PECB BEYOND RECOGNITION

Exam Preparation Guide

ISO/IEC 27032 Lead Cybersecurity Manager

GENERAL

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 the NIST Cybersecurity Framework.

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

- Cybersecurity professionals
- Information security professionals
- Project managers who want to develop their competencies in Cybersecurity Program Management
- Technical experts who want to prepare themselves for cybersecurity functions
- Individuals responsible to develop a Cybersecurity Program in an organization

The exam covers the following competency domains:

Domain 1: Fundamental 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

The content of the exam is divided as follows:

Domain 1: Fundamental concepts of Cybersecurity **Main objective:** Ensure that the candidate understands, and is able to interpret and illustrate the main cybersecurity guidelines and concepts based on ISO/IEC 27032 and the NIST Cybersecurity Framework	
Competencies	**Knowledge statements**
1. Ability to 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 of Cybersecurity 4. Ability to explain and illustrate the main concepts of Cybersecurity	1. Ability to explain and illustrate the main concepts of Cybersecurity 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 5. Knowledge of the Information Security concepts 6. 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: Ensure that the candidate can understand, interpret and illustrate the roles and responsibilities of stakeholders in cybersecurity

Competencies	Knowledge statements
1. Ability to understand the importance of assigning and communicating cybersecurity roles and responsibilities 2. Ability to explain the role of stakeholders in enhancing a Cybersecurity programme 3. Ability to understand the roles and responsibilities of providers and consumers as the main stakeholders in cybersecurity 4. Ability to distinguish between the roles of the individuals and roles of the organization in the cyberspace 5. Ability to understand leaderships' role in defining the roles and responsibilities of involved parties 6. Ability to identify different types of security policies 7. Ability to develop a Cybersecurity Policy	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 the roles of various individuals in the cyberspace 4. Knowledge of government and law enforcement agencies' role and their impact on cyberspace

Domain 3: Cybersecurity Risk Management

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

Competencies	Knowledge statements
1. Ability to understand the Cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals 2. Ability to explain and illustrate the Cybersecurity risk management process 3. Ability to define goals and objectives for a Cybersecurity risk management process 4. Ability to understand and distinguish the overall security risk and Cybersecurity risk 5. Ability to understand and distinguish the overall security risk and Cybersecurity risk 6. Ability to understand and distinguish the overall security risk and Cybersecurity risk	1. Knowledge of the concept of risk and its application in Cybersecurity 2. Knowledge of risk analysis methods 3. Knowledge of the cybersecurity risk management process and the acceptable level of risk in cybersecurity 4. Knowledge of management considerations regarding cybersecurity risk management 5. Knowledge of the implementation of risk management frameworks 6. Knowledge of Cybersecurity assets and their importance

Domain 4: Attack mechanisms and Cybersecurity controls

Main objective: Ensure that the candidate can understand and explain top cyberthreats and their mitigation vectors, and implement key cybersecurity controls as guided in ISO/IEC 27032

Competencies	Knowledge statements
1. Ability to understand the importance of the implementation of cybersecurity controls in support of security requirements 2. Ability to understand the importance of the implementation of cybersecurity controls in support of security requirements 3. Ability to implement key cybersecurity controls based on ISO/IEC 27032 4. Ability to implement key cybersecurity controls based on ISO/IEC 27032	1. Knowledge of application-level controls and their implementation 2. Knowledge of server 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 access control mechanisms 6. Knowledge of network monitoring and tools such as IDS and firewalls used to secure networks or systems 7. Knowledge of attack mechanisms such as malware, botnets, denial-of-service, phishing, spam, exploits kits, data breaches, identity theft, ransomware etc. 8. Knowledge of Cryptography

Domain 5: Information sharing and coordination

Main objective: Ensure that the candidate can establish an Information Sharing and Coordination framework based on the ISO/IEC 27032

Competencies	Knowledge statements
1. Ability to understand and explain the importance and the benefits of information sharing and coordination framework in cybersecurity	1. Knowledge of the establishment of an information sharing and coordination framework that would be beneficial to the community
2. Ability to determine and implement the required methods and processes for information sharing and coordination framework	2. Knowledge of the roles and responsibilities of the key actors during the implementation of an 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	3. Knowledge of techniques and best practices on writing policies, procedures and other types of documents
4. Ability to define and write policies and procedures regarding information sharing and coordination	4. Knowledge of the categorization and classification of information that is collected, kept safe or distributed via information sharing and coordination framework
5. Ability to conduct regular testing and periodic reviews	5. 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
6. Ability to prepare for the operation and conduct awareness and training workshops to prepare stakeholders for the establishment of an information sharing and coordination framework	6. Knowledge of 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: : Ensure that the candidate can implement a framework to enable the business continuity management of the organization's critical processes and activities

Competencies	Knowledge statements
1. Ability to understand the role of business continuity in the context of cybersecurity 2. Ability to understand the objectives and benefits of integrating business continuity within a cybersecurity program 3. Ability to define the format and structure of a cybersecurity continuity plan 4. Ability to understand and explain the concept of critical activities in the cybersecurity continuity context 5. Ability to understand technical approaches that are applicable to improving cybersecurity continuity	1. Knowledge of business continuity management. 2. Knowledge of business continuity objectives and its benefits regarding cybersecurity. 3. Knowledge of the principles of business continuity as indicated in ISO/IEC 27031 4. Knowledge of the concept of critical activities in cybersecurity continuity 5. Knowledge of a recovery plan and its objectives 6. Knowledge of technical approaches for improving cybersecurity continuity

Domain 7: Cybersecurity incident management and performance measurement

Main objective: 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	Knowledge statements
1. Ability to define and implement an incident management process based on 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	1. Knowledge of cybersecurity incident management 2. Knowledge of the ways to avoid cybersecurity incidents before they occur 3. Knowledge of the ways 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 the above-mentioned domains and their relevance, 12 questions are included in the exam, 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 synthesis and 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		2	16.67	10	13.34
		5	X					
	Roles and responsibilities of stakeholders	5	X		1	8.33	5	6.67
	Cybersecurity Risk Management	10	X		2	16.67	15	20.00
		5		X				
	Attack mechanisms and Cybersecurity controls	10	X		2	16.67	20	26.67
		10	X					
	Information sharing and coordination	5	X		1	8.33	5	6.67
	Integrating Cybersecurity Program in Business Continuity Management	5		X	2	16.67	10	13.33
		5		X				
	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	5				
	% of the exam devoted to each level of understanding (cognitive/taxonomy)		58.33	41.67				

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

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

General Information on 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 Reseller 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 detailed information about the online format, please refer 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. They 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 is open book and is not intended to measure memorizing or recalling information. It 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.

Since the exam is "open book," candidates are authorized to use the following reference materials:

- A hard copy of ISO/IEC 27032 standard
- Training course materials (accessed through PECB Exams app and/or printed)
- Any personal notes taken during the training course (accessed through PECB Exams app and/or printed)
- A hard copy dictionary

Any attempts to copy, collude, or otherwise cheat during the exam session will automatically lead to failure of the exam.

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

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). All PECB multiple-choice exams have one question and three alternatives, of which only one is correct.

For specific information about exam types, languages available, and other details, visit the List of PECB Exams.

Receiving the Exam Results

Exam results will be communicated via email. The only possible results are *pass* and *fail;* no specific grade will be included.

- 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 for a re-evaluation by writing to results@pecb.com within 30 working 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 working days from the date when they received the reevaluated exam results to file a complaint through the PECB Ticketing System. Complaints received after 30 days will not be processed.

Exam Retake Policy

There is no limit on the number of times that a candidate may retake an exam. However, there are certain limitations in terms of the allowed time frames between exam retakes.

- If a candidate does not pass the exam on the 1st attempt, they must wait 15 days from the initial date of the exam for the next attempt (1st retake). Retake fees apply.
  Note: *Candidates who have completed the training course but failed the exam are eligible to retake the exam once for free within a 12-month period from the initial date of the exam.*
- If a candidate does not pass the exam on the 2nd attempt, they must wait three months after the initial date of the exam for the next attempt (2nd retake). Retake fees apply.
  Note: *For candidates that fail the exam in the 2nd retake, PECB recommends them to attend a training course in order to be better prepared for the exam.*
- If a candidate does not pass the exam on the 3rd attempt, they must wait six months after the initial date of the exam for the next attempt (3rd retake). Retake fees apply.
- After the 4th attempt, the waiting period for further retake exams is 12 months from the date of the last attempt. Retake fees apply.

To arrange exam retakes (date, time, place, costs), candidates need to contact the PECB Reseller/Distributor who has initially organized the session.

Reschedule the Exam

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

Closing a Case

If candidates do not apply for certification within three years, 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 and pay the required fee.

Exam Security

A significant component of a successful and respected professional certification credential is maintaining the security and confidentiality of the exam. PECB relies upon the ethical behavior of certificate holders and applicants to maintain the security and confidentiality of PECB exams. Any disclosure of information about the content of PECB exams indicates violation of PECB's Code of Ethics. PECB will take action against individuals who violate PECB Policies and the Code of Ethics. These actions include permanently barring individuals from pursuing PECB credentials and revoking the awarded credentials. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

SAMPLE EXAM QUESTIONS

Question 1: Stakeholders in Cyberspace

Please explain why are providers considered as stakeholders and how can you gain their commitment?

Possible answer:

According to clause 10.3 of ISO/IEC 27032, service providers are expected to observe the same roles and responsibilities as consumer organizations, however, they have additional responsibilities in maintaining or even enhancing security of the Cyberspace by:

— providing safe and secure products and services;

— providing safety and security guidance for end-users; and

— providing security inputs to other providers and to consumers about trends and observations of traffic in their networks and services.

By the time that they provide information and services to the cyberspace and the cyberspace environment depends on them, they should be considered stakeholders.

So, providers are affected by the outcome of the Cyberspace or the services in it and also they are involved in Cybersecurity condition.

Question 2: Cybersecurity Controls

For each of the following clauses/controls of the ISO/IEC 27032 standard, please provide an action plan with at least two concrete actions that would be acceptable to ensure conformity to the clause and fulfill control objectives.

Possible answer:

1. *Clause 12.3.d - Review the security configuration*

- *Review all configuration aspects ensuring that security is addressed at every level as well as the exposure of the device to network threats*
- *Conduct an assessment of the device patch level, the logging and authentication mechanisms as well as any available security features*

2. Clause 12.4.a - Use of supported operating systems, with the most updated security patches installed

- *Keep operating system up to date regarding security patches*
- *Ask for reports to ensure that consumers are aware of, and follow organizational policy regarding supported operating systems*

3. Clause 12.4.f – Use phishing filters

Establish a policy for using phishing filters
Enable tools for phishing filters on web browsers

Question 3: Cybersecurity Awareness

How can you make your employees aware about the importance of their involvement in cybersecurity? Please elaborate some of the measures that you would implement.

Possible answer:

Share a policy about the use of supported operating system and there is a need for updates and security patches installed
Share a policy and appropriate information regarding the use of the latest supported software applications, with the most updated patches installed
Share appropriate information and policy on the use of anti-virus and anti-spyware tools
Send notifications to the end users about new updates and potential threats
Advise them to understand and read more about cybersecurity threats
Keep them abreast about the new security capabilities to protect users against risk