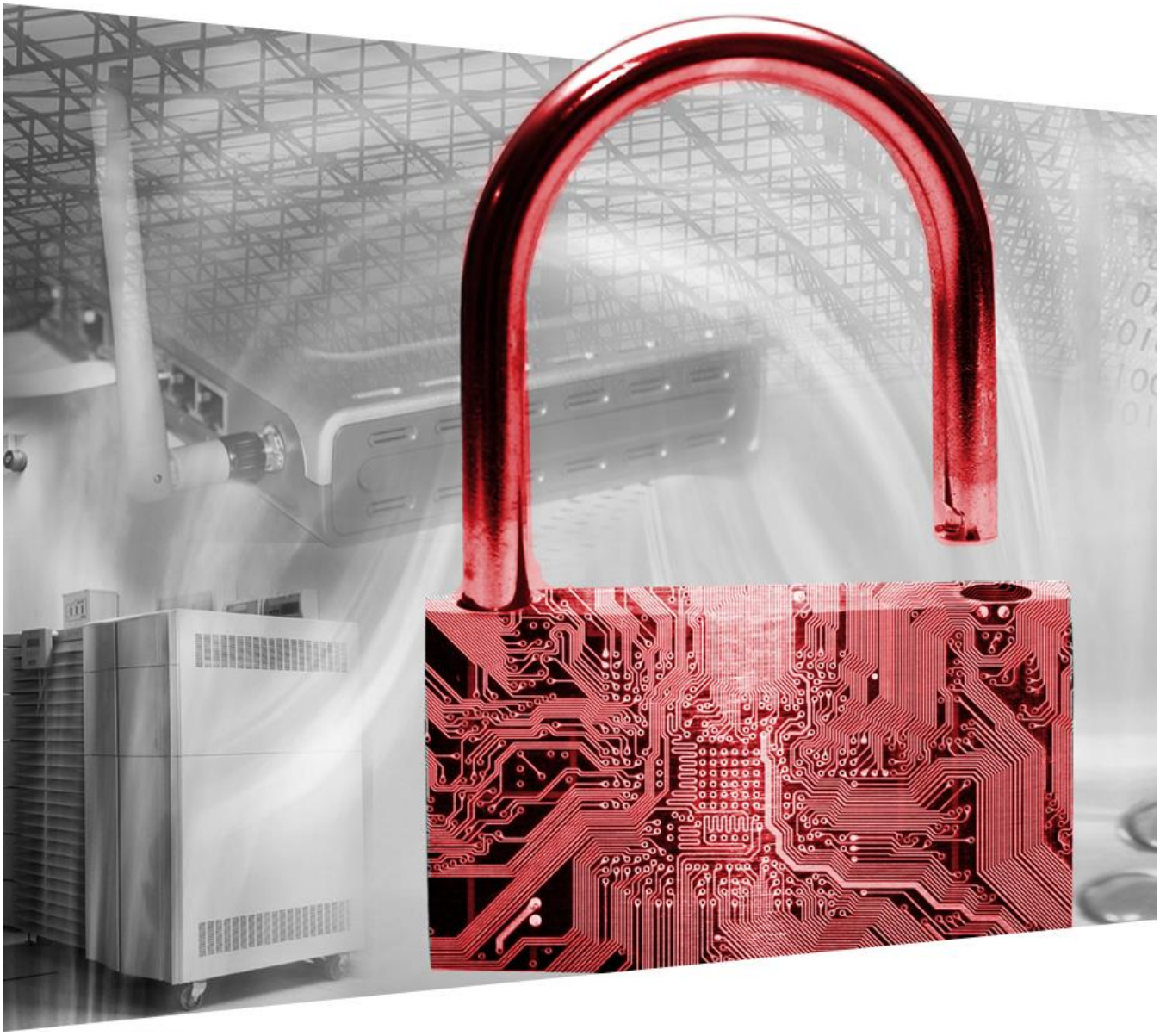
PECB

When Recognition Matters



EXAM PREPARATION GUIDE

ISO/IEC 27032 Lead Cybersecurity Manager

The objective of the "PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager" examination is to ensure that the candidate has the knowledge and competence needed to support an organization in implementing and managing a Cybersecurity Program based on ISO/IEC 27032 and NIST Cybersecurity Framework.

The target population for this examination is:

- Cybersecurity professionals
- Information security professionals
- Project managers wanting to manage the Cybersecurity Program
- Technical experts wanting to prepare themselves for cybersecurity functions
- Persons responsible to develop the Cybersecurity Program

The exam content covers the following domains:

- Domain 1: Fundamental concepts in 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 Cybersecurity Program in business continuity management
- Domain 7: Cybersecurity incident management, and performance measurement

The content of the exam is divided as follows:

Domain 1: Fundamental concepts in cybersecurity

Main objective: To ensure that the candidate can understand, interpret and illustrate the main cybersecurity guidelines and concepts related to the management of a Cybersecurity Program based on ISO/IEC 27032 and NIST Cybersecurity Framework.

Competencies	Knowledge statements
1. Understand and explain the structure of ISO/IEC 27032 and NIST Cybersecurity Framework. 2. Ability to identify, analyze and evaluate the guidance coming from ISO/IEC 27032 and other cybersecurity frameworks. 3. Ability to explain and illustrate the main concepts in cybersecurity. 4. Ability to distinguish and explain the difference between information security and cybersecurity. 5. Ability to distinguish relationship and main differences between ISO/IEC 27032 and other related standards.	1. Knowledge of management principles for implementing a Cybersecurity Program. 2. Knowledge of the main standards and frameworks in cybersecurity. 3. Knowledge of the different sources of cybersecurity frameworks for an organization: laws, regulations, international and industry standards, contracts, market practices, internal policies. 4. Knowledge of the main cybersecurity concepts and terminology. 5. Knowledge of the relationship and the main differences between ISO/IEC 27032 and other related standards.

Domain 2: Roles and responsibilities of stakeholders

Main objective: To ensure that the candidate can understand, interpret and illustrate the roles and responsibilities of stakeholders in cybersecurity

Competencies	Knowledge statements
1. Understand the importance of assigning and communicating cybersecurity roles and responsibilities. 2. Ability to explain the role of stakeholders in enhancing cybersecurity. 3. Understand the roles and responsibilities of providers and consumers as the main stakeholders in cybersecurity. 4. Ability to distinguish the roles of individuals and roles of organization in the cyberspace. 5. Understand leaderships' role in defining the roles and responsibilities of involved parties.	1. Knowledge of the responsibilities and competencies of the Cybersecurity Program Manager. 2. Knowledge of the consumers' role and their impact on cyberspace. 3. Knowledge of roles of individuals in cyberspace. 4. Knowledge of government and law enforcement agencies' role and their impact on cyberspace.

Domain 3: Cybersecurity Risk Management

Main objective: To ensure that the candidate can implement a methodology of risk assessment adapted to the needs of the organization.

Competencies

1. Understand the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
2. Ability to explain and illustrate cybersecurity risk management.
3. Ability to define goals and objectives of cybersecurity risk management.
4. Ability to understand and distinguish the overall security risk and cybersecurity risk.
5. Understand and explain risk management framework based on ISO 27005.

Knowledge statements

1. Knowledge of the concept of risk and its application in cybersecurity.
2. Knowledge of risk analysis methods.
3. Knowledge on managing cyber risks to an acceptable level.
4. Knowledge on how to achieve goals and objectives of cybersecurity risk management.
5. Knowledge of management considerations regarding cybersecurity risk management.
6. Knowledge of the implementation of risk management frameworks.

Domain 4: Attack mechanisms and cybersecurity controls

Main objective: To ensure that the candidate can understand and explain top cyber-threats and their mitigation vectors, and implement key cybersecurity controls as guided in ISO/IEC 27032.

Competencies

1. Understand the importance of the implementation of cybersecurity controls in support of security requirements.
2. Ability to distinguish the four types of cybersecurity controls as indicated in ISO/IEC 27032.
3. Ability to implement key cybersecurity controls as guided in ISO/IEC 27032.
4. Understand and explain top cyber-threats and their mitigation vectors.

Knowledge statements

1. Knowledge of application level controls and their implementation.
2. Knowledge of sever protection controls and operation of secure servers.
3. Knowledge of end user controls and how they can protect the system against exploits and attacks.
4. Knowledge of controls against social engineering attacks and their implementation.
5. Knowledge of attack mechanisms such as malware, botnets, denial-of-service, phishing, spam, exploit kits, data breaches, identity theft, ransomware etc.

Domain 5: Information sharing and coordination

Main objective: To ensure that the candidate can establish an information sharing and coordination framework based on the ISO/IEC 27032

Competencies

1. Ability to understand and explain the importance and the benefits of information sharing and coordination framework in cybersecurity.
2. Ability to determine and implement the required methods and processes for information sharing and coordination framework.
3. Ability to understand, analyze the needs and provide guidance on the attribution of roles and responsibilities in the context of the implementation and management of an information sharing and coordination framework.
4. Ability to define and write policies and procedures regarding information - sharing and coordination.
5. Ability to conduct regular testing and periodic reviews.
6. Ability to prepare for the operation; collate contact list; and conduct awareness and training workshops to prepare stakeholders for the establishment of an information sharing and coordination framework.

Knowledge statements

1. Knowledge on establishing an information sharing and coordination framework that would be beneficial to the community.
2. Knowledge of the roles and responsibilities of the key actors during the implementation of an information sharing and coordination framework.
3. Knowledge of techniques and best practices writing policies, procedures and other types of documents.
4. Knowledge of the categorization and classification of information that is collected, kept safe or distributed via information sharing and coordination framework.
5. Knowledge on developing and implementing methods and processes to ensure effectiveness, efficiency, and reliability of execution for the information sharing and coordination framework.
6. Knowledge on how to prepare for the operation of the information sharing and coordination framework and knowledge on the content of contact lists.

Domain 6: Integrating Cybersecurity Program in Business Continuity Management

Main objective: To ensure that the candidate can implement a framework and process to enable the business continuity management of the organization's critical processes and activities.

Competencies

1. Ability to understand what business continuity is in the context of cybersecurity.
2. Understand what are the objectives and benefits of integrating business continuity within the cybersecurity program.
3. Ability to define a plan format and structure for cybersecurity continuity.
4. Ability to determine whether the continuity of cybersecurity should be integrated within the business continuity management process or within the disaster recovery management process.
5. Ability to understand and explain the concept of critical activities in cybersecurity continuity context.
6. Ability to understand technical approaches that are applicable for improving cybersecurity continuity.

Knowledge statements

1. Knowledge of business continuity management.
2. Knowledge of business continuity objectives and benefits regarding cybersecurity.
3. Knowledge of the principles of business continuity as indicated in ISO 27031.
4. Knowledge of the concept of critical activities in cybersecurity continuity.
5. Knowledge of the recovery plan and its objectives.
6. Knowledge of technical approaches for improving cybersecurity continuity.

Domain 7: Cybersecurity incident management, and performance measurement

Main objective: To ensure that cybersecurity events are detected and identified and that the candidate can evaluate the effectiveness of the implemented processes and procedures within the cybersecurity program

Competencies

1. Ability to define and implement an incident management process based on the best practices.
2. Ability to reduce the possible impact of cybersecurity incidents on the operations of the organization.
3. Ability to explain and illustrate cybersecurity incident management objectives.
4. Ability to prepare and plan the operation of an effective and efficient cybersecurity incident management scheme.
5. Ability to gather evidence during incidents based on forensics policy.
6. Ability to perform testing on technical systems to ensure their reliability.
7. Ability to determine the frequency and objectives of performance measurement.

Knowledge statements

1. Knowledge of cybersecurity incident management.
2. Knowledge on how to avoid cybersecurity incidents before they occur.
3. Knowledge on how to reduce the direct and indirect costs caused by cybersecurity incidents.
4. Knowledge of the characteristics and main processes of a cybersecurity incident management scheme.
5. Knowledge of the roles and responsibilities of the key actors during the implementation of a cybersecurity incident management scheme.
6. Knowledge of digital forensics and their integration into cybersecurity incident response.
7. Knowledge of security testing methods.
8. Knowledge of performance measurement methods.

Based on these 7 domains and their relevance, 150 questions are included in the exam. The passing score is established at **70%** (105/150).

			Level of Understanding (Cognitive/Taxonomy) Required					
		Points per Question	Questions that measure Comprehension, Application and Analysis	Questions that measure Synthesis and Evaluation	Number of Questions per competency domain	% of test devoted to each competency domain	Number of Points per competency domain	% of Points Competency domain
Content Area/Competence Domains	Fundamental concepts in cybersecurity	1	x		22	14.67	22	14.67
	Roles and responsibilities of stakeholders	1	x		18	12	18	12
	Cybersecurity Risk Management	1	x		17	11.33	17	11.33
	Attack mechanisms and cybersecurity controls	1		x	40	26.67	40	26.67
	Information sharing and coordination	1		x	21	14	21	14
	Integrating Cybersecurity Program in Business Continuity Management	1	x		10	6.67	10	6.67
	Cybersecurity incident management, and performance measurement	1		x	22	14.67	22	14.67
Total points		150						
Number of questions per level of understanding			67	83				
% of test devoted to each level of understanding (cognitive/taxonomy)			44.67	55.33				

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

TAKE A CERTIFICATION EXAM

You are required to follow the PECB Online Examination Rules and Policies specified below when taking the exam:

- Log In to PECB EXAMS online software 30 minutes before the beginning of the exam
- Have your ID card with you
- Have an External Camera ready (mandatory)
- Make sure to have a good Internet Connection
- Do not leave the testing area during the exam
- Do not be accompanied by anyone during the exam
- You are not allowed to eat, smoke, or drink except for water during the exam
- You are not allowed during the exam to consult, read aloud, or have any paper, document, book with you in the exam room

For further assistance please find below the link to the PECB EXAMS User Manual which explains in detail how to use the PECB EXAMS online application: https://pecb.com/help/index.php/manual/probo-user-manuals/

The exam duration is three (3) hours.

The questions are multiple choice questions. This type of format was chosen because it measures different levels of studying, and has resulted to be an effective assessment tool. The multiple-choice exam can be used to evaluate a candidate's understanding on many subjects, including both simple and complicated concepts. First and foremost, multiple-choice exam will not commonly demonstrate if the candidate's response is right or wrong, additionally it will demonstrate continuance of the learning process. Because of this particularity, the exam is not "open book" and does not measure the recall of data or information. This type of examination can be adapted to the measurement of a wide range of learning objectives including: reasoning, problem solving, exercising judgement, making inferences and demonstrating knowledge of facts through analysis and interpretation of information. At the end of this document, you will find sample exam questions and their possible answers.

The use of electronic devices, such as laptops, cell phones, etc., is not allowed.

All attempts to copy, collude or otherwise cheat during the exam will automatically lead to the exam's failure.

PECB exams are available in English. For availability of the exam in a language other than English, please contact examination@pecb.com

RECEIVE YOUR EXAM RESULTS

Results will be communicated instantly after taking the exam. The results will include the exact grade of the candidate shown in percentage.

Candidates who successfully complete the examination will be able to apply for a certified scheme.

In the case of a failure, the results will be accompanied with the list of domains in which the candidate had a low grade, to provide guidance for exams' retake preparation.

Candidates who disagree with the exam results may file a complaint. For more information, please refer to www.pecb.com

EXAM RETAKE POLICY

There is no limitation on how many times a candidate can retake the same exam. However, there are some limitations in terms of allowed time-frame in between exams.

When candidates fail the examination, they are only allowed to retake the examination once within 12 months after the first attempt. If second examination is unsuccessful, candidates will be allowed to retake the exam only after 1 year (12 months). Retake fee applies.

Only candidates, who have completed a full PECB training but fail the written exam, are eligible to retake the exam for free, under one condition:

"A candidate can only retake the exam once and this retake must occur within 12 months from the initial exam's date."

When candidates fail the same examination for the second time, their file is automatically closed for 1 year.

CLOSING FILES

Closing a file is equivalent to rejecting a candidate's application. As a result, when candidates request that their file be reopened, PECB will no longer be bound by the conditions, standards, policies, candidate handbook or exam preparation guide that were in effect before their file was closed.

Candidates who want to request that their file be reopened must do so in writing, and pay the required fees.

EXAMINATION SECURITY

A significant component of a successful and respected professional certification credential is maintaining the security and confidentiality of the examination. PECB relies upon the ethical behaviour of certificate holders and applicants to maintain the security and confidentiality of PECB examinations. When someone who holds PECB credentials reveals information about PECB examination content, they violate the PECB Code of Ethics. PECB will take actions against individuals who violate PECB Policies and the Code of Ethics. Actions taken may include permanently barring individuals from pursuing PECB credentials and revoking certifications from those who have been awarded the credential. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

SAMPLE EXAM QUESTIONS AND POSSIBLE ANSWERS

1. The inclusion of billion machines such as: tablets, smart phones, ATM machines, security installation, control systems and so on is called:

    a. Cyberspace
    b. The virtual-space
    c. Internet of Everything

2. Preservation of confidentiality, integrity and availability of information in the cyberspace is the definition of:

    a. Information Security
    b. Cybersecurity
    c. Cyber incident response

3. In the cyberspace the term “stakeholders” refers to:

    a. Hackers and hacktivists
    b. Consumers and providers
    c. Crackers and spammers

4. In order to have an effective risk management program all risks must be:

    a. Transferred
    b. Eliminated
    c. Identified

5. Which of the following is an example of risk sharing?

    a. Deciding not to start or continue with the activity that gives rise to the risk
    b. Taking or increasing risk in order to pursue an opportunity
    c. Allocating the risk to another party or parties