Simplifying Compliance

Introduction to ISO 31000:2018 Risk Management

Photo by Vlad Fonsark from Pexels

Table of Contents

Introduction 2
Why ISO 31000 was revised 3
What are the Main Differences? 3
The Main Changes Considered 4
ISO 31000 Risk Management Principles, Framework and Process 5
Risk Management Principles 6
Risk Management Framework 7
Risk Management Process 8
Key Benefits of Risk Management 9
Conclusion 10
Next Steps 11

Introduction

This Guide has been produced to provide an overview of ISO 31000:2018 standard, to help organisations develop and implement an effective Risk Management strategy

The International Organisation for Standardisation (ISO) has published a revision of its ISO 31000 standard, providing more strategic guidance than its predecessor ISO 31000:2009, placing more emphasis on the involvement of senior management and the integration of risk management into the organization.

The purpose of ISO 31000 is to provide principles and generic guidelines on risk management, and aims to deliver a single universally recognised standard for practitioners and companies employing risk management processes to replace the numerous existing standards, methodologies that varied between industries, subject matters and regions.

What is Risk Management?

- The identification, evaluation and prioritisation of risk to prevent injuries or illness, and the possibility of losing something of value including, protecting financial assets, and social status.

- Risks can come from various sources including uncertainty in financial markets, legal liabilities, accidents, natural causes and disasters, deliberate attack from an opposition, or project failures.

- There are two types of events

    1. Negative events classified as risks
    2. Positive events classified as opportunities

The purpose of risk management is to minimise, monitor, and control the probability or impact of unfortunate events (a risk becoming an issue) or to maximise the realisation of an opportunity.

Risks affecting organisations can have consequences in terms of damage to professional reputation, economic performance as well as environmental, safety and societal outcomes. Therefore, managing risk effectively helps organisations to perform well in an environment full of uncertainty.

The updated version of risk management guidelines released in February 2018 has been developed to help organisations manage the uncertainty.

Why ISO 31000 was revised

ISO assurances is to “keep risk management simple” and “deliver a clearer, shorter and more concise guide that will help organisations use risk management principles to improve planning and make better decisions.”

ISO 31000 can be used to better position an organisation so it can best achieve objectives, improve the identification of threats, identify opportunities, and effectively allocate resources in the management of risk

The revised version of ISO 31000 published in **February 2018** takes into account the evolution of the market and new challenges faced by business and organisations in today’s digital age, and major advancement in technology since the standard was first released in 2009.

One example of this is the increased complexity of economic systems and emerging risk factors such as digital currency, both of which can present new and different types of risks to an organisation on an international scale.

What are the Main Differences?

ISO 31000:2018 provides a more strategic guidance than its predecessor, with more emphasis on both the involvement of senior management and the integration of risk management across the organisation. This includes the recommendation to develop a statement or policy that confirms a commitment to risk management, assigning authority, responsibility and accountability at the appropriate levels within the organisation and ensuring that the necessary resources are allocated to managing risk.

The standard now recommends that risk management is part of the organisation’s structure, processes, objectives, strategy and activities.
It places a greater focus on creating value as the key driver of risk management and features related principles such as continual improvement, the inclusion of stakeholders, being customised to the organisation and consideration of human and cultural factors.

The content has been streamlined to reflect an open systems model that regularly exchanges feedback with its external environment in order to fit a wider range of needs and internal parameters that organisations must consider when managing risk.

The key objective is to make things clearer and easier, using plain language to define the fundamentals of risk management in a way that the reader will find easier to comprehend.

A lot of the complicated language has been eliminated, so the text is cleaner and more precise with the expectation that the reader will find it simpler to understand.
The terminology in this revised standard is now more concise, with certain terms being moved to ISO Guide 73, risk management, which deals specifically with risk management terminology.

Work has commenced on a terminology standard and implementation handbook to further enhance the understanding and applicability of the standard.

Risk is now defined as the “effect of uncertainty on objectives”, which focuses on the effect of incomplete knowledge of events or circumstances on an organisation’s decision making. This requires a change in the traditional understanding of risk, forcing organisations to tailor risk management to their needs and objectives, as a key benefit of the standard.

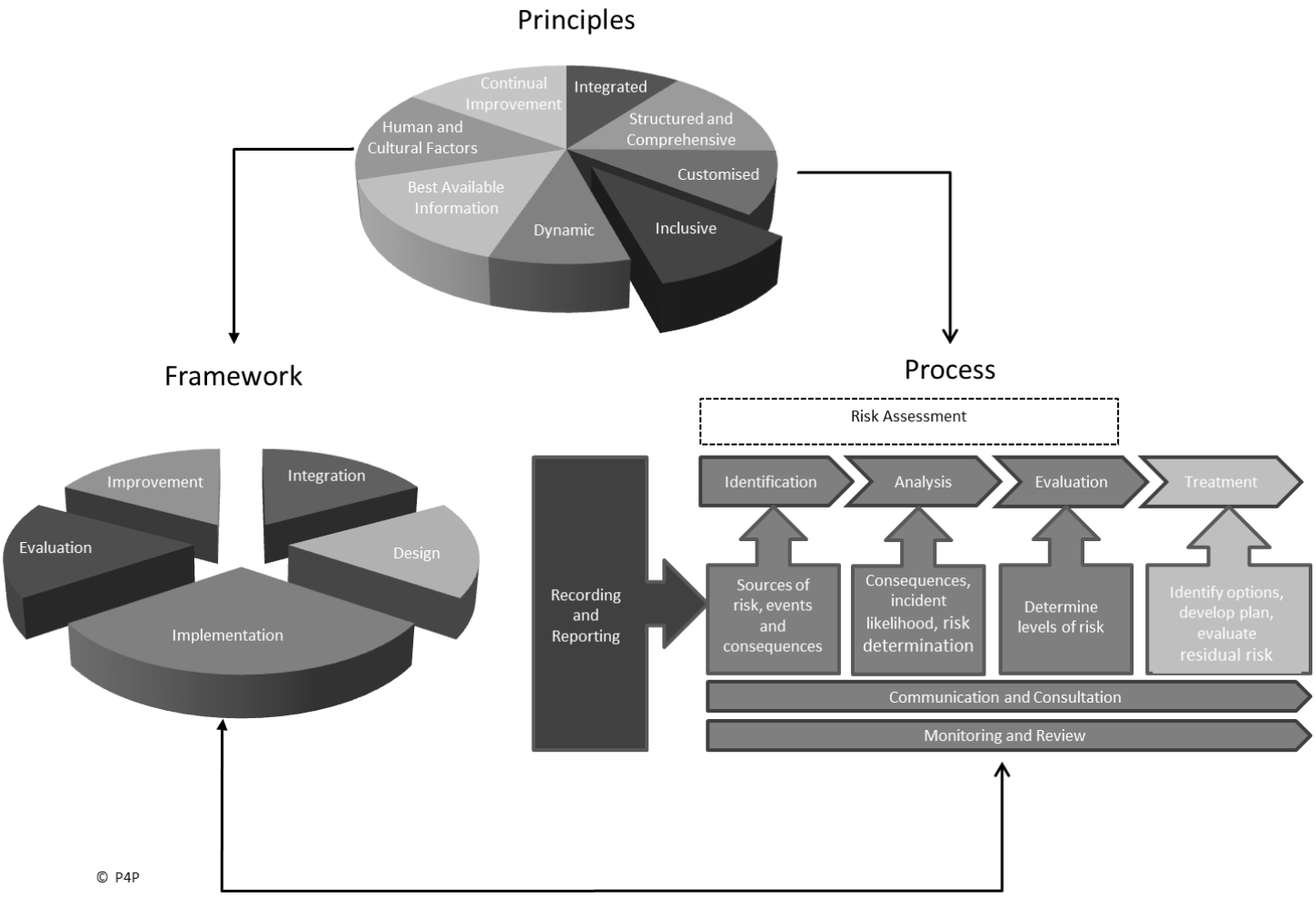
The Main Changes Considered

1. Review of the principles of risk management, which are the key criteria for its success
2. Focus on leadership by top management, and executives who should ensure that risk management process is fully is integrated across all areas and levels of the organisational activities, starting with the governance of the organisation, then strongly aligned with its objectives, strategies and culture
3. Greater emphasis on the iterative nature of risk management, drawing on new experiences, knowledge and analysis that can lead to a revision of process elements, actions and controls at each stage of the process
4. Streamlining of the content with greater focus on sustaining an open systems model that can regularly exchange feedback externally to fit multiple needs and contexts.
5. The revised version provides strong guidance to help executives take a proactive stance on risk and ensure that risk management is integrated into all aspects of decision making at all levels of the organisation. This includes business continuity, compliance, crisis management, HR, IT and organisational resilience.
6. Emphasise on the value of measuring, evaluating success and improving the risk management system. The idea is not to get everything right the first time, but to improve it every time the cycle is completed.

The revised standard is not just a new version of ISO 31000 but serves to provide a whole new meaning to the way we will manage risk tomorrow.

The risk management framework and process should be integrated with other business management systems to ensure consistency and effective management control across all areas of the organisation.
Organisation should consider including strategy and planning, IT, corporate governance, HR, compliance, quality, health and safety, business continuity, crisis management and security.

ISO 31000 Risk Management Principles, Framework and Process

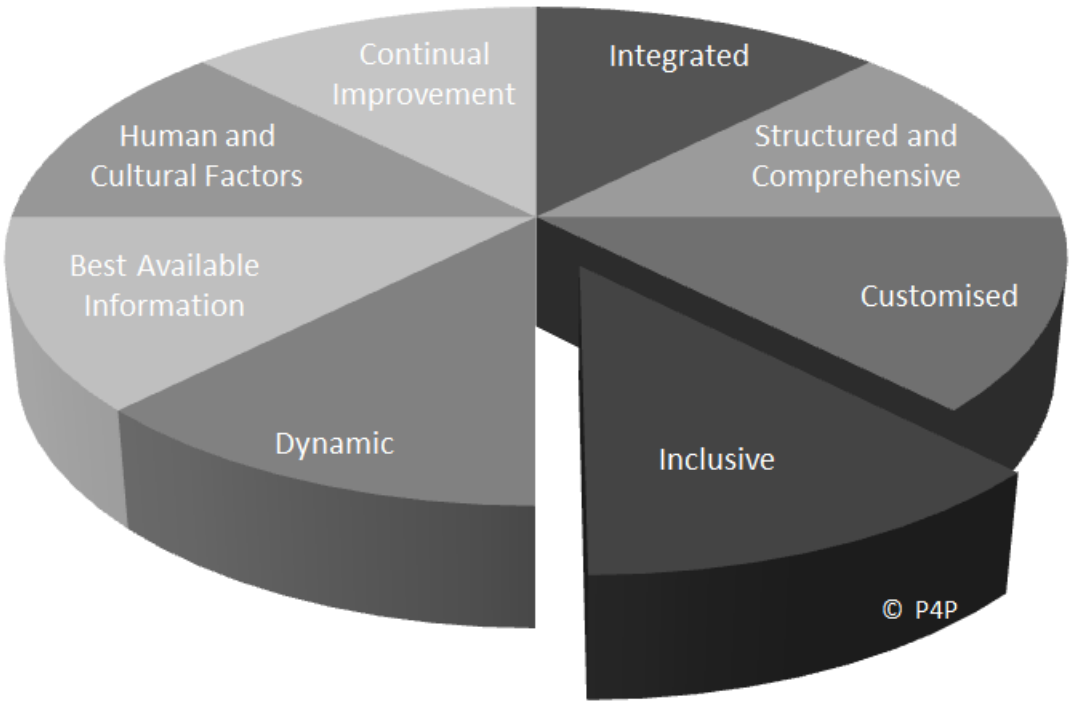


Risk Management Principles

The Principles provide guidance for managing risk

- **Integrated** as part of organisations daily activities
- A **structured and comprehensive** approach for consistent results
- **Customised** to meet organisations internal and external circumstances
- **Inclusive** so the knowledge views and of ideas of all stakeholders are considered to improve risk management awareness

Value Creation and Protection



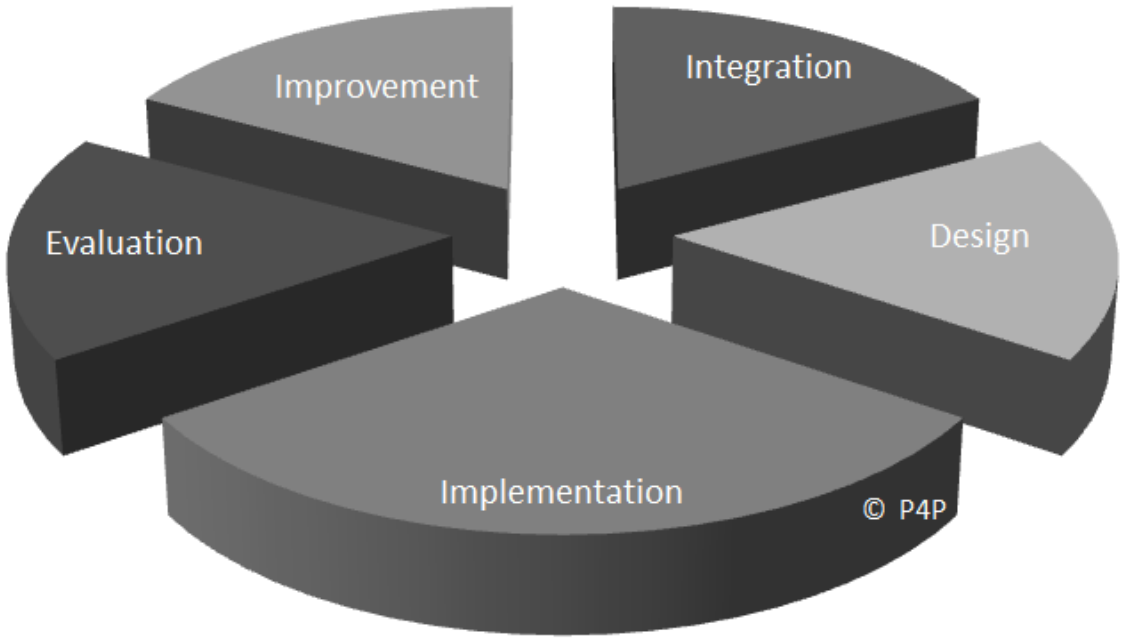
- **Dynamic** to enable appropriate quick response to risk events
- **Best available** current and historical **information**, along with future expectations should be timely, clear and available to stakeholders
- **Human and cultural factors** have an essential influence all aspects of risk management
- **Continual improvement** through learning and experience

Risk Management Framework

The Framework helps integrating risk management with daily activities and functions

- Senior management should show Leadership and commitment to ensure that risk management is integrated into all organisational activities
- **Integration** of risk management is a dynamic and iterative process, and should be customised to the organisation's objectives and operations
- **Design** of the risk management framework includes internal and external considerations. This includes data information systems, interdependencies, organisational structure, roles and accountabilities
- **Implementation** of the risk management framework requires planning and resources to ensure the right decisions are made by the right people at the right time

Leadership and Commitment



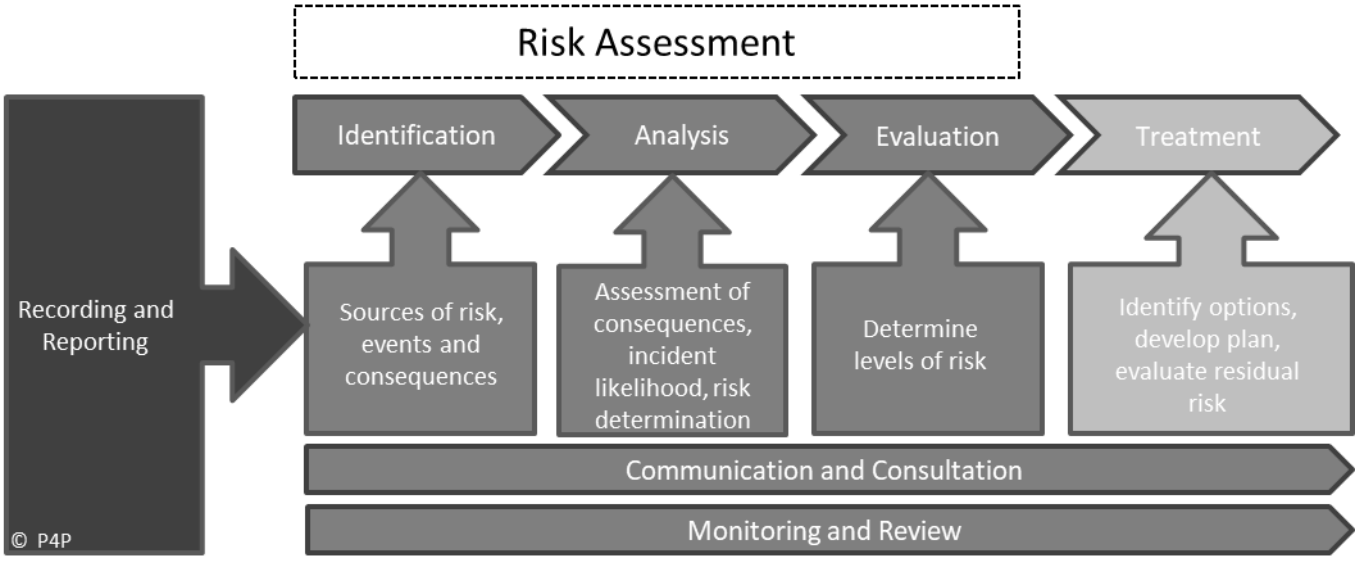
- **Evaluation** of the effectiveness of the risk management framework should be measured frequently against its purpose, implementation plans, indicators and expected behaviour
- Continual **Improvement** to enhance the suitability and effectiveness of the framework, while identifying new opportunities

Risk Management Process

The Process should be customised to align with organisations way of working and objectives

The success of risk management will depend on the process incorporating:

- **Communication and Consultation** ensures internal and external stakeholders are aware and have an understanding of risk, and an opportunity to provide feedback to support decision-making
- Establishing **Scope, Context and Criteria** of risk management activities, will help define the risk management process for effective risk assessment and appropriate treatment
- **Risk Assessment** should be performed regularly and collaboratively with internal and external stakeholder, identifying, analysing and evaluating threats and opportunities.



- **Risk Treatment** involves identifying best options, planning, implementation and measuring the effectiveness of the implemented treatment to ensure it meets with expected outcomes
- **Recording and Reporting** of risk management process outcomes are documented and communicated across the organisation, so as to improve risk management activities and improved decision making

Key Benefits of Risk Management

- Fewer surprises with the ability to identify threats and action them quickly before they become issues
- Helps increased efficiency as potential opportunities are identified contributing to continuous improvements
- Eliminate or mitigate risks, creating a safer environment for employees, visitors and members of the public

- Being prepared for unfortunate events, means consistent and enhanced operations resulting in increased profits
- Continuous improvement lowers costs while increasing quality
- Compliance with legal and regulatory requirements
- Improved mandatory and voluntary reporting

Conclusion

Risk Management is the process of identifying, assessing and controlling threats to an organisation, while identifying any opportunities for continuous improvement.

ISO 31000 is a universally recognised standard providing guidelines on risk management, replacing multiple dated standards, and methodologies that differed between industries and regions.

ISO 31000 provides a framework that supports decision making across all levels of the organisation. It should be customised involving all stakeholders internal and external, and integrated with management systems to ensure consistency and the effectiveness of management.

Principles
Designed to highlight the importance of risk within the context of the organisation, and to help you to understand why risk management is vital to business success.

Framework
Components that support and sustain risk management throughout an organisation

Process
Management of policies, procedures and best practices

Primary befit of risk management to the organisation means threats are identified quickly so they can be eliminated or mitigate creating a safer environment for employees, visitors and members of the public.

For more information on Risk Management visit our free resource library

Next Steps

Success with ISO 31000 and other standards can take many forms.
For some enterprises, it is all about attracting new clients, while others see it as the blueprint for internal efficiency.

Now that the revised versions of ISO 31000 ISO 9001, ISO 14001 and ISO45001 have been published, it's an ideal time to integrate and automate your management systems, where everyone in your organisation can access one set of policies and procedures.

Experience the power of CloudEQMS ™ Enterprise Quality and Risk and Management Solution

Helping your business avoid incidents, accidents and hefty fines

Automate manual risk assessments with "drag & drop" forms to use on or offline on any device.

- Attach photographic, video or sound recording of hazards to risk assessment forms
- Use automatic review and approval workflow processes to ensure all non-conformances and corrective action activities are carried out timely with the ability of escalations and electronic signature for sign-off.

Email enquire@p4p.uk.com for a free no obligation consultation