offer DPO 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. PECB has a team of experts who are responsible for addressing requests, questions, and needs. We do our best to maintain a 24-hour maximum response time without compromising the quality of the services.

### Flexibility and convenience

Online learning opportunities make your professional journey more convenient as you can schedule your learning sessions according to your lifestyle. Such flexibility gives you more free time, offers more career advancement opportunities, and reduces costs.

## PECB Code of Ethics

The Code of Ethics represents the highest values and ethics that PECB is fully committed to follow, as it recognizes the importance of them when providing services and attracting clients.

The Compliance Division makes sure that PECB employees, trainers, examiners, invigilators, partners, distributors, members of different advisory boards and committees, certified individuals, and certificate holders (hereinafter “PECB professionals”) adhere to this Code of Ethics. In addition, the Compliance Division consistently emphasizes the need to behave professionally and with full responsibility, competence, and fairness in service provision with internal and external stakeholders, such as applicants, candidates, certified individuals, certificate holders, accreditation authorities, and government authorities.

It is PECB’s belief that to achieve organizational success, it has to fully understand the clients and stakeholders’ needs and expectations. To do this, PECB fosters a culture based on the highest levels of integrity, professionalism, and fairness, which are also its values. These values are integral to the organization, and have characterized the global presence and growth over the years and established the reputation that PECB enjoys today.

PECB believes that strong ethical values are essential in having healthy and strong relationships. Therefore, it is PECB’s primary responsibility to ensure that PECB professionals are displaying behavior that is in full compliance with PECB principles and values.

PECB professionals are responsible for:

1. Displaying professional behavior in service provision with honesty, accuracy, fairness, and independence
2. Acting at all times in their service provision solely in the best interest of their employer, clients, the public, and the profession in accordance with this Code of Ethics and other professional standards
3. Demonstrating and developing competence in their respective fields and striving to continually improve their skills and knowledge
4. Providing services only for those that they are qualified and competent and adequately informing clients and customers about the nature of proposed services, including any relevant concerns or risks
5. Informing their employer or client of any business interests or affiliations which might influence or impair their judgment
6. Preserving the confidentiality of information of any present or former employer or client during service provision
7. Complying with all the applicable laws and regulations of the jurisdictions in the country where the service provisions were conducted
8. Respecting the intellectual property and contributions of others
9. Not communicating intentionally false or falsified information that may compromise the integrity of the evaluation process of a candidate for a PECB certification or a PECB certificate program
10. Not falsely or wrongly presenting themselves as PECB representatives without a proper license or misusing PECB logo, certifications or certificates
11. Not acting in ways that could damage PECB’s reputation, certifications or certificate programs
12. Cooperating in a full manner on the inquiry following a claimed infringement of this Code of Ethics

To read the complete version of PECB’s Code of Ethics, go to [Code of Ethics | PECB](#).

## **Introduction to ISO/IEC 27035 Lead Incident Manager**

ISO/IEC 27035 series provides guidelines for establishing, implementing, maintaining, and continually improving information security incident management (ISIM). An ISIM program based on ISO/IEC 27035 enables organizations to prepare for, respond to, manage, and recover from information security incidents effectively. The guidelines outlined in ISO/IEC 27035-1 and ISO/IEC 27035-2 are applicable to all organizations, regardless of their size, type, complexity, or the sector they operate in.

The "PECB ISO/IEC 27035 Lead Incident Manager" credential is a professional certification for individuals looking to showcase their expertise in managing information security incidents and leading incident response teams.

PECB certifications are not a license or simply a membership. They attest the candidates' knowledge and skills gained through our training courses and are issued to candidates that have the required experience and have passed the exam.

This document specifies the PECB ISO/IEC 27035 Lead Incident 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 the PECB international office at [certification.team@pecb.com](mailto:certification.team@pecb.com).

## SECTION II: EXAMINATION PREPARATION, RULES, AND POLICIES

---

### Preparing for and scheduling the exam

All candidates are responsible for their own study and preparation for certification exams. Although candidates are not required to attend the training course to be eligible for taking the exam, attending it can significantly increase their chances of successfully passing the exam.

To schedule the exam, candidates have two options:

1. Contact one of our authorized partners. To find an authorized partner in your region, please go to [Active Partners](#). The training course schedule is also available online and can be accessed on [Training Events](#).
2. Take a PECB exam remotely through the [PECB Exams application](#). To schedule a remote exam, please go to the following link: [Exam Events](#).

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](mailto: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<sup>2</sup>
- Manager Exam: \$700
- Foundation Exam: \$500
- Transition Exam: \$500

The application fee for certification is \$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).

---

<sup>2</sup> All prices listed in this document are in US dollars.

## Competency domains

The objective of the “PECB ISO/IEC 27035 Lead Incident Manager” exam is to ensure that the candidate has acquired the necessary competence to support an organization in implementing an information security incident management plan.

The ISO/IEC 27035 Lead Incident Manager certification is intended for:

- Managers or consultants seeking to enhance their knowledge regarding the implementation of information security incident management processes
- Professionals seeking to establish and manage effective incident response teams (IRTs)
- IT professionals and information security risk managers seeking to enhance their knowledge in information security incident management
- Members of incident response teams
- Individuals responsible for incident management within an organization

The content of the exam is divided as follows:

- **Domain 1:** Fundamental principles and concepts of information security incident management
- **Domain 2:** Information security incident management process based on ISO/IEC 27035
- **Domain 3:** Designing and developing an organizational incident management process based on ISO/IEC 27035
- **Domain 4:** Preparing and executing the incident response plan for information security incidents
- **Domain 5:** Implementing incident management processes and managing information security incidents
- **Domain 6:** Improving the incident management processes and activities



## Domain 1: Fundamental principles and concepts of information security incident management

**Main objective:** Ensure that the candidate understands and is able to interpret the main principles and concepts of information security incident management.

Competencies	Knowledge statements
<ol style="list-style-type: none"> <li>1. Ability to explain the main concepts of information security incident management</li> <li>2. Ability to identify the relationship between the concepts of vulnerability, threat, risk and their impact</li> <li>3. Ability to define the concepts of confidentiality, integrity, and availability of information</li> <li>4. Ability to explain the difference between information security event and incident</li> <li>5. Ability to describe the incident management life cycle</li> <li>6. Ability to interpret the classification of security controls and their objectives</li> </ol>	<ol style="list-style-type: none"> <li>1. Knowledge of the main concepts and terminology of ISO/IEC 27035</li> <li>2. Knowledge of the main standards of the ISO/IEC 27000 family</li> <li>3. Knowledge of international industry standards and frameworks for incident management</li> <li>4. Knowledge of confidentiality, integrity, and availability of information</li> <li>5. Knowledge of information security vulnerabilities, threats, and risks</li> <li>6. Knowledge of information security event and incident</li> <li>7. Knowledge of incident management life cycle</li> <li>8. Knowledge of the difference between security control types such as technical, legal, administrative, and managerial controls</li> <li>9. Knowledge of the difference between security controls classified by their function, such as preventive, corrective, and detective controls</li> </ol>

## Domain 2: Information security incident management process based on ISO/IEC 27035

**Main objective:** Ensure that the candidate is able to identify and explain the process for information security incident management based on ISO/IEC 27035.

Competencies	Knowledge statements
1. Ability to outline and explain the objectives of incident management	1. Knowledge of the objectives of incident management
2. Ability to detail the key processes of incident management	2. Knowledge of the key processes of incident management
3. Ability to explain the incident management phases: plan and prepare, detect and report, assess and decide, respond, and learn lessons	3. Knowledge of the incident management phases
4. Ability to explain the preparation, detection, and analysis phases of incident management	4. Knowledge of the incident management phases: plan and prepare, detect and report, asses and decide, respond, and learn lessons 5. Knowledge of preparation, detection and analysis phases of incident management

## Domain 3: Designing and developing an organizational incident management process based on ISO/IEC 27035

**Main objective:** Ensure the candidate is skilled in defining the incident management scope, developing relevant policies, and executing risk assessment, treatment, and prioritization within incident management frameworks.

Competencies	Knowledge statements
1. Ability to define the scope of incident management	1. Knowledge of boundaries of the incident management scope
2. Ability to analyze the internal and external environment	2. Knowledge of the approaches used to analyze the internal and external environment
3. Ability to identify and analyze the interested parties	3. Knowledge of the identification and analysis of the interested parties
4. Ability to conduct the gap analysis	4. Knowledge of information security incident management policy
5. Ability to explain information security incident management policy	5. Knowledge of drafting the incident management policy
6. Ability to draft the incident management policy	6. Knowledge of the content of incident management policy
7. Ability to explain the risk management process	7. Knowledge of the different approaches and methodologies used to perform the risk management process
8. Ability to identify information and supporting assets	8. Knowledge of the different approaches used to perform risk identification
9. Ability to perform the steps of the risk assessment process such as risk identification, risk analysis, risk evaluation, and risk treatment	9. Knowledge of the techniques used to gather information
	10. Knowledge of the identification of information and supporting assets
	11. Knowledge of the risk analysis

## Domain 4: Preparing and executing the incident response plan for information security incidents

**Main objective:** Ensure that the candidate is able to develop, implement, and manage an incident management plan, define roles and responsibilities, effective communication strategies, and coordination with internal and external parties.

Competencies	Knowledge statements
1. Ability to draft the incident management plan	1. Knowledge of information security incident management plan
2. Ability to establish the plan and prepare phase for effective incident response	2. Knowledge of drafting the incident management plan
3. Ability to establish the detect and report phase for identifying, reporting, and recording information security incidents	3. Knowledge of establishing the plan and prepare phase
4. Ability to establish assess and decide phase for evaluating and making decisions in response to identified information security incidents	4. Knowledge of establishing the detect and report phase
5. Ability to establish the respond phase for taking actions to address and mitigate the impact of a security incident	5. Knowledge of establishing the assess and decide phase
6. Ability to establish the learn lessons phase for extracting insights from incidents to enhance incident management processes	6. Knowledge of establishing the respond phase
7. Ability to establish the incident response team	7. Knowledge of establishing the learn lessons phase
8. Ability to define incident coordinator responsibilities	8. Knowledge of establishing the incident response team
9. Ability to define incident response team structure	9. Knowledge of the incident management team structure
10. Ability to define technical and other support	10. Knowledge of the incident response team establishment
11. Ability to define and implement appropriate information security training and awareness programs	11. Knowledge of the relationship with external interested parties
12. Ability to define the scope of incident exercises	12. Knowledge of the principles for an efficient communication strategy
	13. Knowledge of the technical resources
	14. Knowledge of information security incident awareness and training
	15. Knowledge of testing the information

## Domain 5: Implementing incident management processes and managing information security incidents

**Main objective:** Ensure that the candidate develop and manage an effective incident response strategy, incorporating continuous security monitoring, incident detection, classification, response, and reporting, alongside evaluating containment strategies and handling digital evidence.

Competencies	Knowledge statements
1. Ability to implement the incident response monitoring capability	1. Knowledge of implementation of the incident response monitoring capability
2. Ability to implement an ISCM program	2. Knowledge of effective network monitoring
3. Ability to explain the steps for an effective security monitoring process	3. Knowledge of the steps for an effective security monitoring process
4. Ability to define the mechanisms to detect security incidents	4. Knowledge of the critical KPIs for measuring information security performance
5. Ability to analyze attackers methodology and goals	5. Knowledge of the indicators of security incidents
6. Ability to define an incident classification process	6. Knowledge of the categorization of information security incidents
7. Ability to define the approach for information collection	7. Knowledge of the incident classification levels
8. Ability to conduct information security event assessment	8. Knowledge of the difference between incident management log and report
9. Ability to define roles and responsibilities during the response phase	9. Knowledge of the assessment and decision on information security events
10. Ability to conduct forensic analysis	10. Knowledge of responding to information security incidents
11. Ability to define the criteria for determining the strategy	11. Knowledge of the tools and techniques used in conducting forensic analysis

## Domain 6: Improving the incident management processes and activities

**Main objective:** Ensure that the candidate can systematically review and improve the information security incident management process and its outcomes, focusing on lessons learned, risk management, performance indicators, and continual documentation updates.

Competencies	Knowledge statements
1. Ability to explain key activities in the lessons learned phase	1. Knowledge of the key activities in the lessons learned phase
2. Ability to evaluate the incident management team	2. Knowledge of extracting lessons learned
3. Ability to identify areas for improvement	3. Knowledge of identifying areas for improvement
4. Ability to establish performance indicators	4. Knowledge of evaluating the incident management team
5. Ability to select methods and determine the frequency of monitoring	5. Knowledge of reviewing information security risk assessment and management results
6. Ability to determine the appropriate tools to support the continual improvement processes of an organization	6. Knowledge of the main concepts related to continual improvement
	7. Knowledge of the processes related to the continual monitoring of change factors

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 information security incident management	10	12.5	X	
	Information security incident management process based on ISO/IEC 27035	5	6.25		X
	Designing and developing an organizational incident management process based on ISO/IEC 27035	10	12.5		X
	Preparing and executing incident response plan for information security incidents	22	27.5	X	
	Implementing incident management processes and managing information security incidents	23	28.75		X
	Improving the incident management processes and activities	10	12.5		X
	<b>Total</b>	<b>80</b>	<b>100%</b>		
Number of questions per level of understanding				<b>32</b>	<b>48</b>
% of the exam devoted to each level of understanding (cognitive/taxonomy)				<b>40%</b>	<b>60%</b>

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

After successfully passing the exam, candidates will be able to apply for obtaining the “PECB Certified ISO/IEC 27035 Lead Incident Manager” credential.

## 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. **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 information about online exams, go 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 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-dependent, 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).



# PECB

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

- A hard copy of the ISO/IEC 27035 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.

**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).

For specific information about exam types, languages available, and other details, please contact [examination.team@pecb.com](mailto:examination.team@pecb.com) or go to the [List of PECB Exams](#).

## Sample exam questions

*ZylonTech* is a leading multinational software development company based in Los Angeles. The company caters to a diverse clientele, offering robust software applications tailored to various business needs.

Recently, *ZylonTech* decided to implement ISO/IEC 27035-1 and ISO/IEC 27035-2 standards to enhance its incident management and response capabilities. This decision was driven by an unusual spike in data traffic, which raised suspicions of a potential security breach. Luke, the incident coordinator, initiated a technical analysis to identify the source of this anomaly without initially consulting the Incident Response Team (IRT), highlighting a critical moment in the incident handling process.

The incident led to a temporary service interruption, prompting *ZylonTech* to reevaluate and enhance its security measures. The company revised its approach to network monitoring, setting aggressive intervals to ensure real-time data assessment, regardless of system load. This proactive stance aimed to prevent future security breaches and maintain the integrity of *ZylonTech's* services.

Post-incident, *ZylonTech* employed a risk analysis methodology that utilized numerical scales to evaluate the likelihood and consequences of potential threats. This approach allowed the company to prioritize risks effectively and implement controls tailored to mitigate identified vulnerabilities. The adoption of this strategy reinforced *ZylonTech's* commitment to security and ensured alignment with the best practices recommended by ISO standards.

Based on the scenario above, answer the following questions:

- 1. Luke observed an unusually high amount of data traffic that could indicate a potential security incident. According to ISO/IEC 27035-1, did Luke take the correct steps for this situation?**
  - A. Yes, he performed a technical analysis to identify the source of the traffic without consulting the IRT
  - B. **No, he should coordinate the activities of the incident response team**
  - C. No, he should shut down the affected systems immediately to prevent potential data loss
- 2. Which information security principle was affected by the incident that occurred in *ZylonTech*?**
  - A. Confidentiality
  - B. Integrity
  - C. **Availability**
- 3. Which of the following security controls did *ZylonTech* implement?**
  - A. Preventive control
  - B. Detective control
  - C. **Corrective control**

4. Did ZylonTech define the purpose of determining the monitoring interval in network monitoring accordingly?
- A. No, the purpose is to minimize the frequency of checks to reduce the monitoring effort required
  - B. No, the purpose is to optimize the balance between timely detection of issues and preventing system overload
  - C. **Yes, the purpose is to monitor network components as frequently as possible, regardless of the system load**
5. Which risk analysis technique did *ZylonTech* use?
- A. Qualitative risk analysis
  - B. **Semi-quantitative risk analysis**
  - C. Quantitative risk analysis

## Exam Security Policy

PECB is committed to protect the integrity of its exams and the overall examination process, and relies upon the ethical behavior of applicants, potential applicants, candidates and partners to maintain the confidentiality of PECB exams. This Policy aims to address unacceptable behavior and ensure fair treatment of all candidates.

Any disclosure of information about the content of PECB exams is a direct violation of this Policy and PECB's Code of Ethics. Consequently, candidates taking a PECB exam are required to sign an Exam Confidentiality and Non-Disclosure Agreement and must comply with the following:

1. The questions and answers of the exam materials are the exclusive and confidential property of PECB. Once candidates complete the submission of the exam to PECB, they will no longer have any access to the original exam or a copy of it.
2. Candidates are prohibited from revealing any information regarding the questions and answers of the exam or discuss such details with any other candidate or person.
3. Candidates are not allowed to take with themselves any materials related to the exam, out of the exam room.
4. Candidates are not allowed to copy or attempt to make copies (whether written, photocopied, or otherwise) of any exam materials, including, without limitation, any questions, answers, or screen images.
5. Candidates must not participate nor promote fraudulent exam-taking activities, such as:
  - Looking at another candidate's exam material or answer sheet
  - Giving or receiving any assistance from the invigilator, candidate, or anyone else
  - Using unauthorized reference guides, manuals, tools, etc., including using "brain dump" sites as they are not authorized by PECB

Once a candidate becomes aware or is already aware of the irregularities or violations of the points mentioned above, they are responsible for complying with those, otherwise if such irregularities were to happen, candidates will be reported directly to PECB or if they see such irregularities, they should immediately report to PECB.

Candidates are solely responsible for understanding and complying with PECB Exam Rules and Policies, Confidentiality and Non-Disclosure Agreement and Code of Ethics. Therefore, should a breach of one or more rules be identified, candidates will not receive any refunds. In addition, PECB has the right to deny the right to enter a PECB exam or to invite candidates for an exam retake if irregularities are identified during and after the grading process, depending on the severity of the case.

Any violation of the points mentioned above will cause PECB irreparable damage for which no monetary remedy can make up. Therefore, PECB can take the appropriate actions to remedy or prevent any unauthorized disclosure or misuse of exam materials, including obtaining an immediate injunction. PECB will take action against individuals that violate the rules and policies, including permanently banning them 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.

## 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.

Candidates that disagree with the results may request a re-evaluation by writing to [examination.team@pecb.com](mailto:examination.team@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, 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 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.

## SECTION III: CERTIFICATION PROCESS AND REQUIREMENTS

### PECB ISO/IEC 27035 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 27035 scheme have the following requirements:

Credential	Education	Exam	Professional experience	Incident manager project experience	Other requirements
PECB Certified ISO/IEC 27035 Provisional Incident Manager	At least secondary education	PECB Certified ISO/IEC 27035 Lead Incident Manager exam or equivalent	None	None	<a href="#">Signing the PECB Code of Ethics</a>
PECB Certified ISO/IEC 27035 Incident Manager			Two years: One year of work experience in information security incident management	Project activities: a total of 200 hours	
PECB Certified ISO/IEC 27035 Lead Incident Manager			Five years: Two years of work experience in information security incident management	Project activities: a total of 300 hours	
PECB Certified ISO/IEC 27035 Senior Lead Incident Manager			Ten years: Seven years of work experience in information security incident 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. Defining an incident management approach
2. Determining the incident management objectives and scope
3. Performing risk assessment
4. Developing an incident management program
5. Defining risk evaluation and risk acceptance criteria
6. Evaluating risk treatment options
7. Monitoring and reviewing the incident management program

## 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 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 account), including contact details of individuals who will be contacted to validate the candidates' professional experience. Candidates can submit their application in English, French, German, Spanish or Korean languages. They can choose to either pay online or be billed. For additional information, please contact [certification.team@pecb.com](mailto: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](#).

PECB provides support both in English and French.

## 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.

## 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 information security incident management 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.

## ISIM project experience

The candidate's ISIM project log will be checked to ensure that the candidate has the required number of implementation hours.

## **Evaluation of certification applications**

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



## SECTION IV: CERTIFICATION POLICIES

---

### Denial of certification

PECB can deny certification/certificate program if candidates:

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

Candidates whose certification/certificate program has been denied can file a complaint through the complaints and appeals procedure. For more detailed information, refer to [Complaint and Appeal Policy](#) section.

The application payment for the certification/certificate program is nonrefundable.

### Certification status options

#### Active

Means that your certification is in good standing and valid, and it is being maintained by fulfilling the PECB requirements regarding the CPD and AMF.

#### Suspended

PECB can temporarily suspend candidates' certification if they fail to meet the requirements. Other reasons for suspending certification include:

- 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.

#### Revoked

PECB can revoke (that is, to withdraw) the certification if the candidate fails to satisfy its requirements. In such cases, candidates are no longer allowed to represent themselves as PECB Certified Professionals.

Additional reasons for revoking certification can be if the candidates:

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

Candidates whose certification has been revoked can file a complaint through the complaints and appeals procedure. For more detailed information, refer to [Complaint and Appeal Policy](#) section.

## Other statuses

Besides being active, suspended, or revoked, a certification can be voluntarily withdrawn or designated as Emeritus. To learn more about these statuses and the permanent cessation status, go to [Certification Status Options](#).

## Upgrade and downgrade of credentials

### Upgrade of credentials

Professionals can upgrade their credentials as soon as they can demonstrate that they fulfill the requirements.

To apply for an upgrade, candidates need to log into their PECB account, visit the “My Certifications” tab, and click on “Upgrade.” 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. The holders of Master Certifications who fail to submit CPDs and pay AMFs will have their certifications revoked.*

## 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 (\$120). 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](mailto:certification.team@pecb.com) and pay the required fee.

## Complaint and Appeal Policy

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 candidates do not find the response satisfactory, they have the right to file an appeal.

For more information about the Complaint and Appeal Policy, click [here](#).

## 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 27035 Lead Incident 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<sup>3</sup> 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<sup>4</sup>. 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](#).

---

<sup>3</sup> 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.

<sup>4</sup> 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](mailto:examination.team@pecb.com)

**Certification:**

[certification.team@pecb.com](mailto:certification.team@pecb.com)

**Customer Service:**

[support@pecb.com](mailto: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](http://www.pecb.com)