Risk Management Update

ISO 31000 Overview and Implications for Managers

InConsult

Contents

- ISO 31000 highlights 1
- Changes to key terms and definitions 2
- Aligning key components of the risk management framework 3
- The risk management process 4
- The principles of risk management 5
- Strategies for enhancing risk management 7
- ISO 31000 transition implications and tips for managers 8
- More information 9

IMPORTANT NOTE:

This update is not intended to replace ISO 31000. It aims to highlight some of the important changes from AS/NZS 4360 and provide some insight and valuable tips to help organisations who want to implement an effective risk management framework.

ISO 31000 highlights

Background

In November 2009, the International Organization for Standardization (ISO) finally released the very much anticipated and first international risk management standard titled ISO 31000:2009 Risk Management – Principles and Guidelines (ISO 31000) to provide organisations with principles and generic guidelines on risk management.

ISO 31000 has been developed using experts from around the world, from various industries and disciplines. The Standard aims to provide organisations with guidance and a common platform for managing different types of risks, from many sources irrespective of the organisations size, type, complexity, structure, activities or location.

In Australia, ISO 31000 has been adopted by Standards Australia and will be officially known as AS/NZS ISO 31000:2009 Risk Management - Principles and Guidelines. In this briefing, we will refer to it simply as ISO 31000.

The new Standard will replace the popular and highly respected AS/NZS 4360:2004 Risk Management standard. AS/NZS 4360 was originally developed by Australia and New Zealand in 1995 and has served risk managers from around the world well ever since. In fact, ISO 31000 is largely based on AS/NZS 4360 and one could argue that a revised 2009 version of AS/NZS 4360 would virtually look the same as ISO 31000.

Key differences

Whilst the fundamentals of the risk management process in ISO 31000 remain the same as in AS/NZS 4360, there are a number of important changes organisations must consider when adopting ISO 31000:

- ISO 31000 is a true international risk management standard and stands along side other well recognised international standards like the ISO 9000 series of Quality Management standards. The international flavour will be critical for the many global organisations wanting a consistent risk management approach…globally.
- There are changes to important terms and definitions, some new definitions are introduced and some definitions are removed.
- The relationship between the principles for managing risk, the framework for managing risk and the risk management process are better explained and illustrated in ISO 31000.
- There are eleven principles introduced in ISO 31000 that need to be considered to help make risk management effective.
- ISO 31000 now lists and describes five attributes of an enhanced risk management framework.

Implications for organisations

Organisations with a relatively mature risk management framework and already utilising AS/NZS 4360 will need to make only minor, mainly cosmetic changes. We recommend risk managers undertake a review of their current risk management framework and benchmark it against ISO 31000.

Organisations with less developed frameworks that are considering implementing a more proactive, structured risk management approach will find the standard valuable in helping shape the development of their risk management framework.

Whilst ISO 31000 has a few gaps, it marks a significant milestone towards harmonising risk management practices globally and the ISO Working Group which developed the Standard should be commended.

Changes to key terms and definitions

One of the primary objectives of ISO 31000 is to achieve a level of consistency in risk management practice without the rigid uniformity. In order to help achieve this objective, ISO 31000 has redefined some key terms, deleted some terms and introduced new terms.

Whilst many of the definitions are similar to AS/NZS 4360, the amendments to the various terms are an excellent enhancement and reflect the maturity of the new Standard.

Refined definitions

When you bring together experts from many disciplines, cultures and countries, it is not surprising that ISO 31000 has redefined some important and widely used terms.

- **Risk** is now defined as the "effect of uncertainty on objectives". The emphasis is now on the 'effect' rather than the 'chance'. Like AS/NZS 4360, the definition is neutral in terms of negative and positive consequences of uncertainties and there is still a focus on objectives.
- The definition of **risk management** has changed to "coordinated activities to direct and control an organization with regard to risk", rather than listing various components (i.e. culture, processes, structures) as AS/NZS 4360 did.

Deleted definitions

Some of the more "basic" terms contained in AS/NZS 4360 have been removed.

The terms Hazard, Loss, Frequency, Probability, Control Assessment, Risk Avoidance, Risk Reduction, Risk Retention and Risk Sharing were specifically defined in AS/NZS 4360 but they are not specifically defined in ISO 31000.

New definitions

ISO 31000 has introduced some important and more pertinent terms.

- **Risk owner** is defined as a "person or entity with the accountability and authority to manage a risk." This definition will help the risk manager reinforce to management that risk ownership must be with management and not with the risk manager.
- Risk appetite is an area that many organisations struggle with and whilst risk appetite, is not defined in ISO 31000 (it is in ISO Guide 73:2009), the Standard defines **risk attitude** as the organisation's "approach to assess and eventually pursue, retain, take or turn away from risk".
- **Risk management policy** is also defined as a "statement of the overall intentions and direction of an organization related to risk management".
- The **risk management plan** should specify the "approach, the management components and resources to be applied to the management of risk."

ISO has released ISO Guide 73:2009 Risk management - Vocabulary to provide further guidance with respect to generic terms and definitions relating to risk management to support consistency. It contains some of the definitions now deleted from ISO 31000.

Aligning key components of the risk management framework

An effective, structured, proactive and enterprise-wide risk management framework doesn't just happen, the right foundations must be established and the many components must be aligned.

The relationships between the various components of managing risks including the risk management framework is better highlighted and illustrated in ISO 31000 as shown in figure 1 below.

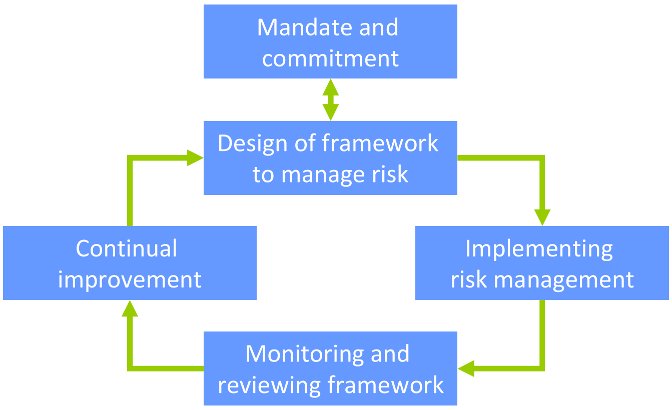
Mandate and commitment
Design of framework to manage risk
Implementing risk management
Monitoring and reviewing framework
Continual improvement

Figure 1: The relationship between various components of the risk management framework

- Mandate and commitment: Risk management is not a one-off project; it is an ongoing activity requiring ongoing commitment. It must be mandated from the Board (or equivalent), implemented by senior management and supported by all levels of management and risk owners to be sustainable.
- Design of framework for managing risk: Like all good projects, processes and strategies, risk management processes must be well designed to support effective implementation. Defining the context of risk management framework, formulating a risk management policy, embedding processes into practice, assigning resources and determining responsibility are all key elements of designing an effective framework to manage risk. Well designed periodic reporting to stakeholders and effective communication mechanisms will support effective implementation.
- Implementing risk management: Once the framework has been designed, implementation is about putting the theory into practice and actually bringing the risk management framework to life. Specifically, this is about ensuring the risk management process is understood by risk owners (through good communication and training), and risk management activities actually take place (through risk assessments, risk workshops, internal controls etc) and decisions and business processes actually factor in risk thinking.
- Monitoring and review: Involves confirmation that the various risk management elements and activities are actually working effectively in line with expectations. Any gaps identified will need to be documented and remediated.
- Continual improvement: This is about continuing to "tweak" and enhance key elements of the risk management framework to either improve current processes and/or progress towards a more mature risk management framework. A highly committed organisation will improve both its processes and mature over time.

The risk management process

The risk management process in ISO 31000 is identical to AS/NZS 4360. As illustrated in figure 2 below, it comprises of five key activities.

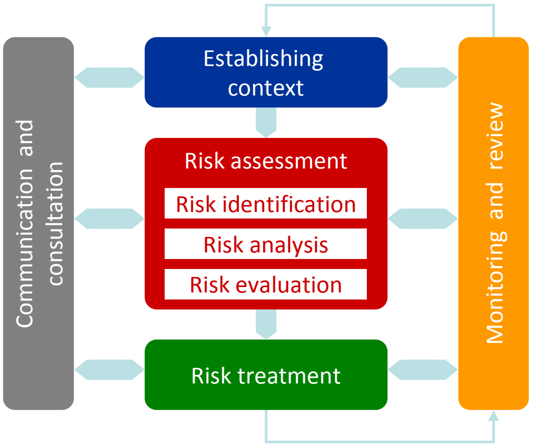

Figure 2: The risk management process

- Communication and consultation: This is concerned with engaging internal and external stakeholders throughout the risk management process. The Standard promotes a "consultative team approach". From the out set, good communication with key stakeholders will help establish expectations, shape the context of risk management and ensure their needs are considered – very important for buy in. Throughout the risk management process, various written and verbal communications between the risk manager, risk owner and stakeholders will continue to occur.
- Establishing context: Establishing context is about setting the parameters or boundaries around the organisations risk appetite and risk management activities. It requires consideration of the external factors such as social, cultural, political and economic and the alignment with internal factors such as strategy, resources and capabilities. PEST Analysis is a simple and widely-used tool that helps you understand the "big picture" of your Political, Economic, Socio-Cultural and Technological environment. The risk manager will then need to establish context of the risk management processes which includes amongst other things establishing a risk management policy, processes, methodologies, plans, risk rating criteria, training and reporting processes.
- Risk assessment: Comprises of the processes for identifying, analysing and evaluating risks. Ideally, the organisation will utilise a range of risk identification techniques including brainstorming, work breakdown analysis, and expert facilitation. ISO/IEC 31010:2009 provides further guidance on selection and application of some systematic techniques for risk assessment. Risk analysis considers possible causes, sources, likelihood and consequences to establish the inherent risk. Existing management controls should be identified and effectiveness assessed to determine the level of residual risk. After this analysis, an evaluation of the level of risk is required to makes decisions about further risk treatment.
- Risk treatment: Where the level of risk remains intolerable, risk treatment is necessary. Risk owners can treat risks by avoiding the risk, treating the risk sources, modifying likelihood, changing consequences or sharing elements of the risk. The remaining level of risk retained should be within risk appetite.
- Monitoring and review: Planned, regular monitoring of the risks and the risk management framework including processes is critical to keeping the risk management framework relevant to the changing needs of the organisation and external influences. Monitoring and review will be undertaken by risk owners, management and the board (or equivalent). An independent review of the risk management framework should be undertaken from time-to-time.

The principles of risk management

A major enhancement to ISO 31000 is the addition of eleven explicit principles to guide risk management practice.

These principles are effectively the "essential qualities" needed for risk management to be effective. Although they are not "new" per se as many organisations recognise these principles, formal recognition in the Standard is welcomed. The principles are:

- Risk management creates and protects value: One of the greatest challenges for risk managers is to demonstrate that risk management adds value. This principle recognises that risk management helps the organisation achieve its objectives. Once an organisation has set goals and established policy and processes, applying risk management thinking helps to maximise the opportunities and minimise downside risks. The introduction lists 18 benefits of managing risk that include increasing the likelihood of achieving objectives, improving stakeholder confidence, minimising losses, improving operational effectiveness and efficiency and establishing a reliable basis for decision making and planning.

- Risk management is an integral part of organisational processes: Risk management activities should not be separate from the main activities and processes of the organisation. Risk management activities should be incorporated into business processes and management controls at all levels and should be part of management's responsibilities.

- Risk management is part of decision making: Every time a manager makes a decision, there is exposure to risk. This principle recognises that good risk management helps managers make better decisions to minimise risk and optimise every opportunity.

- Risk management explicitly addresses uncertainty: Uncertainty is inherent in every business and by identifying and analysing a range of risks, risk owners are better able to implement controls and treatments to mitigate the likelihood and/or consequence of uncertainty and establish a more resilient organisation.

- Risk management is systematic, structured and timely: Like other management systems, risk management should be planned and controlled to ensure efficiency. The standard itself promotes a structured and systematic risk management process and risk management framework in order to achieve a consistent and reliable result.

- Risk management is based on the best available information: Closely linked to the principle of addressing uncertainty, this principle reads a little like a disclaimer. It recognises the fact that information is often limited, costly and imperfect. However, good risk management will consider information from many sources including observation, experience, forecasts and experts.

- Risk management is tailored: Whilst organisations in an industry have similar risks and opportunities, this principle recognises that every organisation is unique, risk management is not proscriptive, it must be appropriate to the organisation and risk management should consider the organisation's stakeholders, context and risk profile.

- Risk management takes human and cultural factors into account: This principle is closely linked to the principle that risk management is tailored whereby the organisations risk management framework should consider cultural elements and both internal and external people…particularly their skills, capabilities, perceptions and intentions. This principle is effectively about addressing the "what's in it for me?" question for stakeholders and risk owners and ensuring risk management activities are appropriate.

- Risk management is transparent and inclusive: Internal and external stakeholders can have a major impact on the organisation. This principle recognises the need to include stakeholders throughout the risk management process including when establishing context and determining risk criteria.

- Risk management is dynamic, iterative and responsive to change: In an ever-changing world, an organisation will need to respond to changes to the internal and external environment. Amending business strategy, management plans, financial plans and organisational structures are essential. Similarly, an organisation's risk management framework and processes need to respond to these changes.

- Risk management facilitates continual improvement and enhancement of the organization: This principle builds on the last principle that risk management is dynamic and iterative. It encourages organisations to be flexible and continually improve their risk management maturity framework along with other elements of their organisation to build resilience and capacity to maximise opportunities.

Strategies for enhancing risk management

Like AS/NZS 4360, ISO 31000 recognises the need to continually improve the risk management framework. However, the new Standard goes further and lists the key attributes of an enhanced risk management framework to assist organisations in measuring their own performance against.

The five attributes of enhanced risk management listed in ISO 31000 are:

- Continual improvement: Organisations should establish performance goals, performance measurements and regular reviews. As part of this performance review, a review of the risk management framework should be undertaken and refinements documented.
- Full accountability for risks: Designated risk owners should have appropriate authority and delegations to manage risk and be adequately trained and competent in the risk management process. Their responsibilities should be clearly defined and communicated via job descriptions.
- Application of risk management in all decision making: Business processes and activities (e.g. meetings) should clearly document, routine and non-routine risk management thinking.
- Continual communications: Organisations should have formal risk management reporting processes in place. This includes reporting of "significant risks" and risk treatments.
- Full integration in the organisation's governance structure: Organisations need to consider risks at both policy and practice levels. This is achieved by explicitly considering risks and the affect of uncertainty on achieving organisational objectives.

Whilst ISO 31000 cannot be used for certification purposes, it does encourage organisations to benchmark and compare their current risk management practices to the principles, attributes and processes in ISO 31000, identify areas for improvement and develop strategies for improvement.

ISO 31000 transition implications and tips for managers

Organisations that have not yet implemented a formal, proactive, structured risk management framework or are struggling to effectively implement one, will find ISO 31000 a very useful guide. Whilst it is not a comprehensive workbook, it still provides adequate step-by-step guidance.

Organisations already using AS/NZS 4360 will be in a good position to adopt the new Standard.

In particular, ISO 31000 will provide an opportunity for managers who lead risk management, internal audit, compliance and governance initiatives in their organisation to reassess their current risk management framework, introduce the new terms and principles to reinvigorate their risk management program.

The transition from AS/NZS 4360 to ISO 31000 will mean two types of enhancements for most organisations:

- Minor enhancements such as changes to terms and definitions.
- Major enhancements like those that require changes to processes, redefined responsibilities etc.

Transition tips

ISO 31000 will affect each organisation differently. As a starting point, here is our suggested "to do list" for a smooth transition to ISO 31000.

□ **Review** your existing risk management framework and compare it to the various elements in ISO 31000. Remember to keep a record of enhancements as evidence of continual improvement.

□ **Update** various risk management framework documentation:

- References to AS/NZS 4360 should be changed to AS/NZS ISO 31000.
- Amend key terms and definitions.
- Re-align documentation with other applicable risk management requirements e.g. Principle 7 for ASX listed companies, APRA's GPS 220 for general insurers.

□ **Redesign** risk management practices and responsibilities to conform with the ISO 31000 approach.

□ **Communicate** amendments and key changes to your documentation to the entire organisation.

□ **Highlight** to all staff that your organisation now follows an international risk management standard.

□ **Engage** stakeholders and particularly risk owners by providing risk management 'refresher' training. The training should:

- Highlight the key changes in ISO 31000 including, new terms, the 11 principles and the attributes of enhanced risk management.
- Highlight key changes/proposed changes to your organisation's risk management practices and framework.

□ **Apply** the refresher training. Risk owners should feel positive about risk management and so risk managers should encourage risk owners to undertake a review of their risks and update their risk register.

More information

To support implementation of ISO 31000, organisations have access to a range of resources from International Organization for Standardization, Standards Australia and SAI Global.

AS/NZS ISO 31000:2009 Risk management - Principles and guidelines

http://infostore.saiglobal.com/store/Details.aspx?ProductID=1378670

Guide 73:2009 Risk management - Vocabulary
http://infostore.saiglobal.com/store/Details.aspx?ProductID=1378617

IEC 31010:2009 Risk management - Risk assessment techniques
http://infostore.saiglobal.com/store/Details.aspx?ProductID=1382224

Risk Management Standard Briefing
http://www.shortcourses.uts.edu.au/code/coursedetails.php?&sc_code=RISKMGT

About InConsult

InConsult is a specialist risk management consulting firm providing a comprehensive range of risk management, audit, governance and business continuity management solutions including risk management training.

InConsult also designs, develops, delivers and supports GuardianERM.net an integrated enterprise risk management, audit, compliance, incident management and business continuity management system that is ready to support in the implementation of ISO 31000.

Contact:	Tony Harb
Address:	L3, 66 King St, SYDNEY NSW 2000
Tel:	+61 2 9241 1344
Email:	info@inconsult.com.au
Website:	www.inconsult.com.au www.guardianerm.com

Sources and references used

- AS/NZS ISO 31000:2009 Risk management – Principles and guidelines
- Guide 73:2009 Risk management - Vocabulary
- IEC 31010:2009 Risk management - Risk assessment techniques
- AS/NZS 4360:2004 Risk management

The information in this briefing is provided for general information purposes only and must not be relied upon as a substitute for independent professional advice. No liability will be accepted for any losses incurred by any person or organisation relying on this document.