



The Standard: ISO 31000 and its Revision



In a world of constant change, risk management is increasingly viewed as a means of improving the likelihood of success in the challenging task of managing the organization's reputation and stakeholder's interest. The unmanaged risk is the greatest source of waste, where as a result thousands of jobs and expertise get lost, and many great companies fail to survive; consequently, standards are considered to be very beneficial since their implementation allows the organizations to compare their existing risk management practices with internationally recognized benchmarks. The ISO 31000 standard should be the first step that shows organization's commitment to ensuring the evolvement of risk management. Therefore, it serves as a guide for identifying and prioritizing important risks. Risk management process is applicable to organizations of all sizes and types, and it is intended to be tailored to meet the varying needs of the organization.

Key Points for an Effective Risk Management Plan

Understanding the value of risk management helps organizations to achieve higher levels of efficiency, flexibility and transparency.

An effective Risk Management includes the following:

- Creates shareholders value by linking risk with organizational performance;
- Established common objectives and clear understanding of the effect of the potential risks;
- Involvement of organization's members in crucial decision-making processes;
- Effective risk assessment process and continuous improvement;
- Increased risk awareness, and incorporation of risk into the organization's culture;
- Appropriate risk management measures that continuously facilitate the detection and updating process of the risks and relevant actions to treat such risks.



The Purpose of ISO 31000

ISO 31000 specifies principles and guidelines of risk management to identify, assess and mitigate risks faced by organizations. It is designed to help organizations ensure conformity with legal and regulatory requirements and international norms. In addition, it increases the possibility of achieving organizational objectives, improves the identification of threats and opportunities, and helps an organization in treating the risks and minimizing the negative impact.

The standard consists of two related documents: ISO Guide 73 and ISO/IEC 31010. The ISO Guide 73 provides definitions and terms that are linked to Risk Management while ISO/IEC 31010 entails risk assessment techniques. This standard provides guidance on how to appropriately identify and manage risks in order to minimize losses and maximize the opportunities. It outlines the principles for effective risk management and a framework for supporting the implementation of continual improvement.

Risk management capabilities can directly affect the costs incurred by the organization, as well as the customer value creation. By effectively managing the uncertainties which occur in the business environment, those capabilities can turn into a source of competitive advantage.

The ability to respond faster to unforeseen events and the willingness to seek greater risks which competitors are not capable of undertaking, gives the organization the opportunity to enhance future profits. Furthermore, risk management is considered as a core aspect of project management process, as it is viewed as a promising tool for protecting organization's reputation and brand, and improving the sustainability and resilience of the organization.

John Roos a Project, Program and Quality specialist stated "ISO benefits exceed the simple satisfaction of having just another certificate on your wall. If such benefits are recognized and acknowledged, the management will provide approval and support to ISO as this ensures the use of professional methods and techniques, and simultaneously a high quality standard".



A structure preview of the ISO 31000

ISO 31000 consists of principles that may be considered as the cornerstone based on which organization's success is built upon; a Risk Management framework comprising 5 components which ensure that the process for managing risk is fully integrated into the organization; and Risk Management processes that emphasize the necessity for active communication and consultation with internal and external stakeholders, and the continuous monitoring and review.

The detailed components of the ISO 31000

11 Principles of Risk Management

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

Risk Management Framework

- Policy and Governance
- Program Design
- Implementation
- Monitoring and Review
- Continual Improvement

Risk Management Process

- Communication and consultation
- Establishing the context
- Risk identification
- Risk analysis
- Risk evaluation
- Risk treatment
- Monitoring and review

