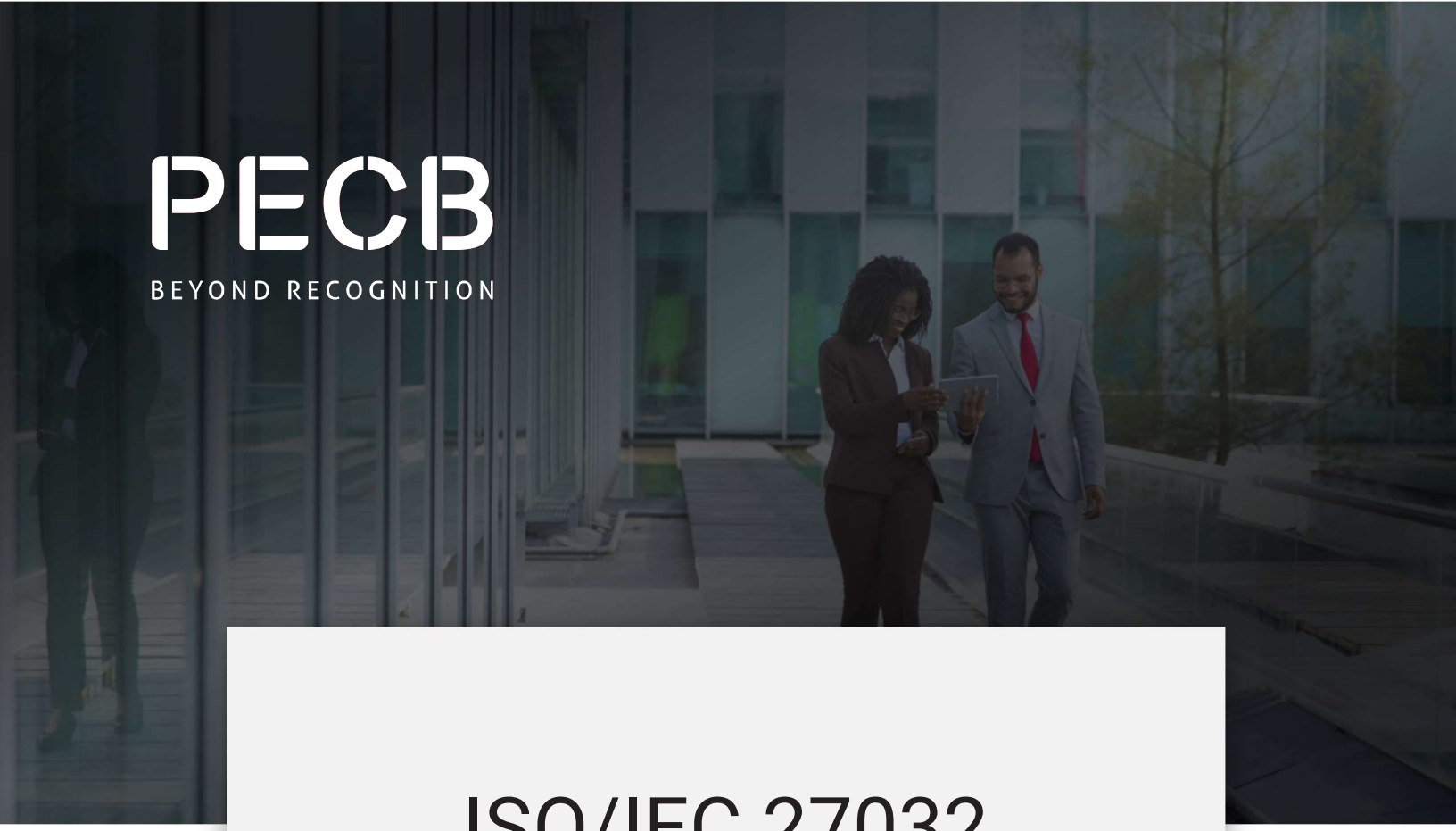

PECB

BEYOND RECOGNITION

ISO/IEC 27032 LEAD CYBERSECURITY MANAGER

Candidate Handbook

PECB

Table of Contents

PECB

SECTION I: INTRODUCTION

About PECB

PECB is a certification body that provides education[1], 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 ISO/IEC 27032 Lead Cybersecurity Manager

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

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

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

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 27032 Lead Cybersecurity 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.

PECB

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: $1000[2]
- 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 objective of the "PECB ISO/IEC 27032 Cybersecurity Manager" exam is to ensure that the candidate has acquired the necessary expertise to support an organization in establishing and managing a cybersecurity program based on ISO/IEC 27032 and NIST Cybersecurity Framework.

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

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

The content of the exam is divided as follows:

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

Domain 1: Fundamental principles and concepts of cybersecurity

Main objective: Ensure that the candidate understands and is able to interpret the principles and concepts of ISO/IEC 27032.

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

Domain 2: Roles and responsibilities of stakeholders

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

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

Domain 3: Cybersecurity risk management

Main objective: Ensure that the candidate can implement and manage a cybersecurity risk management program.

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

Domain 4: Attack mechanisms and cybersecurity controls

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

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

Domain 5: Information sharing and coordination

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

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

Domain 6: Integrating the cybersecurity program in business continuity management

Main objective: Ensure that the candidate is able to integrate the cybersecurity program in the business continuity management plan of the organization.

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

Domain 7: Cybersecurity management and performance measurement

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

Competencies	Knowledge statements
1. Ability to establish an incident management process based on best practices	1. Knowledge of the principles, elements, and phases of the ICT readiness for business continuity (IRBC)
2. Ability to reduce the possible impact of cybersecurity incidents on the operations of the organization	2. Knowledge of a cybersecurity incident management process
3. Ability to set cybersecurity incident management objectives	3. Knowledge of the cybersecurity incident prevention process
4. Ability to manage cybersecurity incidents by conducting several phases such as planning and preparation, detection and reporting, assessment and decision, response, and lessons learned	4. Knowledge of the ways to reduce the direct and indirect costs caused by cybersecurity incidents
5. Ability to prepare and plan the operation of an effective and efficient cybersecurity incident management scheme	5. Knowledge of the characteristics and main processes of a cybersecurity incident management scheme
6. Ability to gather evidence during incidents based on a digital forensics policy	6. Knowledge of the roles and responsibilities of the key actors during the implementation of a cybersecurity incident management scheme
7. Ability to identify the lessons that can be learned from the occurrence of cybersecurity incidents and other incidents	7. Knowledge of digital forensics and their integration into cybersecurity incident response
8. Ability to perform testing on technical systems to ensure their reliability	8. Knowledge of the cybersecurity testing techniques
9. Ability to determine the stages of testing, determine testing techniques, prepare the test and documentation, and conduct post-testing activities	9. Knowledge of performance measurement methods
10. Ability to measure the performance of the cybersecurity program, determine measurement objectives, define what needs to be monitored and measured, and establish performance indicators	10. Knowledge of the monitoring, measuring, analyzing, and evaluating methods of the cybersecurity program
11. Ability to continually improve the cybersecurity program	11. Knowledge of activities that continually improve the cybersecurity program

Based on the above-mentioned domains and their relevance, the exam contains 12 questions, as summarized in the table below:

			Level of understanding (Cognitive/Taxonomy) required					
		Points per question	Questions that measure comprehension, application, and analysis	Questions that measure evaluation	Number of questions per competency domain	% of the exam devoted to each competency domain	Number of points per competency domain	% of points per competency domain
Competency domains	Fundamental principles and concepts of cybersecurity	5	X		1	8.33	5	6.67
	Roles and responsibilities of stakeholders	5	X		1	8.33	5	6.67
	Cybersecurity risk management	5	X		2	16.67	15	20
		10		X				
	Attack mechanisms and cybersecurity controls	5	X		4	33.33	30	40
		5	X					
		10		X				
		10		X				
	Information sharing and coordination	5	X		1	8.33	5	6.67
	Integrating cybersecurity program in business continuity management	5	X		1	8.33	5	6.67
	Cybersecurity incident management and performance measurement	5		X	2	16.67	10	13.33
		5		X				
	Total points	75						
	Number of questions per level of understanding		7	6				
	% of the exam devoted to each level of understanding (cognitive/taxonomy)		58.3	41.7				

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 27032 Lead Cybersecurity 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 essay-type questions. Essay-type questions are used to determine and evaluate whether a candidate can clearly answer questions related to the defined competency domains. Additionally, problem-solving techniques and arguments that are supported with reasoning and evidence will also be evaluated. The exam aims to evaluate candidates' comprehension, analytical skills, and applied knowledge. Therefore, candidates are required to provide logical and convincing answers and explanations in order to demonstrate that they have understood the content and the main concepts of the competency domains.

This is an open-book exam. The candidate is allowed to use the following reference materials:
- A hard copy of the ISO/IEC 27032 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 or go to the List of PECB Exams.

Sample exam questions

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

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

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

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

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

Possible answer:

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

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

Possible answer:
To achieve these objectives, organizations should:

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

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.

PECB

SECTION III: CERTIFICATION PROCESS AND REQUIREMENTS

PECB ISO/IEC 27032 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 27032 scheme have the following requirements:

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

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

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

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 cybersecurity program experience, as well as their current and previous work history. Professional references of persons who fall under the candidate's supervision or are their relatives are not valid.

Cybersecurity program experience

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

Evaluation of certification applications

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

time frame, the Certification Department will validate the application based on the initial information provided, which may lead to the candidates' credential downgrade.

PECB

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 (e.g., ISO/IEC 27001 Lead Auditor certification).

Non-discrimination and special accommodations

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

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

Behavior Policy

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

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

Refund Policy

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

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

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

Address:

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

Tel./Fax:

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

Emails:

Examination:
examination.team@pecb.com

Certification:
certification.team@pecb.com

Customer Service:
customer@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