When Recognition Matters

EXAM PREPARATION GUIDE

PECB Certified ISO 31000 Risk Manager

The objective of the "PECB Certified ISO 31000 Risk Manager" examination is to ensure that the candidate has the knowledge and the skills to master the principles and generic guidelines on risk management using the ISO 31000:2009 standard as a reference framework.

The target population for this examination is:

- Risk managers
- Persons responsible for risk management or conformity within an organization
- Member of the risk management team
- Staff implementing ISO 31000 or involved in a risk management program

The exam content covers the following domains:

- Domain 1: Fundamental concepts, approaches, methods and techniques of risk management
- Domain 2: Risk management program
- Domain 3: Risk assessment
- Domain 4: Risk treatment
- Domain 5: Risk communication, monitoring and improvement

Further information related to ISO 31000 standard: (*source: www.iso.org*)

ISO 31000:2009 can be used by any public, private or community enterprise, association, group or individual. Therefore, ISO 31000:2009 is not specific to any industry or sector.

ISO 31000:2009 can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.

ISO 31000:2009 can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.

Although ISO 31000:2009 provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.

It is intended that ISO 31000:2009 be utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards.

ISO 31000:2009 is not intended for the purpose of certification.

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts in risk management

Main objective: To ensure that the ISO 31000 Risk Manager candidate can understand, interpret and illustrate the main risk management guidelines and concepts related to an risk management framework based on ISO 31000.

Competencies	Knowledge statements
1. Understand and explain the operations of the ISO 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 and risk management 4. Ability to distinguish and explain the difference between information asset, data and record 5. Understand, interpret and illustrate the relationship between the concepts of asset, vulnerability, threat, impact and controls 6. Ability to distinguish relationship and main components of risk management frameworks.	1. Knowledge of the application of the eight ISO management principles to 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 concepts and terminology as described in ISO 31000 5. Knowledge of the concept of risk and its application in organizations 6. Knowledge of the relationship between the concepts of asset, vulnerability, threat, impact and controls 7. Knowledge of the difference between preventive, detective and corrective controls and their characteristics 8. Knowledge of relationship and main components of risk management frameworks.

Domain 2: Risk management program

Main objective: To ensure that the ISO 31000 Risk Manager candidate can implement the processes of an risk management reference frameworks based on ISO 31000.

Competencies	Knowledge statements
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 an risk management framework 2. Ability to define the document and record management processes needed to support the implementation and the operations of an risk management framework 3. Ability to define and design controls & processes and document them 4. Ability the define and writing policies and procedures 5. Ability to implement the required processes of an risk management framework 6. Ability to define and implement appropriate risk management training, awareness and communication plans.	1. Knowledge of the roles and responsibilities of the key actors during the implementation of an risk management framework and in its operation after the end of the implementation project 2. Knowledge of the main organizational structures applicable for an organization to manage its risk 3. Knowledge of the best practices on document and record management processes and the document management life cycle 4. Knowledge of the characteristics and the differences between the different documents related to policy, procedure, guideline, standard, baseline, worksheet, etc. 5. Knowledge of model-building controls and processes techniques and best practices 6. Knowledge of controls and processes deployment techniques and best practices 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 implement risk management training, awareness and communication plans 9. Knowledge of the characteristics and main processes of an risk management incident management process based on best practices 10. Knowledge of change management techniques best practices.

Domain 3: Risk assessment

Main objective: To ensure that the ISO 31000 Risk Manager candidate can perform risk assessment in the context of an ISO 31000.

Competencies	Knowledge statements
1. Ability to understand and interpret Risk Management processes according to ISO 31000 2. Ability to know and describe several recognized risk assessment methodologies 3. Ability to identify, review and select a Risk Assessment Approach appropriate for a specific organization 4. Ability to plan activities for Risk Assessment and integrate risk assessment to risk management framework 5. Ability to lead assessment projects and manage multidisciplinary team.	1. Knowledge of the guidelines and processes from risk management guidelines and framework based on ISO 31000 2. General knowledge of the main risk assessment methodologies 3. Knowledge on planning risk assessment projects and activities by ensuring the participation and support of stakeholders throughout the risk assessment process 4. Knowledge of the guidelines and best practices to integrate risk assessment to risk management framework 5. Knowledge of the best practices on how to perform validation of the project plan 6. Knowledge on risk assessment projects of a more global and more complex nature and rely on a multidisciplinary team.

Domain 4: Risk Treatment

Main objective: To ensure that the ISO 31000 Risk Manager candidate can implement the risk treatment process of a risk management reference framework based on ISO 31000.

Competencies	Knowledge statements
1. Ability to understand and manage risk by identifying it, analyzing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria. 2. Ability to communicate and consult with stakeholders and monitor and review the risk and the controls that are modifying the risk in order to ensure that no further risk treatment is required. 3. Ability to effectively allocate and use resources for risk treatment 4. Ability to select one or more options for modifying risks, and implementing those options.	1. Knowledge of the roles and responsibilities of the key actors during the implementation of a risk treatment plan 2. Knowledge of the best practices on documenting and record risk treatment plan 3. Knowledge on risk evaluation methods and risk criteria 4. Knowledge on communication and monitoring the risk controls metrics to ensure that no further risk treatment is required. 5. Knowledge on risk treatment resource management 6. Knowledge on selection of one or more options for modifying risks, and implementing those options.

Domain 5: Risk communication, monitoring and improvement

Main objective: To ensure that the ISO 31000 Risk Manager candidate can implement the processes for risk communication, monitoring and improvement risk management reference frameworks based on ISO 31000.

Competencies	Knowledge statements
1. Ability to understand, analyze needs and provide guidance on the attribution of roles and responsibilities in the context of the implementation of risk communication, monitoring and review of a risk management framework 2. Ability to define the document and record management processes needed to support the implementation of communication, monitoring and review of a risk management framework 3. Ability to implement a documented system that will detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and identify emerging risks 4. Ability to define and implement appropriate risk management training, awareness and communication plans 5. Ability to define and implement an incident management process based on best practices. 6. Ability to transfer a project to operations and manage the change management process.	1. Knowledge of the main organizational structures applicable for an organization to manage its risk 2. Knowledge of the best practices on document and record management processes and the document management life cycle 3. Knowledge of model-building controls and processes techniques and best practices to measure their effectiveness and efficiency 7. Knowledge of controls and processes deployment techniques and best practices on monitoring and detection of changes in the external and internal context and identify emerging risks 4. Knowledge of techniques and best practices to write policies, procedures and others types of documents 5. Knowledge of the characteristics and the best practices to implement Risk communication, monitoring and improvement 1. Knowledge of change management techniques best practices.

Based on these 5 domains and their relevance, 5 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 in risk management	5	x		1	20.00	5	10.00
	Risk management program	5	x		1	20.00	5	10.00
	Risk assessment	20	x		1	20.00	20	40.00
	Risk treatment	10		x	1	20.00	10	20.00
	Risk communication, monitoring and improvement	10		x	1	20.00	10	20.00
Total points		50						
Number of Questions per level of understanding			3	2				
% of Test Devoted to each level of understanding (cognitive/taxonomy)			60.00	40.00				

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

After successfully passing the exam, candidates will be able to apply for the credentials of PECB Certified ISO 31000 Risk Manager, 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 proctor and the exam confirmation letter.

The exam duration is two (2) hours.

The questions are essay type questions. This type of format was chosen because the intent is to determine whether an examinee can write a clear coherent answer/argument and to assess problem solving techniques. Because of this particularity, the exam is set to be "open book" and does not measure the recall of data or information. The examination evaluates, instead, comprehension, application, analysis, synthesis and evaluation, which mean that even

if the answer is in the course material, candidates will have to justify and give explanations, to show they really understood the concepts. At the end of this document, you will find sample exam questions and their possible answers.

As the exams are “open book”; candidates are only authorized to use:

- A copy of the ISO 31000:2009 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 attempt 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 by email in a period of 6 to 8 weeks, after taking the exam. The results will not include the exact grade of the candidate, only a mention of pass or fail.

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 action

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.