PECB

When Recognition Matters

WHITEPAPER

ISO 31000:2018

RISK MANAGEMENT – GUIDELINES

Principal Authors

- Eric LACHAPELLE, PECB
- Faton ALIU, PECB
- Enis EMINI, PECB

CONTENT

INTRODUCTION

The ability of predicting what the future holds and choosing effectively among varying alternatives lies at the center of contemporary societies and organizations. Risk management helps us navigate over a broad range of decision-making processes, from making investment decisions to safeguarding our health, from waging war to planning families, from paying insurance premiums to wearing a seatbelt when we drive, from planting sugar canes to promoting delicious sweets, and many other aspects of life.

Nowadays, people and organizations rely way less on traditions and superstition than they did in the earlier days, and this may not be due to mankind being more rational itself, but rather because of our ability to understand risk, which allows us to make more informed and rational decisions.

The opportunity to manage risk, including here the amount and type of risks that the organizations accept to pursue or retain in order to make forward-looking choices, are key ingredients that catalyze the progress of the economic system.

Risk is an inseparable part of any business which affects its operations and activities, leading them to implement proper risk management processes to effectively manage and treat such risks. Successful organizations are those that have the ability to identify and manage risks, before those risks become destructive actualities that impair the organization's reputation and its' ability to operate. Maybe one of the best ways to understand unexpected occurrences and the importance of properly responding to them is through the words of Arthur Rudolph, one of the scientists who developed the Saturn 5 rocket that launched the first Apollo mission to the moon:

"You want a valve that doesn't leak and you try everything possible to develop one, but the real world provides you with a leaky valve. You have to determine how much leaking you can tolerate"

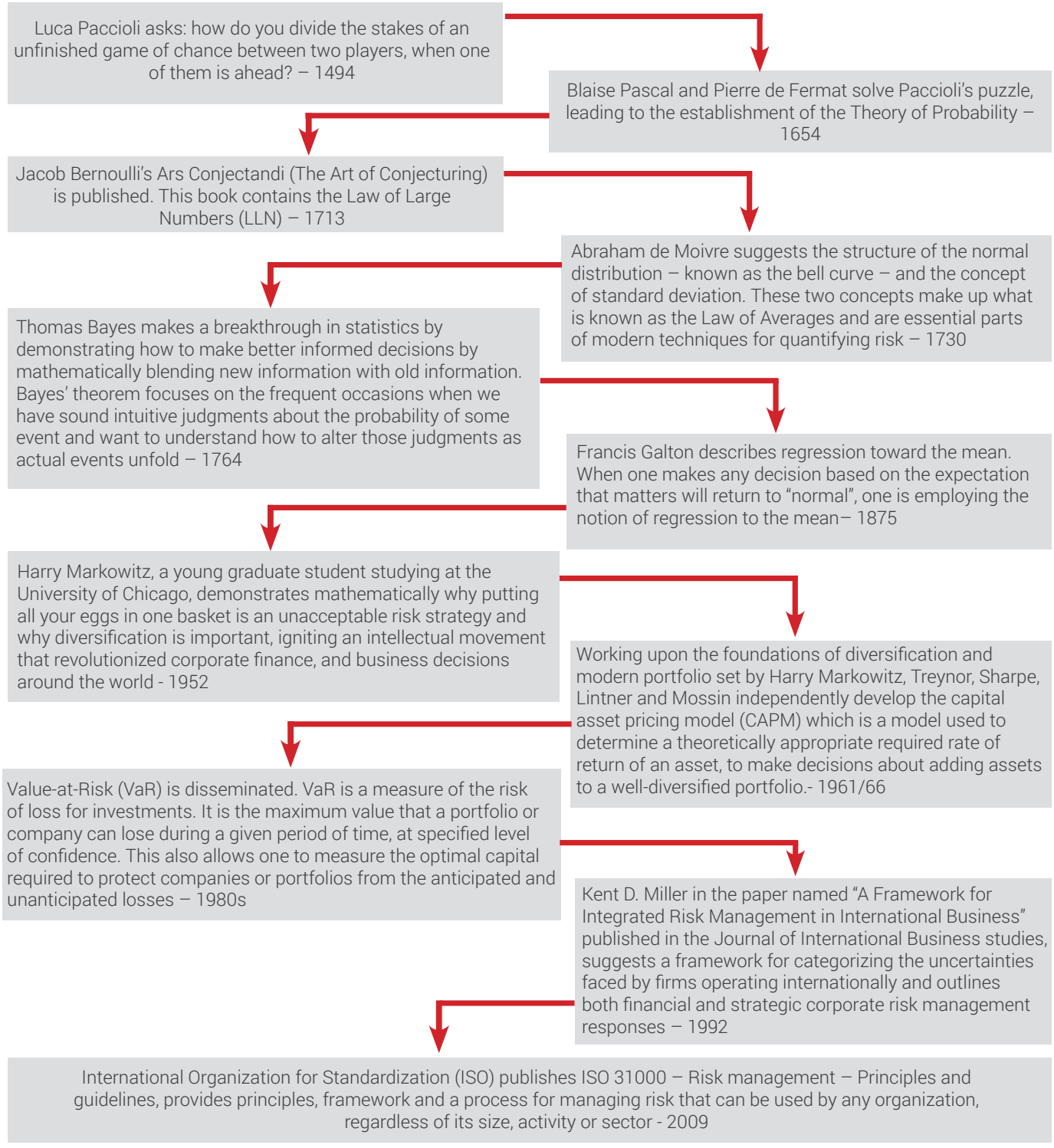
In the past, organizations generally identified and managed risks individually by employing different insurances as the means of preventing IT failures, breaches, and or legal risks. This can, at times, be insufficient and can contribute to the creation of a "silo" approach to the risk management, leading to a lack of coordination and potentially reducing the organization's ability to identify strategic and reputational risks.

The establishment of a risk management process and structure based on ISO 31000 can help organizations close operational gaps derived by risks through the creation of a holistic organization-wide approach to risk management that facilitates communication and provides the fundamental steps on how to design and implement a risk management framework, and how to continually improve the risk management framework by following the ISO 31000 guidelines.

A BRIEF HISTORY OF RISK MANAGEMENT

Mankind didn't always perceive and understand the concept of "risk", neither did it manage it in the way we do today.
The figure below presents some of the major milestones that led to our understanding of the concept of risk, the development of risk management methodologies and the way we perceive and treat risks nowadays.

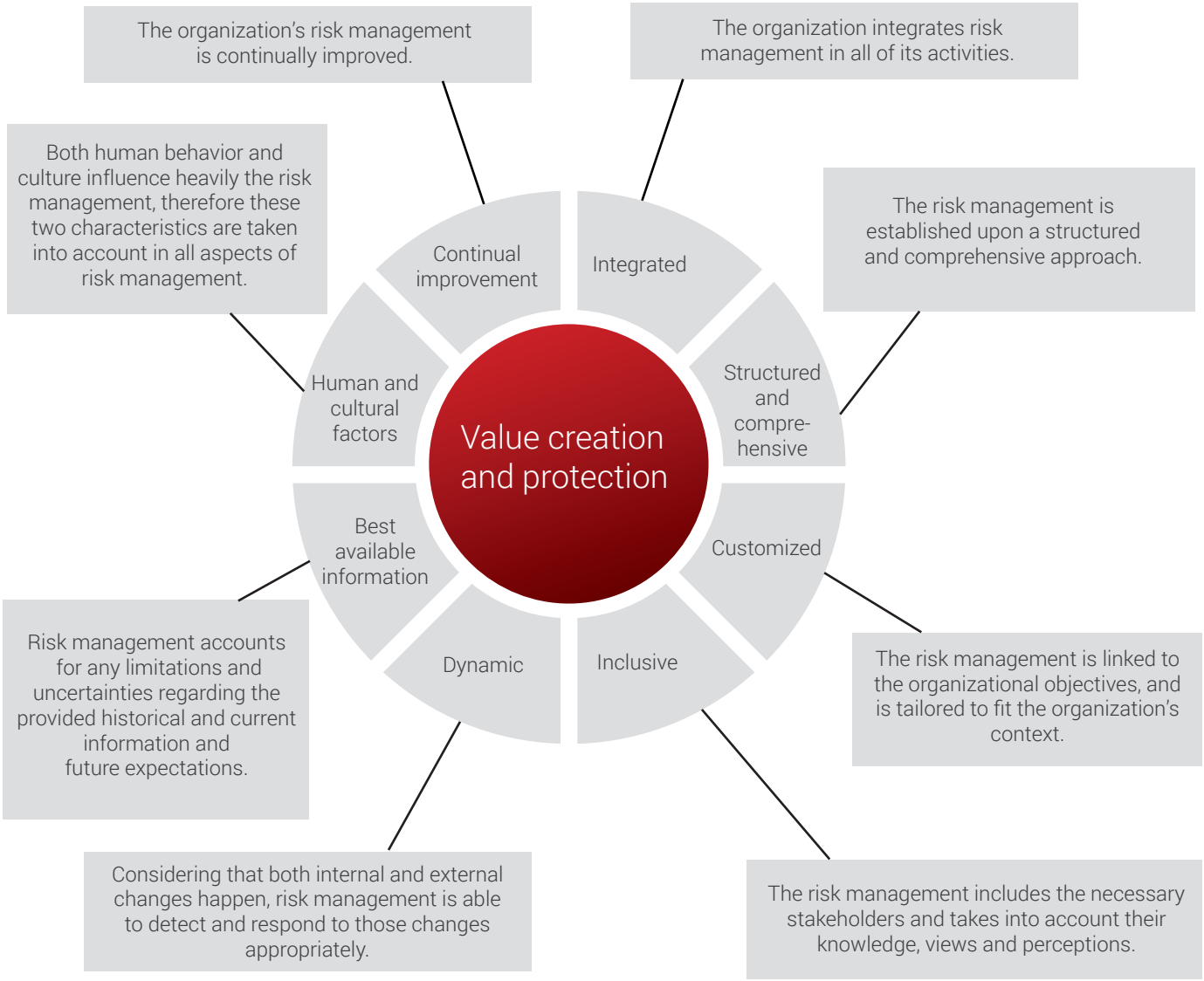
The timeline starts with a mathematical puzzle, created by a 15th century Italian mathematician and concludes with the publication of ISO 31000, which is the main subject of this whitepaper.



Risk Management Principles based on ISO 31000

Risk management is a management process that stimulates the cost-effective accomplishment of organization's objectives; furthermore, the standard also states that the purpose of risk management is the creation and protection of value. This leads us toward the question: How does a risk management process, based on ISO 31000, support organizations in the creation and protection of value, and consequently, in the achievement of organizational objectives? In addition to providing answers to such questions, ISO 31000 also provides a set of principles, a framework and a risk management process that the organizations can follow.
The standard proposes 8 principles which organizations should consider when establishing their risk management framework and processes.

The standard proposes 8 principles which organizations should consider when establishing their risk management framework and processes



Furthermore, the purpose of risk management principles provided by ISO 31000 is to link the framework and practice of risk management to the organization's strategic goals.

Risk culture

The risk management principles can also help in the creation of a risk culture within the organization.

But, what is the "risk culture"? The concept of risk culture is relatively new, meandering slowly into peoples' attention after the financial crisis of 2008. There are a myriad of questions surrounding this concept, and a lot of attempts to define in exact words what it represents. ERM Initiative Faculty defines risk culture as "the system of values and behaviors present in an organization that shapes risk decisions of management and employees". This, however, indicates that the concept remains rather ambiguous and abstract, and is yet to be seen whether it will become an organizational reality.

ISO 31000 does not attempt to define what risk culture is, and this may be mainly because of the novelty of this concept, and its similarity to the principle of "Human behavior and culture" presented in the standard. Therefore, the concept of risk culture is synthesized with the principle of human behavior and culture provided in the standard, referring to it simply as a risk culture while keeping in mind the synthesis.

Why is risk culture important?

1. Firstly, all organizations, in one way or another have adopted a risk culture, whether it is a proper one or a weak one. A proper culture most likely will lead toward the right risk outcomes, whereas a weak risk culture can lead to less satisfactory outcomes. Furthermore, the organization's risk culture will also either support or undermine the organization's success in the long term, or to translate it into the terminology of ISO 31000, it will determine whether the organization will create and protect value or not.

2. Secondly, organizations may spend considerable amount of time and resources in the development of rules, frameworks and processes, only to realize that those are misunderstood and not applied properly, either intentionally or due to the lack of the necessary knowledge and expertise. The organization's risk culture can be the catalyzer of an effective risk management process, and the promoter of informed risk-taking.

How can Risk Management activities be integrated into the organization's processes?

Integrating risk management can sometimes be difficult as it relies on the understanding of organizational structure and context. Organizational structures vary depending on the organization's purpose, aims, objectives and complexity.

What are the benefits of integrating the risk management process into the organization's operations and activities?

- Organizations will have a properly designed and implemented risk management framework that will ensure that the risk management process is part of all activities throughout the organization, including decision making, and that changes in external and internal contexts will be adequately captured.

- Organizations will be able to continually improve the suitability, adequacy and effectiveness of risk management framework and the way the risk management process is integrated.

- Organizations will have a risk management process that is an integral part of management and decision-making and is integrated into the structure, operations and processes of the organization.

Integrating risk management into an organization is an iterative and dynamic process that does not have a universal formula but needs to be customized to the organization's needs and culture. Therefore, risk management should be a part of, and not isolated from, the organizational purpose, governance, leadership and commitment, strategy, objectives and operations.

Having in mind that ISO 31000 does not provide requirements but only recommendations, organizations are allowed to choose what part of the recommendations they want to follow in order to manage risk properly. However, to properly identify, analyze, evaluate and treat the risks, PECB recommends to follow all recommendations of ISO 31000 and also provides training courses to enable risk managers to advance their skills and support organizations that they work for to align ISO 31000 standard objectives with organizations objectives.

Prior to selecting a risk management framework as the most suitable for the organization, the top management should identify the risk types that the organization faces, or may potentially face in the future. Depending on the nature and type of the organization, the industry and country in which it operates in, its day-to-day operations and activities, the risk management framework and processes can vary from one company to another. The ISO 31000, however, is suitable for each organization as it provides a universal framework and process to manage risk properly.

I. Identifying risk types

An organization aiming to implement a risk management process should be aware of all the risk types that have been or can be faced by the organization while they operate. This can be achieved by considering all of the past risk registers and identifying whether any risk from the past has been intertied or is still present. In case the organization does not have risk registers at all, the top management should provide the risk management team with enough information on what risks have been faced in the past and what were their sources. In case the organization has not faced any risk in the past, they still should identify potential risks so the organization does not have to suffer any consequences.

Some risk types presented by PECB that can be faced by organizations of any type include:

Operational risk – the loss resulting from inadequate procedures, policies, and systems within the organization

Financial risk – the process of coping with uncertainties that derive from financial markets

The main sources of financial risk include:

- The organization's exposure to changes in market prices;
- Actions and transactions with other organizations;
- Internal actions and organizational failures.

Credit risk - the loss that is generated due to the inability of the counterparty to meet its' obligations
Information technology risk – the operational, financial, and project failures due to the usage of new technology

Integration risk – the negative outcomes triggered by the integration of new processes and technology, and/or lack of communication

Security risk - the losses encountered due to the information security incidents or physical incidents

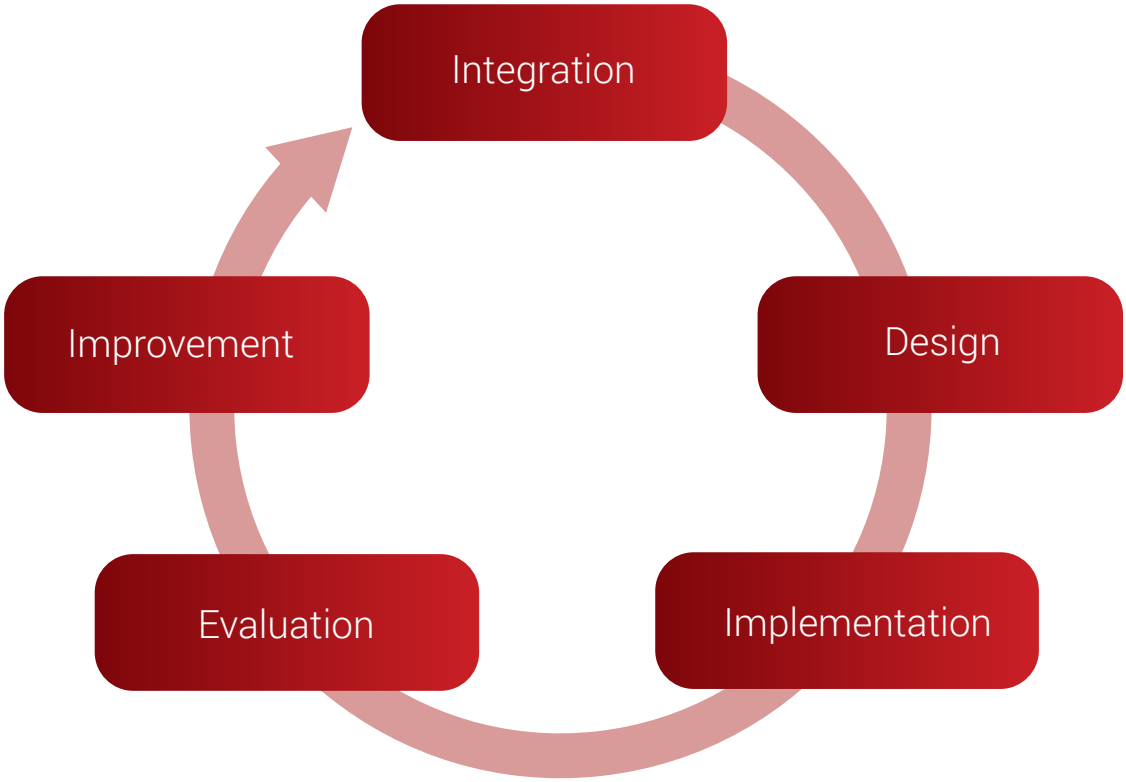
Legal risk – the risk that emerges because of the inability to comply with the applicable regulatory obligations

II. Designing a Risk management framework

After the risk management team has gained a comprehensive knowledge of the risk types that can be faced by the organization and the principles of risk management, they can start designing an appropriate risk management framework with the support and leadership of the organization's top management. The ISO 31000 underlines the development of a framework that will fully integrate the risk management process into an organization. The framework assures that an organization-wide process is supported, iterative and effective. That means that risk management will be an active component in governance, strategy and planning, management reporting processes, policies, values and culture. The framework is intended to be adapted to the particular needs and structure of all organizations, regardless of their size, and it is facilitated by leadership and commitment of the organization's top management. However, the commitment of the top management alone is not enough; therefore, the commitment of the whole organization needs to be pursued (a proper risk culture as discussed above).

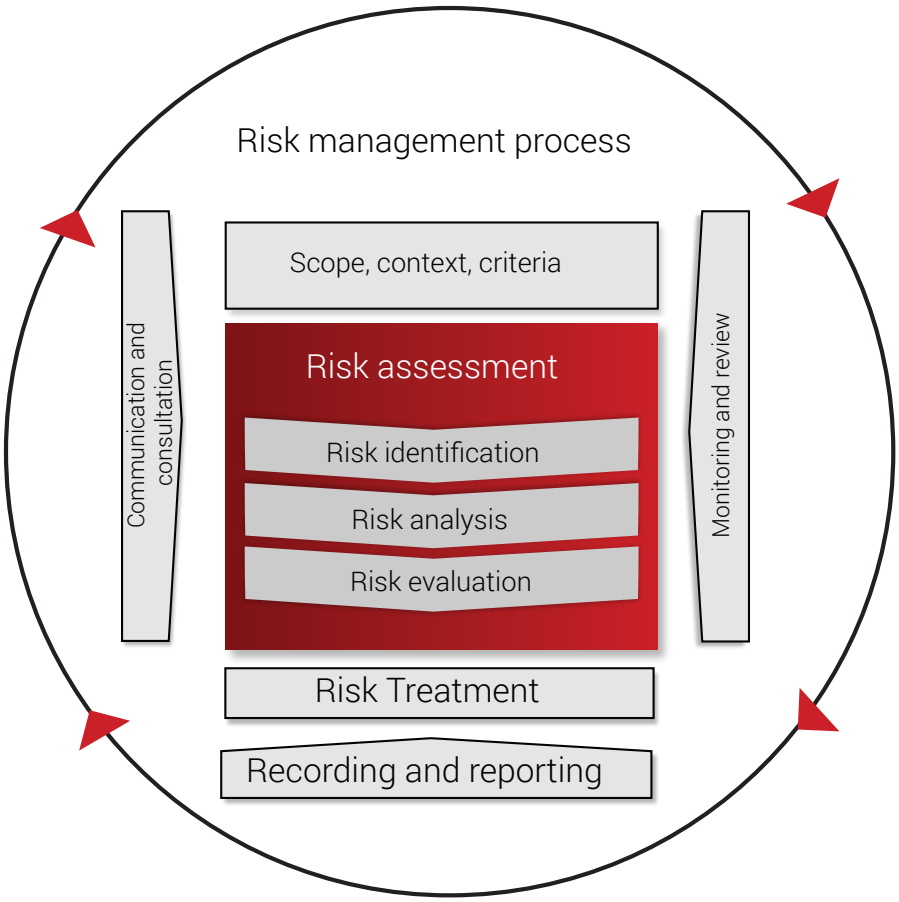
Successful implementation of the ISO 31000 risk management framework requires the engagement and awareness of stakeholders. This allows organizations to explicitly address uncertainty in decision-making, while also ensuring that any new or subsequent uncertainty can be taken into account as it arises.

The framework includes activities such as: demonstrating leadership and commitment to risk management, integrating risk management into organizational processes, designing the framework for managing risk (which includes understanding the organization and its context, articulating risk management commitment, assigning roles, authorities, responsibilities and accountabilities, allocating appropriate resources and establishing communication and consultation), implementing the risk management process, evaluating the risk management process and adapting and continually improving the framework.



III. Implementing the Risk management process

The organization's risk management process should involve the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk



The main purpose of the risk management process is to enable the organization to assess the existing or potential risks that may be faced, evaluate the risks by comparing the risk analysis results with the established risk criteria, and treat such risks using the risk treatment options. The organization should use such process in the decision making process

Steps to an effective implementation/integration of the Risk Management process:

Establishing the context: When establishing the context, the organization needs to take into account the organization's external environment (political, social, etc.) and internal environment (objectives, strategies, structures, ethics, discipline, etc.). The organization's context must be understood before the full range of risks can be identified. While establishing the context, the organization should define the purpose and scope of its risk management activities, and determine the objectives of the risk management process and the specific objectives of risk assessment. Furthermore, the organization should define the scope and boundaries related to the risk management process and identify all of the constraints that affect the scope. After identifying the constraints, the organization should define the risk criteria which will be used during the whole process.

Risk identification: The identification of risks should be a formal, structured process that includes risk sources, events, their causes and their potential consequences. Simply said, risk identification is about the creation of a comprehensive list of risks (both internal and external) that the organization faces, and can involve input from sources such as historical data, theoretical analysis, expert options, and stakeholder's needs. The risk identification process enables the organization to identify its assets, risk sources, risk events, existing measures and consequences. By identifying such elements the organization will be ready to begin the risk analysis process.

Risk analysis: The organization should analyze each risk that was identified in the previous step. Based on the level of risk that is determined after the risk analysis, the organization is able to define whether the risk is acceptable or not. As so, if the risk turns out to be unacceptable, the organization can take actions to modify the risk to correspond to the acceptable level of risk.

The organization should use a formal technique to consider the consequence and likelihood of each risk, and these techniques can be qualitative, semi-quantitative, quantitative, or a combination thereof, based on the circumstances and the intended use.

Risk evaluation: This step offers the organization the opportunity to have a mechanism that helps them rank the relative importance of each risk, so that a treatment priority can be established.

Risk treatment: Proper risk management requires rational and informed decisions about risk treatment. Typically, such treatments include: avoidance of the activity from which the risk originates, risk sharing, managing the risk by the application of controls, risk acceptance and taking no further action, or risk taking and risk increasing in order to pursue an opportunity.

Remember that organizations do not always find themselves in trouble because of their excessive and reckless behavior. Sometimes organizations fall behind their competitors as a result of their reluctance to take risks and pursue opportunities.

Communication and consultation: Proper risk management requires structured and ongoing communication and consultation with those affected by the organization's operations. The communication seeks to promote awareness and understanding of risk and the means to respond to it, whereas consultation involves obtaining feedback and information to support decision-making.

Recording and reporting: Another step of the risk management process based on ISO 31000 is the recording and reporting, i.e. the outcomes of the risk management process are to be documented and reported through appropriate mechanisms. Recording and reporting is important for reasons such as communication of the risk management activities and outcomes pertaining to those activities throughout the organization and providing the necessary basis and information for making informed decisions.

Monitor and review: Considering that both the external and internal environment are subject to constant change, the purpose of this step is to help organizations assure and improve the quality and effectiveness of the risk management process.

Monitoring includes actions such as examining the progress of treatment plans, monitoring the established controls and their effectiveness, ensuring that activities which are proscribed are being avoided, and checking that the environment has not changed in a way that affects the risks.

Summary

During the last few years, the importance of risk management as part of a strong corporate governance has been increasingly acknowledged and brought into attention. The tumult at the beginning of the 21st century, mainly with the collapse of multinational organizations and then the 2008 financial crisis, showed the need for increased awareness on the uncertainty factors related to the operational environment and behavior of the organizations.

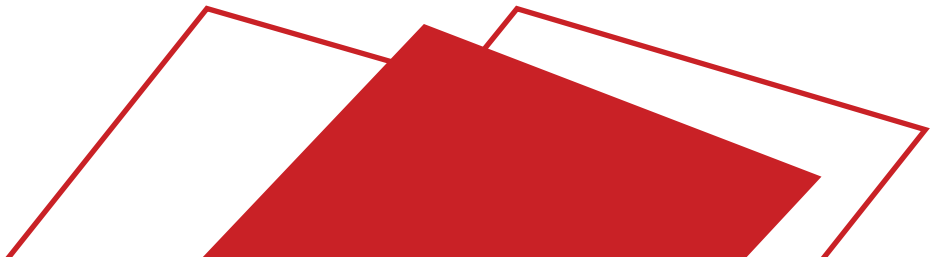
These events displayed the need for a "tool" that would establish a foundation and the means necessary to prevent organizations from engaging in reckless behavior, causing dreadful consequences, but at the same time support them in pursuing opportunities, making informed decisions, and prospering in the current economic system.

This "tool" came in the form of ISO 31000 (the first standard in the family of risk management standards), an international standard that was published by ISO for the first time in 2009, and then revised and published in 2018.

ISO 31000 was developed with the aim of providing best-practice structure and guidance to all operations concerned with risk management and targets the people who create and protect value in organizations through managing risks, making decisions, setting and achieving objectives and improving performance. The standard contains a set of principles, a comprehensive risk management framework and a risk management process which we have discussed in this whitepaper.

It is understandable that the application of ISO 31000 alone is not going prevent bad business decisions or even another global financial crash.

But one thing that can be acknowledged is that the ISO 31000 certainly offers the organizations an opportunity to understand the causes and identify the necessary treatments required to reduce the uncertainty of their future.



Training and certification of professionals

PECB has created a training roadmap and personnel certification schemes which are strongly recommended. The certification of individuals serves as a documented evidence of professional competencies and experience, while also demonstrating that the individual has attended one of the related courses and successfully completed exams.

Personnel certifications demonstrate that the professionals have gained competencies based on best practices. The certifications allow the organizations to make informed selections of employees or services based on the competencies that are represented by the certification designation. Finally, they provide incentives for the professionals to constantly improve their skills and knowledge, and serve as a tool for employers to ensure that the training and awareness sessions have been effective.

PECB training courses are offered globally through a network of authorized training providers and they are available in several languages. The table below gives a short description of the PECB official training courses for Risk Management based on ISO 31000.

Training title	Short description	Who should attend?
ISO 31000 Introduction	The ISO 31000 Introduction training course enables you to comprehend the basic concepts of Risk Management.	• Individuals interested in Risk Management • Individuals aspiring to gain knowledge about the main Risk Management processes
ISO 31000 Foundation	The ISO 31000 Foundation training enables you to learn the basic elements of implementing a Risk Management process and framework. During this training course, you will be able to understand the fundamental Risk Management strategies.	• Individuals involved in Risk Management • Individuals seeking to gain knowledge on the main Risk Management processes • Individuals interested to pursue a career in Risk Management
ISO 31000 Lead Risk Manager	The ISO 31000 Risk Manager training enables you to gain comprehensive knowledge of the fundamental principles, framework and process of Risk Management based on ISO 31000. During this training course, you will also gain a thorough understanding of the best practices of Risk Management and be able to effectively apply them in an organization in order to successfully implement a Risk Management process.	• 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
ISO 31000 Lead Risk Manager	The ISO 31000 Lead Risk Manager training enables you to acquire the expertise to support and lead an organization and its team to successfully identify, understand and manage a risk process based on ISO 31000. During this training course, you will also gain comprehensive knowledge of the best practices used to implement a Risk Management framework that provides the foundation for designing, implementing, monitoring, reviewing and continually improving a Risk Management process in an organization.	• Managers or consultants seeking to master their skills to support an organization during the implementation of a Risk Management framework and process based on ISO 31000 • Professionals responsible for the effective management of risk within an organization • Expert advisors seeking to gain comprehensive knowledge of the key concepts, processes and strategies of Risk Management • Individuals responsible for establishing a Risk Management policy • • Risk Management team members

PECB

+1-844-426-7322

customer@pecb.com

Help Center

www.pecb.com