

Impact of ISO 31000 on Existing ERM Programs

February 2010



Background

The International Organisation for Standardisation has published a new standard for risk management, **ISO 31000:2009, Risk Management – Principles and Guidelines**. Whilst this sounds like a very dry title, don't be alarmed – ISO 31000 takes a common sense approach to risk management. The importance of the standard will be seen as it helps organisations of any size and in any industry strive towards their business goals by managing risk effectively.

ISO 31000 pulls together and replaces a number of similar international standards and will also supersede national standards such as AS/NZS 4360:2004. In fact, AS/NZS 4360, which was due for revision in 2009, has formed the basis of ISO 31000.

There is no doubt AS/NZS 4360 has been an outstanding success. Developed in Australia and New Zealand, the standard has been broadly accepted locally and beyond. Ask any antipodean business how they manage risk, you can almost guarantee the answer will be the same – according to the process defined by AS/NZS 4360.

And now, at the height of AS/NZS 4360's influence, it is disappearing. This makes a review of the high-level elements of ISO 31000 timely, and forces risk managers everywhere to answer this question:

What does ISO 31000 mean for my existing ERM program?

The answer to this question probably depends on the methodology used to develop your existing ERM program. If the basis is AS/NZS 4360, there will be significant common ground. If you have used another standard such as COSO, the challenges may be greater due to the comparative lack of flexibility within COSO.

Let's examine some of the key themes in ISO 31000.

Definition of Risk

ISO 31000 provides a new definition of risk: **The effect of uncertainty on objectives**. Many individuals and organisations see risk as an inherently negative thing that should be avoided at all costs – ISO 31000 builds on the AS/NZS 4360 principle that striving towards business goals always carries an element of risk and uncertainty. It is the effective management of that risk which enables us to meet our goals.

The critical message here, particularly for the risk manager who has struggled to gain internal support and traction for risk programs, is that this is music to the Chief Executive's ears. The CEO, rightfully so, is totally focused on achieving business goals – the language of ISO 31000 supports this 100%.

What ISO 31000 may really mean for your existing ERM program is a higher profile and the necessary support from the top of the organisation that is a pre-requisite for success. Furthermore, objectives may be relevant to any level of the organisation, (e.g., business unit, team or project) and can have many

different aspects such as environmental, financial and organisational health and safety. This integration promotes engagement with the risk management process throughout the whole organisation.

ISO 31000's Key Principles

ISO 31000 contains 11 key principles that again position risk management as a fundamental process in the success of the organisation rather than a wearisome burden on the organisation's business managers. Details of these principles can be found within the standard but the following five are worthy of further discussion:

- **Principle 1** Risk management creates and protects value
- **Principle 2** Risk management is an integral part of the organisation's processes
- **Principle 3** Risk management is part of decision making
- **Principle 5** Risk management is systematic, structured and timely
- **Principle 11** Risk management facilitates continual improvement of the organisation

These principles clearly give you as a risk manager the platform to raise the profile of your current ERM program within your organisation.

The concept of creation and protection of value should resonate strongly with the organisation's Board of Directors and Chief Executive. Including risk management as an integral part of the organisation's processes and decision making implies that, as a critical discipline, line managers cannot ignore or pay lip service to risk management. Using a systematic, structured and timely approach makes risk management a continual and active process and not a once a year exercise that can be left on the shelf to gather dust.

The Risk Management Framework

The risk management framework is the management system that defines and describes how risk management will be embedded and executed at all levels of the organisation. An effective framework is critical to the success of ERM in our business.

For organisations defining their risk management framework for the first time and for organisations wanting to re-establish their framework, the new standard provides some valuable guidance which details the attributes of a successful framework.



Figure 1: ISO 31000 risk management framework approach

The framework itself should be subject to continual improvement, with the standard defining a “Design => Implement => Monitor => Improve” management model. The standard makes many good recommendations regarding the framework but the area that should stand out for the risk manager is the Monitoring of the system. It is easy to think that this relates to the monitoring of risk levels and control effectiveness across the organisation but it relates directly to **monitoring the success of the framework**.

The implication here is that it is equally important to report the number of completed risk assessments to the risk and audit committee as it is to report unacceptable risk levels. Again the emphasis shifts to risk management being an integral part of the organisation’s management process.

Risk Assessment

At the heart of any risk management process lies the actual assessment of risk – how the risk is identified, analysed, evaluated and treated. For those organisations that have based their existing ERM program on AS/NZS 4360 the good news is that this fundamental activity remains almost identical in ISO 31000.

The risk assessment process is shown in the familiar diagram below:

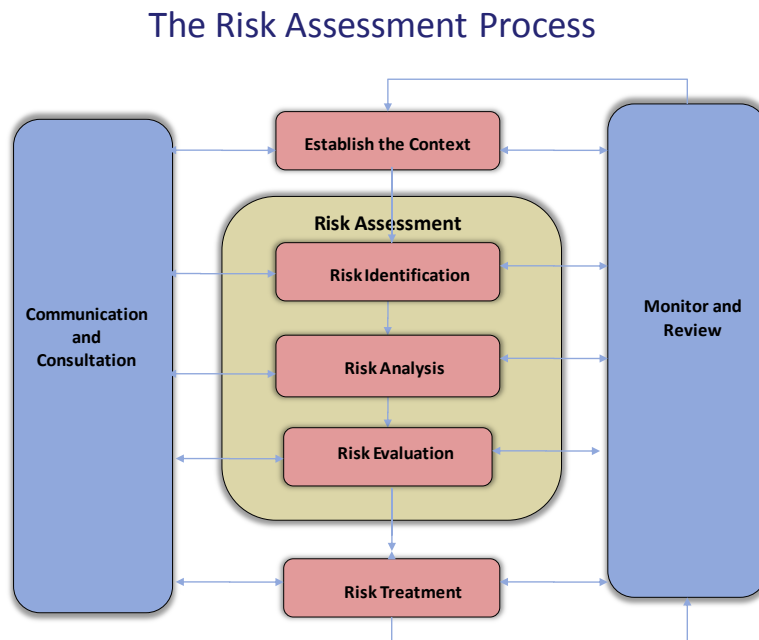


Figure 2: Standard risk assessment process flow

Summary

In summary, ISO 31000 brings good news to the risk management professional. Those organisations adopting the standard should expect to see a rising perception of the importance of risk management, more visibility of the risk management process and certainly more traction with the leadership of the organisation.

One important point to bear in mind is that ISO 31000 is a guideline standard and not a standard that requires accreditation. This gives the risk manager the flexibility to implement the risk management processes in a manner and within timescales that suit the organisation.

Jon Piercey
Vice President – Asia/Pacific
Methodware

Jon Piercey is a senior risk executive based in Sydney who runs Methodware's operations throughout Asia and the Pacific.

Methodware is a world-leading developer of governance, risk and compliance management software solutions with more than 1,800 clients in over 80 countries. Methodware solutions are used for enterprise and operational risk management, internal audit, regulatory compliance, investigation management, data privacy and vendor management. Visit methodware.com to learn more.