PECB BEYOND RECOGNITION

Exam Preparation Guide

EBIOS Risk Manager

GENERAL

The objective of the "PECB Certified EBIOS Risk Manager" exam is to ensure that the candidate has the necessary competence to: support an organization to identify, analyze, prioritize and manage information security risks. Furthermore, the objective of this exam is to ensure that the candidate also has the knowledge and skills to support an organization in implementing and managing an information security risk management program using EBIOS methodology as a reference framework.

The EBIOS Risk Manager exam is intended for:

- Risk managers
- Persons responsible for information security or conformity within an organization
- Members of an information security team
- IT consultants
- Staff implementing or seeking to comply with EBIOS or involved in a risk management program

The exam covers the following competency domains:

- **Domain 1:** Fundamental principles and concepts of an information security risk management
- **Domain 2:** Concepts and techniques to conduct an information security risk management study based on EBIOS
- **Domain 3:** Concepts and techniques for analyzing and communicating results of an information security risk management study based on EBIOS

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts of an information security risk management

Main objective: Ensure that the candidate understands and is able to interpret the main risk management guidelines and concepts based on EBIOS methodology

Competencies	Knowledge statements
1. Ability to understand and explain the operations of the organization and the development of risk management standards 2. Ability to identify, analyze and evaluate the guidance coming from risk management frameworks for an organization 3. Ability to explain and illustrate the main concepts in risk management 4. Ability to distinguish and explain the difference between information asset, data and record 5. Ability to identify significant aspects for an effective risk management 6. Ability to understand and distinguish the different types of risk 7. Ability to understand, interpret and illustrate the relationship between the concepts of asset, vulnerability, threat, impact and controls 8. Ability to distinguish the relationship between EBIOS, ISO/IEC 27005, and other related standards and/or methodologies 9. Ability to understand jurisdiction-specific and arbitration requirements 10. Ability to evaluate and classify evidence/arbitrations by its nature, strength and usefulness 11. Ability to completely and accurately report the findings including the result of the analysis 12. Ability to identify and understand the presence of your audience during the presentation of findings	1. Knowledge of the application of the principles of risk management 2. Knowledge of the main standards in risk management 3. Knowledge of the different sources of risk management frameworks for an organization: laws, regulations, international and industry standards, contracts, market practices, internal policies 4. Knowledge of the main risk management concepts and terminology 5. Knowledge of the concept of risk and its application in information security 6. Knowledge of the relationship between the concepts of asset, vulnerability, threat, impact and controls 7. Knowledge of the relationship and differences between ISO/IEC 27005 and EBIOS methodology 8. Knowledge of the relationship between the concepts of asset, threat, likelihood, impact and controls

PECB

Domain 2: Concepts and techniques to conduct an information security risk management study based on EBIOS

Main objective: Ensure that the candidate can conduct an information security risk management study based on EBIOS, and use it as a reference framework for the implementation of a risk management process within an organization

Competencies

1. Ability to understand, analyze needs and provide guidance on the attribution of roles and responsibilities in the context of the implementation and management of a risk management framework
2. Ability to define the document and record management processes needed to support the implementation and the operations of a risk management framework
3. Ability to define and design controls & processes and document them
4. Ability to define and write policies and procedures
5. Ability to implement the required processes of a risk management framework
6. Ability to define and implement appropriate risk management training, awareness and communication plans
7. Ability to define and implement an incident management process based on best practices
8. Ability to transfer a project to operations and manage the change management process
9. Ability to understand and interpret the recommendations for a risk management framework provided by EBIOS methodology
10. Ability to understand, interpret, and apply the risk management process based on the recommendations of EBIOS methodology
11. Ability to understand the context of an organization whendesigning the risk management framework
12. Ability to understand the establishment of a risk management policy

Knowledge statements

1. Knowledge of the roles and responsibilities of the key actors during the implementation of a risk management framework and in its operation after the end of the implementation project
2. Knowledge of the main risk assessment techniques suggested by EBIOS methodology
3. Knowledge of the main organizational structures applicable for the management of the risk within an organization
4. Knowledge of the best practices on document and record management processes and the document management life cycle
5. Knowledge of model-building controls, processes and techniques
6. Knowledge of controls and processes deployment technique
7. Knowledge of techniques and best practices to write policies, procedures and others types of documents
8. Knowledge of the characteristics and the best practices to conduct risk management training, awareness and communication plans
9. Knowledge of the characteristics and main processes of an information security incident management process based on best practices
10. Knowledge of change management techniques
11. Knowledge of the objectives of a risk management program and risk assessment process
12. General knowledge of the main risk assessment methodologies
13. Knowledge on planning risk assessment projects and activities by ensuring the participation and support of stakeholders throughout the risk assessment process

13. Ability to lead assessment projects and manage multidisciplinary teams 14. Ability to perform a risk management study based on EBIOS in various settings and establishments 15. Ability to identify primary and supporting assets of an organization 16. Ability to identify the consequences in terms of confidentiality, integrity and availability of assets 17. Ability to assess the likelihood and determine the level of risk for each identified incident scenario 18. Ability to calculate the level of risk in terms of the combination of consequences and their likelihood 19. Ability to understand and interpret information security risk management processes according to EBIOS	14. Knowledge on risk assessment projects of a more global and more complex nature 15. Knowledge of information gathering techniques. 16. Knowledge on identification of assets, risk sources, vulnerabilities, existing measures, impacts, incident likelihood and the relation between these concepts 17. Knowledge on likelihood assessment and risk level determination for different identified incident scenarios 18. Knowledge of risk level estimation according to the evaluation criteria and the risk acceptance criteria

Domain 3: Concepts and techniques for analyzing and communicating results of an information security risk management study based on EBIOS

Main objective: Ensure that the candidate can perform risk management communication activities in the context of EBIOS

Competencies	Knowledge statements
1. Ability to use language as a flexible tool to share and collect information, exchange ideas and openly explore a variety of perspectives by adjusting the style and content to each individual, audience and circumstance in different meetings 2. Ability to use communication skills to encourage participation and collaboration of all the participants in a meeting to influence the success of the meeting 3. Ability to comprehend and evaluate requirements of information security risk communication objectives 4. Ability to establish an efficient internal communication within the organization 5. Ability to understand the steps that can be taken when there are no risk treatment options available or if treatment options do not sufficiently modify the risk. 6. Ability to understand the importance of risk communication and consultation 7. Ability to understand and determine the principles of risk communication 8. Ability to understand the importance of and reasons for recording and reporting of risk management activities 9. Ability to understand the control of records of risk management activities 10. Ability to understand risk reporting 11. Ability to document the risk management process and its outcomes 12. Ability to monitor and review risk management activities 13. Ability to establish an efficient communication with the external stakeholders	1. Knowledge of different techniques and methodologies to conduct effective meetings. These activities involve the coordination of every detail of a meeting 2. Knowledge of best practices used in the presentation and meetings. Knowledge of the guidelines and processes from risk management guidelines and frameworks based on EBIOS 3. Knowledge on the outcomes of risk analysis and risk prioritization 4. General knowledge of the information security communication process 5. Knowledge of the principles of an efficient communication strategy 6. Knowledge of establishing internal communication within the organization 7. Knowledge of establishing external communication with stakeholders 8. Knowledge of communication activities 9. Knowledge of monitoring and review of specific elements of risk factors 10. Knowledge of monitoring and review of risk management 11. Knowledge of setting continual improvement objectives 12. Knowledge of the risk analysis techniques recommended by EBIOS methodology 13. Knowledge of the main advantages and disadvantages of each risk analysis approach 14. Knowledge on the identification and analysis of stakeholders, and their involvement in the risk management process 15. Knowledge of EBIOS recommendations on how to define the scope and boundaries related to the risk management process

14. Ability to ensure communication and consultation between the decision-makers and external & internal stakeholders 15. Ability to establish a risk communication plan 16. Ability to record the information security risk management decisions and activities 17. Ability to monitor and review the risk management process, risks and controls 18. Ability to ensure continual improvement of the risk management program	16. Knowledge of the constraints affecting the scope 17. Knowledge on how to identify the assets, risk sources, risk events, the existing measures to mitigate risk, and the consequences that might happen if the risk occurs 18. Knowledge of the methods to assess the risk consequences, incident likelihood, and the level of risk determination based on EBIOS methodology 19. Knowledge on how to evaluate the identified and analyzed risks based on risk evaluation criteria 20. Knowledge on the risk treatment options, the establishment of risk treatment plan, and the evaluation of residual risk 21. Knowledge on the risk treatment plan acceptance, and residual risk acceptance 22. Knowledge of the main purpose of risk communication and consultation 23. Knowledge of the recording and reporting goals of risk management activities based on EBIOS methodology 24. Knowledge on important factors of risk reporting based on the recommendations of EBIOS methodology

Based on the above-mentioned domains and their relevance, 7 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 information security risk management	5	X		3	42.85	15	30
		5	X					
		5		X				
	Concepts and techniques to conduct an information security risk management study based on EBIOS	10	X		2	28.57	20	40
		10		X				
	Concepts and techniques for analyzing and communicating the results of an information security risk management study based on EBIOS	10	X		2	28.57	15	30
		5		X				
	Total points	50						
	Number of questions per level of understanding		4	3				
	% of the exam devoted to each level of understanding (cognitive/taxonomy)		57.14	42.85				

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

After successfully passing the exam, candidates will be able to apply for the "PECB Certified EBIOS" 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 EBIOS methodology
- Training course materials(accessed through PECB Exams app and/or printed)
- Any personal notes made by the candidate 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.

PECB

Sample Exam Questions

Question 1: Identification of assets
Explain why these are the assets with the highest value to the organization. Please also identify whether the following are primary or supporting assets:

Possible answer:
Asset 1: website (primary asset)

Justification of the value: The website of the company is the main marketing tool and supports the selling process.

Asset 2: The two owners (supporting asset)

Justification of the value: They are the ones creating original and innovative products.

Question 2: Identification of risk associated with information security
Identify threats, vulnerabilities and impacts associated with the incident scenarios below and indicate if it is possible that the impacts affect the availability, integrity and/or the confidentiality of the information. Complete the risk matrix.

Possible answer:

Statements	Vulnerabilities	Threats	C	I	A	Potential Impacts
1. The webmaster who designed the corporate Website takes care of the updates and the uploading of the site	*Absence of segregation of duties.* *Only one person is available for this function*	*Treatment errors* *Malicious act* *Webmaster leaves the company or becomes sick*		*X*	*X*	*Website containing erroneous information: loss of credibility* *Unavailable website: loss in revenues*

Address:
Head Quarters
6683 Jean Talon E,
Suite 336 Montreal,
H1S 0A5, QC,
CANADA

Tel./Fax.
T: +1-844-426-7322
F: +1-844-329-7322

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. Visit Help Center here: www.pecb.com/help

Emails:
Examination: examination@pecb.com
Certification: certification@pecb.com
Customer Care: customer@pecb.com

Copyright © 2020 PECB. Reproduction or storage in any form for any purpose is not permitted without a PECB prior written permission.