riskza
corporate sustainability

ISO 31000:2018 RISK MANAGEMENT: HOW DO I GET STARTED?

info@riskza.com | www.riskza.com | 0861 RISK ZA | 28 Siphosethu Road, Mt. Edgecombe, KZN

CONTENTS

GETTING STARTED WITH RISK MANAGEMENT

INTRODUCTION

When Tony Hayward became CEO of BP, in 2007, he vowed to make safety his top priority. He instituted rules that all employees use lids on coffee cups while walking and refrain from texting while driving. Three years later, on Hayward's watch, the Deepwater Horizon oil rig exploded in the Gulf of Mexico, causing one of the worst man-made disasters in history.

A U.S. investigation commission attributed the disaster to management failures that crippled "the ability of individuals involved to identify the risks they faced and to properly evaluate, communicate, and address them."

Hayward's story reflects a common problem. Risk management is often treated as a compliance issue that can be solved by drawing up lots of rules and making sure that all employees follow them. In truth, rules-based risk management will not diminish either the likelihood or the impact of a disaster such as Deepwater Horizon.

ABOUT ISO 31000:2018 RISK MANAGEMENT

PRINCIPLES AND GUIDELINES

Risk management should play a key role in strategic management, which is why enterprise risk management (ERM) and the ISO 31000 guidelines for risk management have emerged. ISO 31000:2018 defines risk as 'the effect of uncertainty on outcomes'. Identifying risks and determining ways to respond to them helps enterprises to learn about their processes, the organisation, and the environment in which they operate. The practice also raises awareness of how things might change in the future, and prepares businesses for negative events and opportunities.

The International Organization for Standardization revised ISO 31000:2009 and released the current version in February 2018 to bring risk management principles up to date with the contemporary business context and the future threats the rapidly changing environment might present.

EFFECTIVE RISK MANAGEMENT

Implementing effective risk management systems requires that an organisation develops specific structures and processes in order to plan and control risk in a systematic way, at all levels of management. The ISO 31000:2018 risk management guidelines can be customised and applied to any organisation and its context, and it is not sector specific. In other words, the risk management principles contained in ISO 31000:2018 do not replace standards that are used to manage specific risks in areas such as the environment, and occupational health and safety. Rather, the standard is a high-level document that supports existing ISO management systems standards, and can be used to integrate risk into existing management activities. Adopting consistent processes within a comprehensive framework can help to ensure that risk is managed effectively, efficiently and coherently across an organisation.

The 2018 version of the standard has been significantly shortened, and complicated terminology has been simplified. It includes improvements by taking into consideration human and cultural factors that can affect an organisation's ability to achieve its objectives, and emphasises the importance of embedding risk management in decision-making processes at all levels of management in an enterprise. It also includes cross-cutting activities like communication and consultation, monitoring and review.

The standard is intended to be used by a wide-range of people who create and protect value by managing risks, making decisions, setting and achieving objectives, and improving performance. The standard provides a set of voluntary guidelines, which cover:

1. Risk Management Principles
2. Risk Management Framework
3. Risk Management Process

WHAT DOES ISO 31000:2018 HELP ORGANISATIONS TO ACHIEVE?

When properly implemented and applied, ISO 31000:2018 assists organisations to:

- Increase the likelihood that objectives will be achieved.
- Improve the ability to identify threats and opportunities.
- Improve the overall resilience of the organisation.
- Improve operational efficiency and effectiveness.
- Encourage employees to identify and treat risk.
- Improve risk management controls.
- Comply with legal and regulatory requirements.
- Improve the effectiveness of governance activities.
- Establish a sound basis for planning and decision making.
- Improve loss prevention and incident management activities.
- Encourage and support continuous organisational learning.
- Improve the trust and confidence of stakeholders.
- Enhance both mandatory and voluntary reporting.
- Comply with international norms and standards.

ISO 31000:2018 RISK MANAGEMENT PRINCIPLES

The standard states that the purpose of risk management is to create and protect value. A total of eight principles are presented in the standard, which are described below:

1. Framework and processes should be customised and proportionate.
2. Appropriate and timely involvement of stakeholders is necessary.
3. A structured and comprehensive approach is required.
4. Risk management is an integral part of all organisational activities.
5. Risk management anticipates, detects, acknowledges and responds to changes.
6. Risk management explicitly considers any limitations of available information.
7. Human and cultural factors influence all aspects of risk management.
8. Risk management is continually improved through learning and experience.

The first five principles provide guidance on how a risk management initiative should be designed; principles six, seven and eight relate to the way in which the risk management process should work.

CULTURE AND BEHAVIOUR

One message is very important: an aim of ISO 31000:2018 is to create and build a culture that focuses on identifying and managing risks. Why is risk culture important?

1. A strong risk culture will most likely lead an organisation towards the right risk outcomes, whereas a weak risk culture can lead to less satisfactory or harmful outcomes.The organisation's risk culture either supports or undermines the organisation's success in the long term, or in the words of ISO 31000:2018: *it will determine whether the organization will create and protect value or not.*
2. Organisations may spend time and resources developing rules, frameworks and processes, only to discover that they are not understood or applied properly. The organisation's risk culture is the catalyst for an effective risk management process, and promotes informed risk-taking.

INTEGRATING RISK MANAGEMENT ACTIVITIES INTO ORGANISATIONAL PROCESSES

By integrating risk management into an organisation's processes, the task becomes iterative and dynamic. This is beneficial as:

- A properly designed and implemented risk management framework will ensure that the risk management process is part of all activities throughout the organisation, and that changes in external and internal contexts will be adequately captured.
- Organisations will be able to continually improve the suitability, adequacy and effectiveness of risk the management framework, and the way the risk management process is integrated.
- Organisations 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 organisation.

DESIGNING A RISK MANAGEMENT FRAMEWORK

Once organisational risks have been adequately identified, ISO 31000:2018 underlines developing a framework that supports an organisation-wide risk management process that is iterative and effective. This means that risk management will be an active component in governance, strategy and planning, management reporting processes, policies, values and culture.

Successfully implementing the ISO 31000:2018 risk management framework requires that all employees in an organisation are engaged in and aware of the process. The framework should include activities such as:

- Demonstrating leadership and commitment to risk management;
- Integrating risk management into organisational processes;
- Designing the framework for managing risk;
- Implementing the risk management process;
- Evaluating the risk management process; and
- Adapting and continually improving the framework.

IMPLEMENTING THE RISK MANAGEMENT PROCESS

The purpose of the risk management process is to help organisations assess the existing or potential risks that they may face, evaluating these risks by comparing the risk analysis results with the established risk criteria, and treating risks using risk treatment options.

8 STEPS TO EFFECTIVELY IMPLEMENTING THE RISK MANAGEMENT PROCESS

1. Establishing the organisational context. External and internal environment; Purpose and scope of the risk management activities; Scope and boundaries related to the risk management process.
2. Risk identification. Identifying risks should be a formal, structured process that includes risk sources, events, their causes and their potential consequences.
3. Risk analysis. Analyse each risk identified in the previous step to establish whether the risk is acceptable or not, and take actions to modify the risk to correspond to an acceptable level of risk.
4. Risk evaluation. Rank the relative importance of each risk, so that a treatment priority can be established.
5. Risk treatment. 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.
6. Communication and consultation. A structured and ongoing communication and consultation process with those involved in the organisation's operations to promote awareness and understanding of risk and the means to respond to it, and obtaining feedback and information to support decision making.
7. Recording and reporting. Document and report on the outcomes of the risk management process to facilitate informed decisions.
8. Monitor and review. The purpose of this step is to help organisations assure and improve the quality and effectiveness of the risk management process.

SUMMARY

The importance of risk management as part of strong corporate governance has been increasingly acknowledged over the past decade. The global financial crisis of 2008, and other similar events, highlighted the need for a "tool" that would assist organisations to avoid engaging in reckless behaviour.This "tool" came in the form of ISO 31000:2009 and the revised version published in February 2018. Although ISO 31000:2018 alone will not prevent bad business decisions, it offers organisations an opportunity to understand the causes and identify the necessary treatments required to reduce the uncertainty of their future, and improve business performance.

HOW CAN RISK ZA HELP?

TRAINING OF RISK PROFESSIONALS

Risk ZA offers an **Enterprise Risk Assessor** training course based on ISO 31000 and 31010.

This course has been developed to assist organisations manage risk in all aspects of their operations. The methodologies taught are internationally recognized best practice, including the framework proposed by ISO 31000:2018 and techniques recommended by IEC/DIS 31010.

The following International Standards require competent risk assessors:
- ISO 9001:2015 - Quality Management
- ISO 14001:2015 - Environmental Management
- ISO 45001:2018 - Occupational Health and Safety Management (Replacing OHSAS 18001)
- FSSC ISO 22000 – Food Safety Management
- ISO 39001:2012 - Road Traffic Safety Management

WHO SHOULD ATTEND

By promoting a universally appropriate approach to performing risk assessments the course is appropriate for delegates from all industries. The course should be attended by all staff involved with the performance or review of risk assessments, from coordinators to managers.

Competence and knowledge should be shared through the levels of the organisation.

Contact us to discuss which of our ISO 31000:2018 training course/s would best suit you and your organisation: +27 (0) 31 569 5900 or info@riskza.com