PECB

When Recognition Matters

EXAM PREPARATION GUIDE

PECB Certified ISO 31000 Risk Manager

The objective of the "PECB Certified ISO 31000 Risk Manager" exam is to ensure that the candidate has acquired the necessary knowledge and skills to interpret risk management concepts, principles and generic guidelines provided in the ISO 31000 standard.

The ISO 31000 Risk Manager exam is intended for:

- Managers or consultants responsible for the effective management of risk within an organization
- Individuals seeking to gain comprehensive knowledge of Risk Management concepts, processes and principles
- Advisors involved in Risk Management

The exam covers the following competency domains:

- **Domain 1:** Fundamental principles and concepts in Risk Management
- **Domain 2:** Risk management framework and process
- **Domain 3:** Risk assessment techniques based on IEC/ISO 31010

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts of Risk Management

Main objective: Ensure that the ISO 31000 Risk Manager candidate understands, and is able to interpret and illustrate the ISO 31000 concepts, principles, and recommendations.

Competencies	Knowledge statements
1. Ability to understand and explain the organization`s operations and the development of risk management standards. 2. Ability to explain and illustrate the main concepts of risk management. 3. Ability to interpret the advantages of effective risk management in an organization. 4. Ability to understand the risk management principles. 5. Ability to identify significant aspects for an effective risk management. 6. Ability to understand and distinguish the different types of risk.	1. Knowledge of the main standards related to risk management. 2. Knowledge of the main concepts and terminology as described in ISO 31000. 3. Knowledge of the concept of risk and its application in organizations. 4. Knowledge of the main advantages and benefits that organizations can gain by an effective implementation of a risk management process. 5. Knowledge of the ISO 31000 risk management principles and their application in organizations. 6. Knowledge of the main elements to be applied by an organization for a succesful risk management process. 7. Knowledge of risk types, including: strategic risks, financial risks, compliance risks, and operational risks.

Domain 2: Risk Management framework and process

Main objective: Ensure that the ISO 31000 Risk Manager candidate can contribute in the development of a risk management framework, and is able to manage risks based on the risk management process, as recommended by ISO 31000.

Competencies	Knowledge statements
1. Ability to understand and interpret the recommendations for the risk management framework provided by ISO 31000. 2. Ability to distinguish the relationships and main components of the risk management framework. 3. Ability to understand, interpret, and apply the risk management process based on the recommendations of ISO 31000. 4. Ability to understand the context of an organization when designing the risk management framework. 5. Ability to understand the establishment of a risk management policy. 6. Ability to identify who is accountable for the development, implementation and maintenance of the risk management framework. 7. Ability to integrate the risk management process into the organization's processes. 8. Ability to identify the necessary resources for the risk management implementation. 9. Ability to understand and identify the appropriate risk analysis approach. 10. Ability to establish the external and internal context of the organization. 11. Ability to identify all relevant stakeholders in the risk management process. 12. Ability to define the risk management process scope and boundaries. 13. Ability to define the risk criteria. 14. Ability to identify, analyze, evaluate, and treat risks. 15. 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. 16. Ability to understand the importance of risk communication and consultation. 17. Ability to understand and determine the principles of risk communication. 18. Ability to set and define risk communication	1. Knowledge of the ISO 31000 risk management framework and its recommendations. 2. Knowledge of the relationship and main components of risk management frameworks (Leadership and Commitment, Integration, Design, Implementation, Evaluation, Improvement). 3. Knowledge of the risk management process activities, including communication and consultation, scope, context and criteria, risk assessment, risk treatment, monitoring and review, and recording and reporting. 4. Knowledge on how to undestand an organization's external and internal context. 5. Knowledge of the ways that can be used to articulate commitment to risk management. 6. Knowledge on how to define organizational roles, authorities, responsibilities and accountabilities for an effective risk management. 7. Knowledge of the ISO 31000 recommendations on accountability and risk owners. 8. Knowledge on how to integrate risk management in the organization's practices and processes in a way that is relevant, effective and efficient. 9. Knowledge on the allocation of appropriate resources needed for risk management implementation. 10. Knowledge of the risk analysis techniques recommended by ISO 31000. 11. Knowledge of the main advantages and disadvantages of each risk analysis approach. 12. Knowledge on how to establish the organization`s internal and external context for the risk management process. 13. Knowledge on the identification and analysis of stakeholders, and their involvement in the risk management process. 14. Knowledge of the ISO 31000 recommendations on how to define the scope and boundaries related to the risk management process. 15. Knowledge of the constraints affecting the scope.

objectives. 19. Ability to understand the importance of and reasons for recording and reporting of risk management activities. 20. Ability to understand the control of records of risk management activities. 21. Ability to understand risk reporting. 22. Ability to document the risk management process and its outcomes. 23. Ability to monitor and review risk management activities.	16. 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. 17. Knowledge of the methods to assess the risk consequences, incident likelihood, and the level of risk determination based on ISO 31000. 18. Knowledge on how to evaluate the identified and analyzed risks based on risk evaluation criteria. 19. Knowledge on the risk treatment options, the establishment of risk treatment plan, and the evaluation of residual risk. 20. Knowledge on the risk treatment plan acceptance, and residual risk acceptance. 21. Knowledge of the main purpose of risk communication and consultation. 22. Knowledge of the principles of an efficient risk communication. 23. Knowledge of the main objectives of the risk communication. 24. Knowledge of the importance of recording and reporting of the risk management processes. 25. Knowledge of the recording and reporting goals of risk management activities based on ISO 31000. 26. Knowledge of the tools and techniques used to control and register records. 27. Knowledge on important factors of risk reporting based on the recommendations of ISO 31000. 28. General knowledge on the risk management documentation. 29. Knowledge on the documentation pyramid. 30. Knowledge on risk management documentation criteria. 31. Knowledge on types of documents that are necessary for risk management documentation. 32. Knowledge on how to monitor the risk management activities. 33. Knowledge of the elements to be considered during the risk management review.

Domain 3: Risk assessment techniques based on IEC/ISO 31010

Main objective: Ensure that the ISO 31000 Risk Manager candidate can understand, interpret and apply the risk assessment techniques provided by the IEC/ISO 31010 standard.

Competencies	Knowledge statements
1. Ability to understand and interpret the risk assessment techniques provided by IEC/ISO 31010 standard. 2. Ability to understand the strongly applicable techniques for risk identification, risk assessment and risk evaluation. 3. Ability to understand the strongly applicable techniques for identifying risk consequences, risk probability and level of risk.	1. Knowledge of the main risk assessment techniques provided by IEC/ISO 31010, including brainstorming, decision tree analysis, bow tie analysis, root cause analysis, business impact analysis, scenario analysis, failure mode effect analysis, cause and effect analysis, and consequence/probability matrix. 2. Knowledge on how to determine which risk assessment techniques are strongly applicable for risk identification. 3. Knowledge on how to determine which risk assessment techniques are strongly applicable for risk analysis. 4. Knowledge on how to determine which risk assessment techniques are strongly applicable for risk evaluation. 5. Knowledge on how to determine which risk assessment techniques are strongly applicable for identifying risk consequences, risk probability and level of risk.

Based on these 3 domains and their relevance, 7 questions are included in the exam, as summarized in the following table:

			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 per competency domain
Competency/Domains	Fundamental principles and concepts of Risk Management	5	X		1	14.28	5	10
	Risk Management framework and process	10		X	5	71.43	40	80
		10	X					
		5		X				
		10	X					
		5		X				
	Risk assessment techniques based on IEC/ISO 31010	5	X		1	14.28	5	10
	Total points	50	4	3				
	Number of questions per level of understanding							
	% of Test devoted to each level of understanding (cognitive/taxonomy)		57.14	42.86				

The passing score is established at **70%.**

After successfully passing the exam, candidates will be able to apply for the "PECB Certified ISO 31000 Risk Manager" credential, depending on their level of experience.

TAKE A CERTIFICATION EXAM

Candidates will be required to arrive at least thirty (30) minutes before the beginning of the certification exam. Candidates arriving late will not be given additional time to compensate for the late arrival and may be denied entry to the exam room (if they arrive more than 5 minutes after the beginning of the exam scheduled time).

All candidates will need to present a valid identity card with a picture such as a driver's license or a government ID to the invigilator.

The exam duration is two (2) hours. Non-native speakers recive an additional twenty (20) minutes.

The exam contains essay type questions: This type of format was selected as a means of determining whether an examinee can clearly answer training related questions, by assessing problem solving techniques and formulating arguments supported with reasoning and evidence.

The exam is set to be “open book”, and does not measure the recall of data or information. The examination evaluates the candidates’ comprehension, application and analyzing skills. Therefore, candidates will have to justify their answers by providing concrete explanations as to demonstrate that they have been capable of understanding the training concepts. At the end of this document, you will find samples of exam questions and potential answers.

As the exam is “open book”; candidates are authorized to use:

- A copy of the ISO 31000 standard,
- Course notes from the Participant Handout,
- Any personal notes made by the student during the course, and
- A hard copy dictionary.

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 failure of the exam.

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 by email within a period of 6 to 8 weeks from your examination date. The candidate will be provided with only two possible examination results: pass or fail, rather than an exact grade.

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

In case of exam failure, the results will be accompanied with the list of domains in which the candidate had received low grading as to provide guidance in case of retaking the exam.

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

EXAM RETAKE POLICY

There is no limit on the number of times a candidate may retake an exam. However, there are some limitations in terms of the allowed time-frame in between exam retakes, such as:

- If a candidate does not pass the exam on the first attempt, he/she must wait 15 days for the next attempt (1st retake). Retake fee applies.

Note: *Students, who have completed the full training but failed the written 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 second attempt, he/she must wait 3 months (from the initial date of the exam) for the next attempt (2nd retake). Retake fee applies.

- If a candidate does not pass the exam on the third attempt, he/she must wait 6 months (from the initial date of the exam) for the next attempt (3rd retake). Retake fee applies.

After the fourth attempt, a waiting period of 12 months from the last session date is required in order for the candidate to retake the same exam. Regular fee applies.

For the candidates that fail the exam in the 2nd retake, PECB recommends to attend an official training in order to be better prepared for the exam.

To arrange exam retakes (date, time, place, costs), the candidate needs to contact the PECB partner who has initially organized the session.

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 the PECB examination content, they violate the PECB Code of Ethics. PECB will take action against individuals who violate the PECB Policies and 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 rights.

SAMPLE EXAM QUESTIONS AND POSSIBLE ANSWER

Question 1:
After assessing and treating risk, some residual risk might still remain present. Risk treatment does not always yield the desired results and as such, the risk might not be mitigated to an acceptable level. What actions should be undertaken in these cases? Please provide any circumstances or scenarios when risks are retained and not treated any further, even though they are above the threshold of risk acceptance criteria.

Possible answer:
ISO 31000 describes the purpose of risk treatment as the selection and implementation of options for addressing risk.

If risk treatment options do not yield the desired results, the organization should record the risks and keep them under review. When risk treatment options do not bring down the risks to the organization’s acceptable levels, one may take some of the following actions:

- Decide whether the residual risk level is tolerable
- Be aware of the nature and extent of the residual risk
- Assess the effectiveness of that treatment

Furthermore, the decision-makers should be aware of the nature and extent of the residual risk after risk treatment. Some of the circumstances when the risks are retained and not treated any further, even if they are above the threshold of acceptable risks, are:

- Taking or increasing the risk in order to pursue an opportunity
- Removing the risk source
- Changing the likelihood or the consequences

- Sharing the risk with another party or parties
- Retaining the risk by informed decision

Question 2:
It is stated in ISO 31000 that the risk management process should be an integral part of management and decision-making and should be integrated into the structure, operations and processes of the organization.

Please explain and elaborate why the integration of the risk management into organizational processes is important.

Possible answer:
Risk management process should be an integral part of management and decision-making taking into consideration the aim of each organization which is the optimization of benefits and opportunities and the minimization of dangerous impacts from its operations. The top management and the organization should understand that risk management is not a stand-alone process and it should be integrated into the organization's processes and activities.

Embedding the risk management process in the culture and practices of the organization is crucial because it makes the risk management process an intrinsic part of the organization`s processes. The organization must embed risk management to all strategic, tactical and operational processes of the organization, starting from design to implementation. This ensures that the risk management processes will be supported by all employees of the organization; thus the likelihood of achieving business objectives will increase.

The activities of various processes of the organization must be structured to meet the specific needs of the business process or structure. The business process or structure will be reviewed to determine and identify the incorporated activities and necessary adjustments of risk management.