


The logo for PECB, featuring the letters 'PECB' in a bold, white, sans-serif font. The letters are spaced out, with the 'E' and 'C' having a slight gap between them.

PECB

BEYOND RECOGNITION

A photograph of two business professionals, a woman in a dark suit and a man in a light suit, standing in a modern office hallway. They are looking at a tablet together. The background shows large glass windows and a modern building exterior.

Chief Information Security Officer (CISO)

Candidate Handbook

Table of Contents

SECTION I: INTRODUCTION	3
About PECB	3
The Value of PECB Certification.....	4
PECB Code of Ethics.....	5
Introduction to Chief Information Security Officer (CISO).....	6
SECTION II: EXAMINATION PREPARATION, RULES, AND POLICIES	7
Preparing for and scheduling the exam.....	7
Competency domains.....	8
Taking the exam.....	18
Exam Security Policy.....	22
Exam results.....	23
Exam Retake Policy.....	23
SECTION III: CERTIFICATION PROCESS AND REQUIREMENTS	24
PECB CISO credentials	24
Applying for certification	24
Professional experience	25
Professional references	25
Project experience	25
Evaluation of certification applications	25
SECTION IV: CERTIFICATION POLICIES	26
Denial of certification.....	26
Certification status options	26
Upgrade and downgrade of credentials	27
Renewing the certification.....	27
Closing a case	27
Complaint and Appeal Policy	27
SECTION V: GENERAL POLICIES	28
Exams and certifications from other accredited certification bodies	28
Non-discrimination and special accommodations	28
Behavior Policy.....	28
Refund Policy	28

SECTION I: INTRODUCTION

About PECB

PECB is a certification body that provides education¹, 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

¹ 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 Chief Information Security Officer (CISO)

As the digital landscape evolves, the security of organizational assets and information infrastructure has become crucial. Consequently, the Chief Information Security Officer (CISO) role has never been more pivotal. Organizations globally face numerous information security threats, and it is CISO's responsibility to navigate the complex environments, ensuring both security and compliance. This training course will provide participants with a comprehensive understanding of the strategies, technologies, and leadership skills essential for the CISO role.

This training course encompasses the latest risk assessment methodologies, governance frameworks, incident response strategies, and emerging threat landscape. It elaborates on the role of the CISO in managing security, taking proactive measures, creating dynamic strategies, and fostering a security awareness organizational culture. After successfully completing this training course, participants will be able to implement a holistic information security program and ensure compliance with security frameworks and regulations.

The "Chief Information Security Officer" certification demonstrates an individual has proficiency in establishing and leading an information security program. By acquiring this certification, individuals enhance their skills to tackle contemporary information security challenges and position themselves as leaders in the field.

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 who have the required experience and have passed the exam.

This document specifies the PECB Chief Information Security Officer 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.

.

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.

Application fees for examination and certification

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

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

The application fee for certification is \$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 CISO credential is a professional certification for individuals aiming to showcase their expertise in implementing and leading a comprehensive information security program.

The role of CISO encompasses a wide range of responsibilities, and therefore, requires a diverse skill set. While technical knowledge and expertise are critical, arguably the most important skill for a CISO to lead an information security program effectively is strategic leadership.

The CISO certification is intended for:

- Professionals actively involved in the management of information security
- Experienced CISOs seeking to enhance their knowledge, stay updated with the latest trends, and refine their leadership skills
- IT managers responsible for overseeing information security programs and assets
- Security professionals who aspire to advance into leadership roles, such as security architects or security analysts
- Professionals responsible for managing information security risk and compliance within organizations
- Executives, including CIOs, CEOs, and COOs, who play a crucial role in decision-making processes related to information security
- Professionals aiming for executive-level information security roles

The content of the exam is divided as follows:

- **Domain 1:** Fundamental concepts of information security
- **Domain 2:** The role of CISO in an information security program
- **Domain 3:** Selecting a security compliance program, risk management, and security architecture and design
- **Domain 4:** Operational aspects of information security controls, incident management, and change management
- **Domain 5:** Fostering an information security culture, monitoring, measuring, and improving an information security program

Domain 1: Fundamental concepts of information security

Main objective: Ensure that the candidate is able to interpret the fundamental concepts and principles of information security.

Competencies	Knowledge statements
<ol style="list-style-type: none"> 1. Ability to explain the main concepts of information security 2. Ability to explain confidentiality, integrity, and availability (the CIA triad) 3. Ability to explain disclosure, alteration, and denial (the DAD triad) 4. Ability to explain identification, authentication, authorization, and accountability (IAAA) security framework 5. Ability to identify and categorize different types of threats and vulnerabilities 6. Ability to recognize and mitigate common attack vendors 7. Ability to explain information security policies and procedures 8. Ability to classify security controls 9. Ability to identify types of malicious software and social engineering attacks 10. Ability to recognize the importance of physical security, network security, application security, cloud security, threat intelligence, and cryptography in protecting information assets 	<ol style="list-style-type: none"> 1. Knowledge of the main concepts and principles of information security 2. Knowledge of the CIA triad 3. Knowledge of the DAD triad 4. Knowledge of the identification, authentication, authorization, and accountability (IAAA) security framework 5. Knowledge of the various types of threats and vulnerabilities 6. Knowledge of the security policies and procedures 7. Knowledge of the information security risks 8. Knowledge of the type and function of security controls 9. Knowledge of various security standards and frameworks 10. Knowledge of malicious software and social engineering attacks 11. Knowledge of physical security, network security, application security, threat intelligence, and cryptography

Domain 2: The role of CISO in an information security program

Main objective: Ensure that the candidate is able to define, establish, manage, and improve an information security program, while successfully embodying the role of a CISO in aligning security imperatives with the organization’s objectives.

Competencies	Knowledge statements
1. Ability to define the role and responsibilities of a CISO within an organization	1. Knowledge of the core responsibilities of a CISO within an organization
2. Ability to engage and cooperate with other executives	2. Knowledge of the responsibilities of the CISO, CIO, CTO, and CPO
3. Ability to understand and compare the responsibilities of the CISO, CIO, CTO, and CPO	3. Knowledge of key leadership traits necessary for the CISO role
4. Ability to address and overcome common challenges encountered by a CISO	4. Knowledge of effective communication strategies
5. Ability to obtain leadership qualities necessary for the role of the CISO	5. Knowledge of potential challenges that a CISO might face
6. Ability to adhere to ethical standards	6. Knowledge of ethical considerations and standards pertaining to the CISO role
7. Ability to define clear and relevant information security objectives aligned with organizational goals	7. Knowledge of the information security program
8. Ability to establish a comprehensive information security program	8. Knowledge of information security objectives
9. Ability to design and implement an effective organizational structure for the information security program	9. Knowledge of organizational structures that support information security
10. Ability to define the scope of an information security program	10. Knowledge of the scope of an information security program
11. Ability to allocate and manage resources effectively for the information security program	11. Knowledge of the resources, tools, and personnel essential for a robust information security program
12. Ability to develop and implement proactive information security strategies	12. Knowledge of strategic planning and implementation in the context of information security

Domain 3: Selecting a security compliance program, risk management, and security architecture and design

Main objective: Ensure that the candidate is able to interpret, develop, and maintain an organization’s compliance program, manage risks effectively, analyze the existing security controls, and design robust security architectures by selecting a suitable security architecture and design framework.

Competencies	Knowledge statements
1. Ability to develop, implement, and monitor a compliance program based on the organization’s specific needs	1. Knowledge of key regulatory frameworks and standards applicable to the industry
2. Ability to ensure compliance to industry-specific regulations and standards	2. Knowledge of various bodies and their specific role related to information security
3. Ability to regularly review and update the compliance program	3. Knowledge of the core functions, categories, and subcategories outlined in NIST Cybersecurity framework
4. Ability to educate and train employees on compliance requirements and best practices	4. Knowledge of the implementation tiers and how they support the risk management process
5. Ability to coordinate with legal and other departments to ensure comprehensive compliance	5. Knowledge of the objectives and requirements of the NIS 2 Directive
6. Ability to identify, evaluate, and prioritize risks within the organizational context	6. Knowledge of the methods to implement and monitor the effectiveness of CIS controls
7. Ability to evaluate the effectiveness of security controls	7. Knowledge of COBIT’s framework structure, including its governance components and management practices
8. Ability to identify gaps in existing security controls	8. Knowledge of ISO/IEC 27001 requirements for an information security management system (ISMS)
9. Ability to examine information security capabilities in key areas such as risk and resilience, intelligence and awareness operational security, physical security, and supply chain management	9. Knowledge of ITIL’s five stages, PCI DSS, CSA STAR Program, GDPR, and HIPPA requirements
10. Ability to use gap analysis in identifying and evaluating existing information security capabilities	10. Knowledge of an information security policy and its role in guiding organizational behavior and ensuring security compliance
11. Ability to develop and implement risk mitigation strategies	11. Knowledge of information security capabilities
12. Ability to identify, analyze, and evaluate risks	12. Knowledge of supply chain management capabilities
13. Ability to select information risk treatment options	13. Knowledge of risk assessment methodologies
14. Ability to create a risk treatment plan	14. Knowledge of risk mitigation techniques and tools
15. Ability to identify risk management tools and software that can be utilized to automate processes	15. Knowledge of the principles of continuous risk management monitoring

-
- | | |
|--|--|
| 16. Ability to connect risk communication to business objectives | 16. Knowledge of risk identification techniques, risk analysis methods, and risk evaluation criteria |
| 17. Ability to establish a risk communication plan with internal and external parties | 17. Knowledge of risk treatment process on addressing, mitigating, transferring, or accepting risks |
| 18. Ability to record, report, monitor, and review risks | 18. Knowledge of effective risk communication strategies |
| 19. Ability to explain security architecture and design | 19. Knowledge of monitoring and review mechanisms for improving the risk management process |
| 20. Ability to select a security architecture framework and align it with business resources | 20. Knowledge of frameworks and methodologies that guide effective risk management |
| 21. Ability to explain zero-trust principle architecture | 21. Knowledge of principles and structures of organizational security architectures and their application |
| 22. Ability to select security architecture design component | 22. Knowledge of Zachman, SABSA, TOGAF, and OSA security architecture framework |
| 23. Ability to explain the difference between information security systems and infrastructure security | 23. Knowledge of zero-trust principle |
| | 24. Knowledge of security architecture components such as NFV, SASE, SSE, overlay network services, and multi-cloud architecture |

Domain 4: Operational aspects of information security controls, incident management, and change management

Main objective: Ensure that the candidate is able to select, design, implement, and evaluate information security controls, manage security incidents, and oversee the IT change management process.

Competencies	Knowledge statements
<ol style="list-style-type: none"> 1. Ability to classify, select, and implement effective information security controls 2. Ability to document established information security controls comprehensively 3. Ability to implement controls specifically for threat intelligence and operational security 4. Ability to incorporate physical security within the broader framework of information security controls 5. Ability to design and implement controls for supply chain management 6. Ability to identify emerging technologies relevant for CISOs 7. Ability to test and evaluate the effectiveness of the established security controls 8. Ability to effectively manage information security incidents 9. Ability to monitor, document, and report security incidents 10. Ability to design and implement incident response training and security awareness programs 11. Ability to develop business continuity plans 12. Ability to draft and execute a disaster recovery plan 13. Ability to explain and implement IT change management processes 14. Ability to categorize and prioritize IT changes based on their impact and relevance 15. Ability to establish change management controls to oversee and ensure successful transitions 16. Ability to recognize and carry out roles and responsibilities in IT change management, including the role of the CISO 	<ol style="list-style-type: none"> 1. Knowledge of various classification of information security controls 2. Knowledge of the processes and best practices for the selection and design of controls 3. Knowledge of documentation standards for information security controls 4. Knowledge of controls specific to threat intelligence and their applications 5. Knowledge of the key components of operational and physical security controls 6. Knowledge of supply chain management controls and their importance in ensuring end-to-end encryption 7. Knowledge of emerging technologies and their implications for CISOs 8. Knowledge of testing protocols and evaluation metrics for security controls 9. Knowledge of the lifecycle of information security incident management 10. Knowledge of monitoring techniques and documentation standards for security incidents 11. Knowledge of designing incident response training modules and the importance of security awareness programs 12. Knowledge of business continuity planning 13. Knowledge of disaster recovery planning 14. Knowledge of IT change management and its importance 15. Knowledge of three categories of IT changes 16. Knowledge of change management controls mechanisms 17. Knowledge of the step-by-step procedure for efficient IT change management

18. Knowledge of the various roles and responsibilities within the IT change management
19. Knowledge of the role of the CISO in overseeing and guiding IT change management

Domain 5: Fostering an information security culture, monitoring, measuring, and improving an information security program

Main objective: Ensure that the candidate is able to develop and evaluate effective training and awareness programs, establish robust monitoring process, and comprehend the importance of assurance programs.

Competencies	Knowledge statements
1. Ability to establish and improve a training and awareness program	1. Knowledge of the key components of awareness and training programs
2. Ability to carry out the responsibilities of the CISO in awareness and training program	2. Knowledge of the CISO's role in guiding and directing training and awareness activities
3. Ability to allocate funding effectively for the training and awareness program	3. Knowledge of the funding needs and allocations strategies for training programs
4. Ability to design competence development program structures	4. Knowledge of different structures and types of competence development programs
5. Ability to select and implement effective training methods	5. Knowledge of different training methods and their effectiveness
6. Ability to adapt and explain cultural change within the organization	6. Knowledge of the mechanisms for cultural change within organizations
7. Ability to evaluate the outcomes of training sessions	7. Knowledge of evaluation techniques for training outcomes
8. Ability to implement continuous monitoring practices for information security	8. Knowledge of information security continuous monitoring (ISCM) and its importance
9. Ability to assess the overall effectiveness of the information security program	9. Knowledge of assessment techniques for the evaluation of the security program
10. Ability to define and use relevant security metrics and key performance indicators (KPIs)	10. Knowledge of designing relevant metrics and KPIs for information security
11. Ability to evaluate performance and review KPIs	11. Knowledge of performance evaluation and KPI reviews
12. Ability to effectively report measurement results	12. Knowledge of effective reporting mechanisms for measurement results
13. Ability to explain and implement an assurance program	13. Knowledge of the foundations and significance of an assurance program
14. Ability to test, review, and report on information security procedures	14. Knowledge of techniques to test and review information security procedures and report results
15. Ability to conduct comprehensive security audits	15. Knowledge of the security auditing procedures
16. Ability to explain the importance of penetration testing and analyze its outcomes	16. Knowledge of risk assessment methodologies and their impact on security
17. Ability to incorporate vulnerability scanning activities in the organization's assurance program	17. Knowledge of the principles and practices of penetration testing
18. Ability to assess the overall security posture of the organization	18. Knowledge of vulnerability scanning tools and methodologies

19. Ability to guide and oversee internal and external audits

19. Knowledge of the security posture assessments

20. Knowledge of internal and external audit processes

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 concepts of information security	9	11.25	X	
	The role of CISO in an information security program	20	25	X	
	Selecting a security compliance program, risk management, and security architecture and design	20	25	X	
	Operational aspects of information security controls, incident management, and change management	21	26.25		X
	Fostering an information security culture, monitoring, measuring, and improving an information security program	10	12.5		X
Total		80	100%		
Number of questions per level of understanding			49	31	
% of the exam devoted to each level of understanding (cognitive/taxonomy)			61.25%	38.75%	

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

After successfully passing the exam, candidates will be able to apply for obtaining the “PECB Chief Information Security Officer” 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:

- 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 or go to the [List of PECB Exams](#).

Sample exam questions

Zootron, a leading German tech firm, recently underwent a structural transformation in its IT Department. Recognizing the rising cyber threats, they established a dedicated position for a Chief Information Security Officer (CISO). Jenah, with a background in both technology and management, was appointed.

In the first month, Jenah reviewed the fundamentals of information security. She recognized gaps in managing cybersecurity risks and noncompliance with privacy and security standards and identified risks through a detailed assessment.

By the third month, Jenah initiated an awareness and training program. She advocated for fostering a positive work culture, boosted productivity, and secured funding for training, ensuring a blend of methods to accommodate all learners. She also stated the need for continuous monitoring and implemented practices to manage risks, monitor anomalies, assess vulnerabilities, and recognize threats. She used tools that provided insights on various security measures in order to evaluate the effectiveness of *Zootron's* information security program.

After six months, Jenah proposed the initiation of an assurance program. This included a thorough security audit which aimed to evaluate the company's network, identify weaknesses, and ensure compliance with the applicable standards and regulations. The audits were conducted by *Zootron's* professionals who were also tasked with advising the organization on the improvement measures. Moreover, Jenah proposed the usage of tools to detect security potential risk exposures in *Zootron's* system, as well as simulated hacking attacks to identify the root causes of cybersecurity attacks. This initiative would help *Zootron* to identify weak spots in the organization's existing capabilities for protecting information security technology components, services, and software applications as well as cloud-based systems.

Based on the scenario above, answer the following questions:

- 1. Based on the information Jenah collected during the first month, which compliance frameworks should the company implement?**
 - A. COBIT and HIPAA
 - B. **NIST CSF and GDPR**
 - C. CIS controls and CSA STAR program
- 2. When Jenah initiated an awareness and training program, what did she emphasize?**
 - A. Adhering to strict security protocols
 - B. The collaboration between departments
 - C. **The cultural transformation**
- 3. How did Jenah ensure the effectiveness of *Zootron's* information security program?**
 - A. **By implementing ISCM practices and KPI metrics**
 - B. By focusing on training awareness programs only
 - C. By conducting an external audit

4. Based on the scenario above, Jenah proposed simulated hacking attacks within Zootron to identify the root cause of the potential attacks. Is this acceptable?
 - A. **Yes, attack simulations can be done by authorized users within the organization**
 - B. No, attack simulations are unethical and cannot be conducted by individuals within the organization
 - C. No, Jenah should have waited for real attacks to occur to identify their root cause

5. Which information security capability of Zootron did Jenah's assurance program initiative aim to improve?
 - A. Supply chain management
 - B. **Operational security**
 - C. Threat intelligence

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 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 CISO 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 CISO scheme have the following requirements:

Credential	Exam	Professional experience	Information security project experience	Other requirements
PECB Information Security Officer	PECB Chief Information Security Officer Exam	None	None	Signing the PECB Code of Ethics
PECB Chief Information Security Officer		Five years: Two years of work experience in information security	Project activities: a total of 300 hours	

Effective information security practices for a CISO should adhere to best implementation strategies, encompassing the following key aspects:

1. Developing secure business and communication practices
2. Identifying security objectives and metrics
3. Ensuring that the company is in regulatory compliance with relevant bodies' rules
4. Enforcing adherence to information security best practices
5. Managing the incident response team
6. Conducting electronic discovery and digital forensic investigations
7. Conducting employee security awareness training

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.

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 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.

Project experience

The candidate's information security project log will be checked to ensure that the candidate has the required number of project activity 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 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.

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 accommodations³ 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 arrangements⁴. 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