PECB BEYOND RECOGNITION

Exam Preparation Guide

ISO 31000 Risk Manager

GENERAL

The objective of the "PECB Certified ISO 31000 Risk Manager" exam is to ensure that the candidate has the necessary competence to: comprehend fundamental concepts about risk management and understand the importance and benefits of principles and generic guidelines that can be obtained by this standard.

The ISO 31000 Risk Manager exam is intended for:

- Managers or consultants involved in and concerned with the implementation of risk management in an organization
- Individuals seeking to gain knowledge about the risk management principles, framework, and process
- Individuals responsible for the creation and protection of value in their organizations
- Individuals interested in pursuing a career in risk management
- Advisors involved in risk management

The exam covers the following competency domains:

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

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts of a risk management **Main objective:** Ensure that the candidate understands and is able to interpret ISO 31000 principles and concepts	
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 candidate understands, is able to 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	1. Knowledge of the ISO 31000 risk management framework and its recommendations 2. Knowledge of a relationship and main components of risk management frameworks (leadership and commitment, integration, design, implementation, evaluation, improvement) 3. Knowledge of a 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 a 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

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 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	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 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 a risk treatment options, the establishment of risk treatment plan, and the evaluation of residual risk 20. Knowledge on a 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 a 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 a risk management documentation 29. Knowledge on a 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 ISO/IEC 31010

Main objective: Ensure that the candidate understands, is able to interpret, and apply the risk assessment techniques provided by ISO/IEC 31010 standard

Competencies	Knowledge statements
1. Ability to understand and interpret the risk assessment techniques provided by ISO 31000 standard 2. Ability to understand strongly applicable techniques for risk identification, risk assessment and risk evaluation 3. Ability to understand strongly applicable techniques for identifying risk consequences, risk probability and level of risk	1. Knowledge of the main risk assessment techniques provided by ISO 31000, 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 1. Knowledge on how to determine which risk assessment techniques are strongly applicable for identifying risk consequences, risk probability and level of risk

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 a 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 ISO/IEC 31010	5	X		1	14.28	5	10
	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	42.86				

The exam passing score is **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.

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 copy of ISO 31000 standard
- 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.

Sample Exam Questions

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.

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