PECB

When Recognition Matters

WHITEPAPER

ISO 31000

RISK MANAGEMENT – PRINCIPLES AND GUIDELINES

CONTENT

PRINCIPAL AUTHORS

Eric LACHAPELLE, PECB

Besnik HUNDOZI, PECB

INTRODUCTION

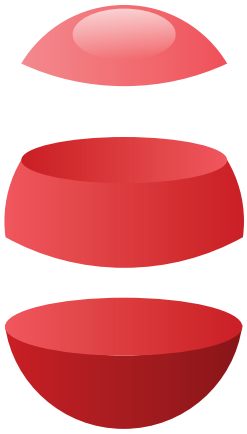
ISO 31000 is an international standard issued in 2009 by ISO (International Organization for Standardization), and it is intended to serve as a guide for the design, implementation and maintenance of risk management.

All types and sizes of organizations face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is risk.

Risk is involved in any activity of an organization. ISO 31000:2009 describes a systematic and logical process, during which organizations manage risk by identifying it, analyzing and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria.

Risk management can be applied to an entire organization, at its many areas and levels, at any time, as well as to specific functions, projects and activities.

RISK – Effect of uncertainty on objectives



1. Positive view
   Potential gain
2. Neutral view
   Probability of events
3. Negative view
   Harmful event

AN OVERVIEW OF ISO 31000:2009

ISO 31000 provides principles and generic guidelines to assist organizations in establishing, implementing, operating, maintaining and continually improving their risk management framework.

It is not specific to any industry or sector, so it can be used by any public, private or community enterprise, association, group or individual. This standard 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.

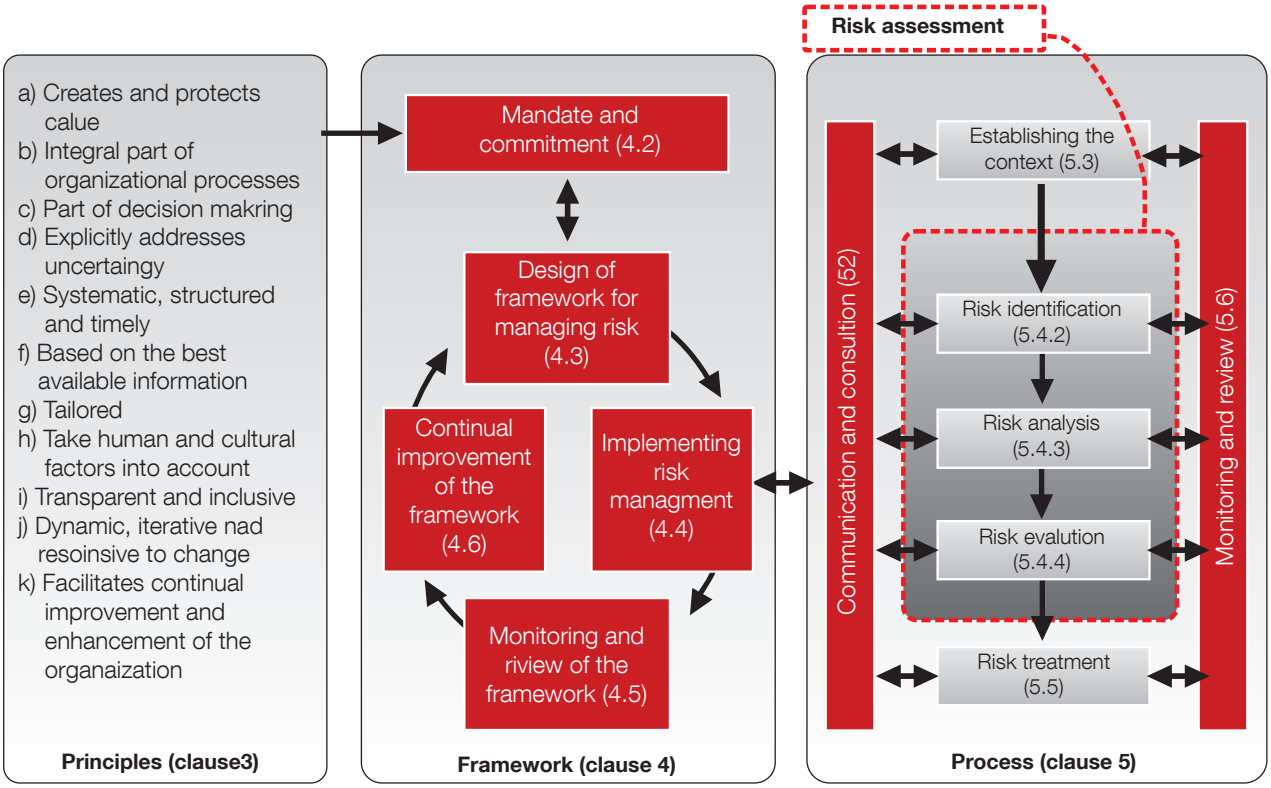
This standard is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes,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

WHAT IS RISK MANAGEMENT?

Risk management is defined as a set of coordinated activities to direct and control an organization with regard to risk.

STRUCTURE OF ISO 31000

This figure shows the relationships between the risk management principles, framework and process.



KEY CLAUSES OF ISO 31000:2009

ISO 31000 is organized into the following main clauses:
Clause 3: Principles
Clause 4: Framework
Clause 5: Process

Each of these key activities is listed below.

CLAUSE 3: PRINCIPLES OF RISK MANAGEMENT

In order to have an effective risk management, an organization has to comply with these 11 principles.

1. Risk management creates and protects value;
2. Risk management is an integral part of all organizational processes;
3. Risk management is part of decision making;
4. Risk management explicitly addresses uncertainty;
5. Risk management is systematic, structured and timely;
6. Risk management is based on the best available information;
7. Risk management is tailored;
8. Risk management takes human and cultural factors into account;
9. Risk management is transparent and inclusive;
10. Risk management is dynamic, iterative and responsive to change;
11. Risk management facilitates continual improvement of the organization.

CLAUSE 4: FRAMEWORK

ISO 31000 states that the success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements what will embed it throughout the organization at all levels.

The framework:
- assists in managing risks effectively through the application of the risk management process;
- ensures that information about risk derived from the risk management process is adequately reported; and
- ensures that these information is used as a basis for decision making and accountability at all relevant organizational levels.

This clause describes the necessary components of the framework for managing risk and the way in which they interrelate in an iterative manner.

Mandate and commitment: Management of the organization needs to demonstrate a strong and sustained commitment to risk management by defining risk management policy, objectives, ensuring legal and regulatory compliance, ensuring necessary resources are allocated to risk management, communicating the benefits of risk management to all stakeholders.

Design of framework for managing risk: Before the implementation, the organization must design a framework for managing risk. This includes:
- Understanding of the organization and its context
- Establishing risk management policy
- Ensuring accountability, authority and appropriate competence for risk management
- Integrating risk management into organizational processes
- Allocating appropriate resources
- Establishing internal and external communication and reporting mechanisms

Implementing risk management: The organization must implement the framework for managing risk and risk management process.

Monitoring and review of the framework: To ensure effectiveness of the risk management the organization should measure risk management performance and progress, review whether the risk management framework, policy and plan are still appropriate and review the effectiveness of the risk management framework.

Continual improvement of the framework: Based on results of monitoring and review, decisions should be made on how the risk management framework, policy and plan can be improved.

Risk assessment: Risk assessment is the overall process of risk identification, analysis and evaluation.

- Risk identification: Through applying risk identification tools and techniques, the organization should identify risk sources, areas of impacts, events and causes, and their potential consequences.

- Risk analysis: Risk analysis involves the development of understanding of the risk, consideration of the causes and risk sources, their positive and negative consequences, the likelihood that those consequences can occur, provides an input to risk evaluation and decision whether risks need to be treated, and on the most appropriate risk treatment strategies and methods.

- Risk evaluation: The purpose of this step is to assist in decision making about which risks need treatment and priority for treatment implementation.

Risk treatment: Risk treatment options should be selected based on the outcome of the risk assessment, the expected cost for implementing and benefiting from these options.

Monitoring and review: Monitoring and review can be periodic or ad hoc, and should be a planned part of the risk management process.

Recording the risk management process: Risk management activities should be traceable. In the risk management process, records provide the foundation for improvement in methods and tool, as well as in the overall process.

CLAUSE 5: PROCESS

ISO 31000 states that the success of risk management will depend on the effectiveness of the management

- The risk management process should be:
  - An integral part of management;
  - Embedded in the culture and practices;
  - Tailored to the business processes of the organization.

- Risk management process comprises the following activities:

Communication and consultation: Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.

Establishing the context: By establishing the context, the organization articulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process.

LINK BETWEEN ISO 31000 AND OTHER STANDARDS

ISO 31000 can be easily linked with other Risk Management standards, like ISO Guide 73:2009 – Risk management vocabulary, and ISO/IEC 31010:2009 – Risk management – Risk assessment techniques. ISO/IEC 31010 is a supporting standard for ISO 31000 and provides guidance on selection and application of systematic techniques for risk assessment.

LINK WITH ISO 27005

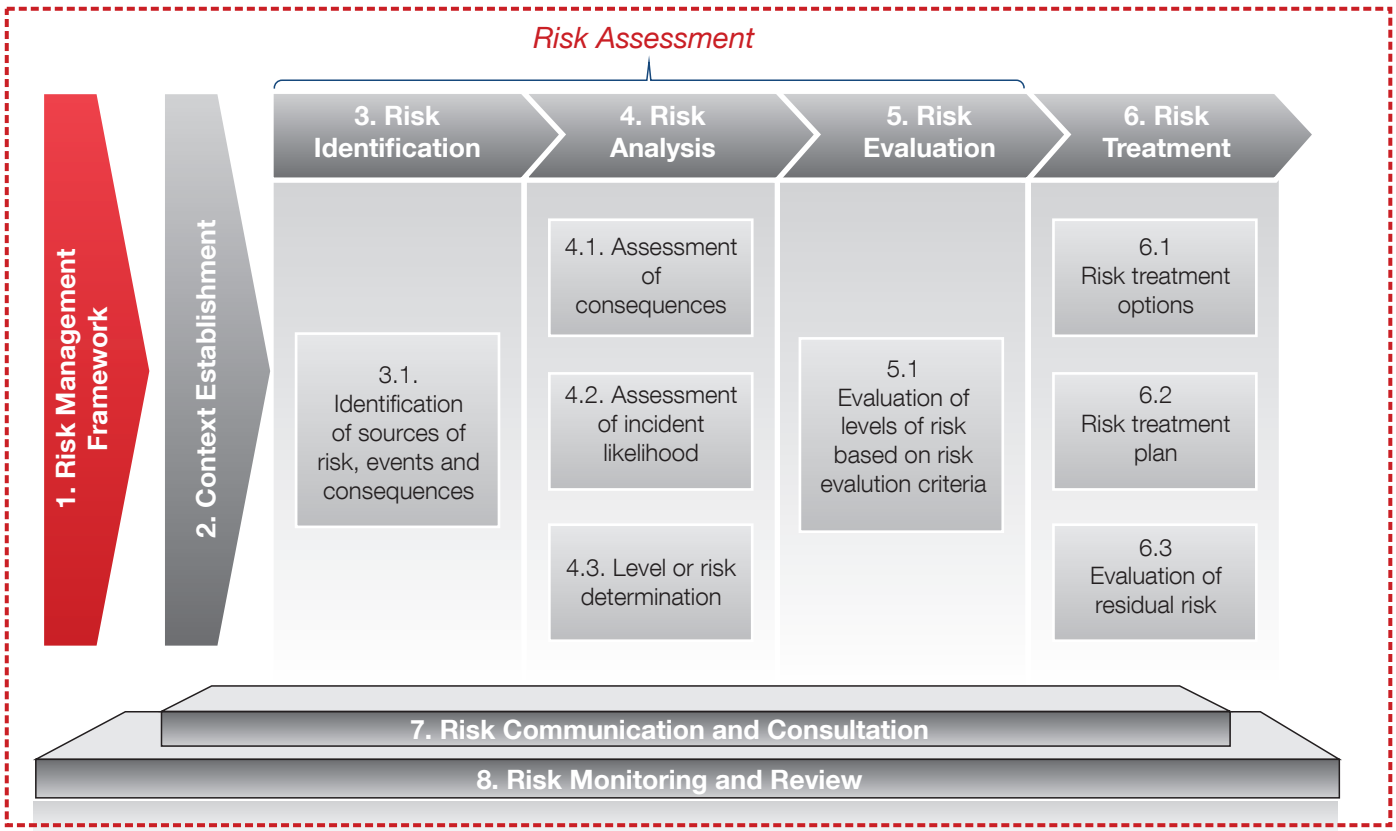
Based on the ISO 31000 framework, the ISO 27005 standard explains in detail how to conduct a risk assessment and a risk treatment, within the context of information security.

RISK MANAGEMENT – THE BUSINESS BENEFITS

As with all major undertakings within an organization, it is essential to gain the backing and sponsorship of executive management. By far the best way to achieve this, rather than through highlighting the negative aspects of not having risk management, is to illustrate the positive gains of having an effective risk management framework in place.

Risk management allows an organization to ensure that it knows and understands the risks it faces. The adoption of an effective risk management process within an organization will have benefits in a number of areas, examples of which include:

- Increased likelihood of achieving objectives
- Encouraged proactive management
- Awareness of the need to identify and treat risk throughout the organization
- Improved identification of opportunities and threats
- Compliance with relevant legal and regulatory requirements and international norms
- Improved mandatory and voluntary reporting
- Improved governance
- Improved stakeholder confidence and trust
- Establishment of a reliable basis for decision making and planning
- Improved controls
- Effective allocation and use of resources for risk treatment



IMPLEMENTATION OF RISK MANAGEMENT WITH PECB RISK MANAGEMENT FRAMEWORK

Making the decision to implement a risk management framework based on ISO 31000 is often a very simple one, as the benefits are well documented. By following a structured and effective methodology, an organization can be sure to cover all minimum practices required for the implementation of risk management programme. There is no single blueprint for implementing ISO 31000 that will work for every company, but there are some common steps that will allow you to balance the often conflicting requirements and prepare you for a successful certification audit.

PECB has developed a framework for risk management. It is called "PECB Risk Management Framework" and is based on applicable best practices.

...and experience for/of those ...related courses and exam.

Training title	Short description	Who should attend?
ISO 31000 Introduction	• One day training • Introduction to concepts of risk management • Does not lead to certification	• Practitioners wanting to understand ISO 31000 and gain a deeper knowledge of the risk management processes as described in the international standard • Staff involved in any stage of risk management program
ISO 31000 Risk Manager	• Three day training • Manage the implementation and management of risk management framework • 2 hour exam	• Risk managers • Business Process Owners • Business Finance Managers • Business Risk Managers • Regulatory Compliance Managers • Project Management

CHOOSING THE RIGHT CERTIFICATION:

The certified ISO 31000 Risk Manager credential is a professional certification for professionals needing to demonstrate the competence to implement, maintain and manage a risk management program according to ISO 31000.

Credential	Exam	Professional experience	Risk assessment experience
Provisional Risk Manager	Certified ISO 31000 Risk Manager Exam	None	None
Risk Manager	Certified ISO 31000 Risk Manager Exam	Two years One year of risk management related work experience	Risk management activities totaling 200 hours

PECB

+1-844-426-7322

customer@pecb.com

Customer Service