BROADLEAF CAPITAL INTERNATIONAL PTY LTD
ABN 24 054 021 117
PO Box 1098
Mitcham North
VIC 3132
Australia
www.Broadleaf.com.au
Tel: +61 (0) 3 9893 0011
Mobile: +61 (0) 412 121 631
Fax: +61 (0) 3 9893 0011
Purdy@Broadleaf.com.au

LexisNexis 5th Annual Risk Management Conference

HOW TO BRING YOUR ERM FRAMEWORK INTO LINE WITH ISO 31000[1]

Grant Purdy
Associate Director Broadleaf Capital International
Chair, Standards Australia and New Zealand Joint Technical Committee on Risk Management (OB7)
Nominated expert, ISO Risk Management Working Group

1 Abstract:

The new ISO Risk Management standard will guide those companies who have not previously embarked on Enterprise Risk Management (ERM). It will also provide a challenge for those who have adopted this strategy but where it is not as yet working effectively.

This paper will explain the practical steps organisations can take now to move into compliance with ISO 31000:2009[2]. These steps are to:

1. Adopt a new paradigm for risk and risk management;
2. Take stock of their current framework and processes for risk management and conduct a gap analysis to ascertain whether they possess all the necessary elements;
3. Evaluate their risk management maturity and needs so as to assess what improvements or changes are needed;
4. Then, to develop their strategies for making those changes and for sustaining effective risk management.

2 Introduction

The new ISO standard has been written with a wide range of organisations in mind. It not only provides information on the process to be adopted generally for risk management, but also contains advice on how that process should be implemented through the development and implementation of a 'framework'. Such a framework 'integrates' risk management into the organisational context and provides the mandate, resources and management system to enable effective risk management to take place, to improve and to adapt in time.

[2] Draft international standard ISO/DIS 31000, Risk management — Principles and guidelines on Implementation, ICS 03.100.01, International Organization for Standardization, 2008

3 Five Steps to Implementation

This paper suggests, quite simply, that the implementation of risk management under ISO 31000 should follow the processes described in that standard. In particular, those wishing to improve or advance risk management within their organisations should use the principles and attributes of good practice given in the standard as a means to benchmark and evaluate what they are doing now.

Furthermore, the strategies developed and adopted to improve an organisation's approach to risk management, to bring it into line with the 'performance' requirements of ISO 31000, should follow the advice given in Clause 5 of the Standard.

3.1 Step 1 – Change the Paradigm for Risk and Risk Management

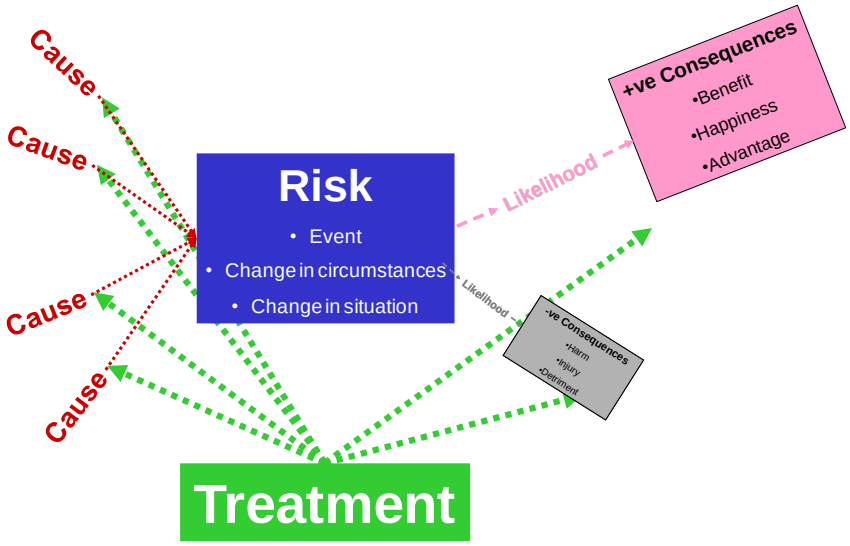
Many risk management practitioners have learnt to their cost that it is very difficult to implement effective risk management in an organisation if management, particularly at a senior level, don't have a mature understanding of risk and how it can be managed.

ISO/IEC Guide 73[3] - the guide to risk management vocabulary being issued at the same time as ISO 31000 - defines risk as:

"effect of uncertainty on objectives".

That definition is consistent with that in AS/NZS 4360:2004[4]: "the chance of something happening that will impact objectives". However, the new definition moves our thinking on and beyond 'events' and 'things that happen'. Certainly the new definition is a world away from the way many people still think of risk as 'hazards' or 'things that go wrong'. Unfortunately, in many organisations the terms 'risk' and 'hazard' are still confused and the link between objectives and risk is not properly understood and appreciated.

Figure 1: Risk Management Process System



[3] ISO/TMB WG on Risk management N 066, Date: 2008-04-01, ISO/IEC CD 2 Guide 73, ISO/TMB WG on Risk Management, International Organization for Standardization, 2008.
[4] AS/NZS 4360:2004, Risk Management, Standards Australia and Standards New Zealand, ISBN 0 7337 5904 1.

ISO 31000 is predicated upon risk being the uncertainty that lies between us and our objectives. This concept is quite simple and, of course, very relevant to managers and executives. It implies a top-down approach where risk management become a key process to enable the organisation to determine and achieve its objectives. Risk is not positive, nor negative. It's just risk.

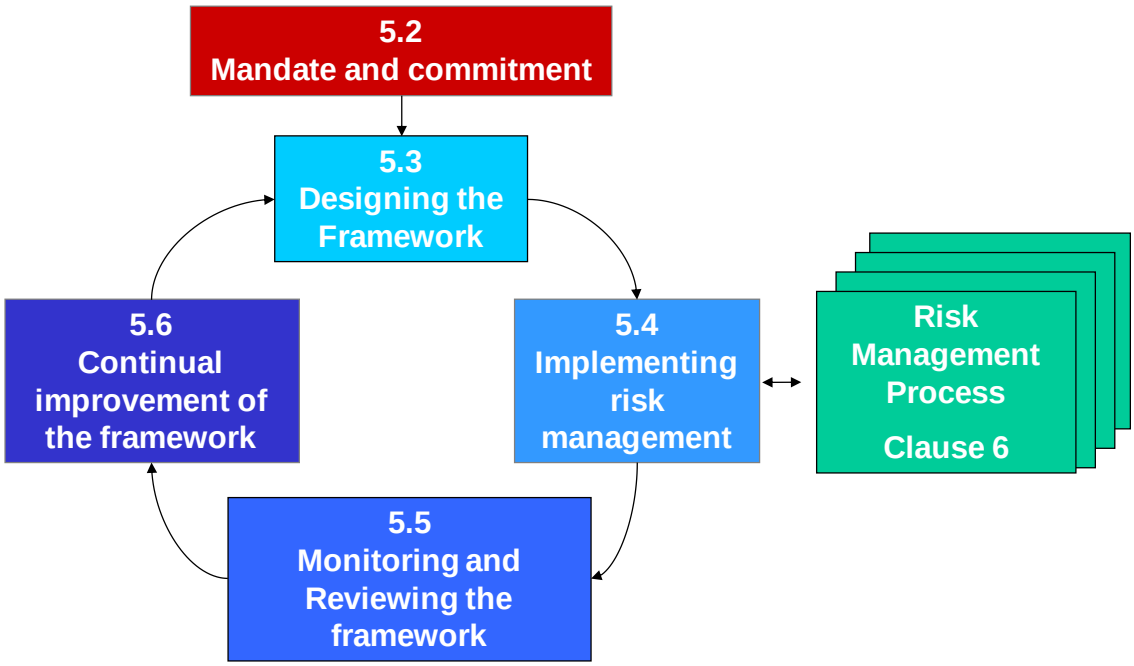
Of course consequences can be both negative and positive and the main purpose of the risk management process is to treat the causes of the risk so as to magnify the likelihood and size of the positive, beneficial consequences while acting to shrink the likelihood and size of the negative, detrimental consequence. This system is shown in Figure 1 above.

Unless management, especially senior management, appreciate this paradigm for risk and risk management, then no real progress can be made in the implementation of the Standard. Achieving this understanding must be tackled first, as part of the obtaining of a mandate.

3.2 Step 2 – Take Stock

Clause 5 of the Standard contains full advice on how a framework should be developed, implemented and kept up to date and effective. Figure 2 contains the outline of the steps given in Clause 5 which is based on the 'Deming' Quality Management Plan-Do-Check-Act model[5].

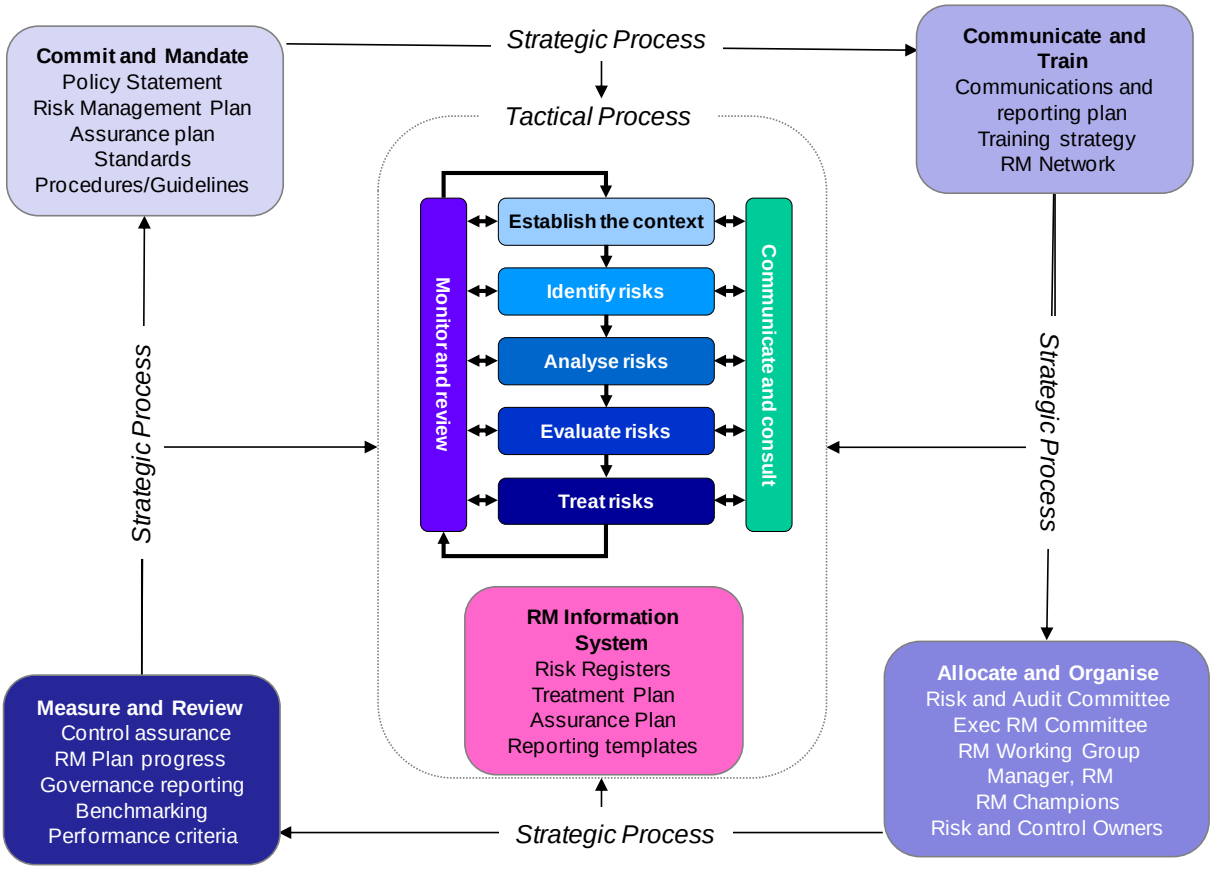
Figure 2: Steps to develop, implement and sustain a risk management framework



Of course the risk management framework must be designed to suit the organisation, its internal and external context. However the framework for all organisations, whatever their size or purpose, should still contain certain essential elements for risk management to be effective. Figure 3 contains a general scheme showing all the required elements, including those for the risk management process and risk management information system.

[5] Deming, W. Edwards (1986). Out of the Crisis. MIT Press. ISBN 0-911379-01-0.

Figure 3: Risk Framework Elements



The starting point for improving an organisation's approach to risk management should always be a gap analysis that 'takes stock' and evaluates what processes and systems are present now. If any of the essential elements are missing it is highly unlikely that risk management will become effective. Normally this evaluation is conducted using a gap analysis protocol and Figure 4 contains an extract from one.

3.3 Step 3 – Evaluate Your Maturity

Unfortunately, some organisations who have attempted to implement ERM and other forms of risk management in the past and have been ill-advised, ill-directed or have followed a deficient standard. Because of this, dysfunctional systems of risk management are often encountered that not only yield very little return for the investment that has been made, but are often viewed as a compliance overhead or an imposition, more concerned with the reporting of risks rather than with their effective treatment.

Clause 4 of ISO 31000 contains a list of practical and important 'principles' that should be the starting point for any maturity evaluation. These principles address not only "*does the process element or system exist*" but also "*is it effective and relevant for your organisation*" and "*does it add value*". In fact the first principle is that Risk Management must add value.

The annex to ISO 31000 also contains a list of attributes that seek to represent excellence in risk management, particularly ERM. These should be treated as aspirational goals, representing stretch targets for existing good risk management processes and frameworks. Figure 5 show an example extract from an evaluation against the 'principles' and 'attributes'.

Figure 4: Section of a gap analysis protocol

Element		Component	Criteria	Criticality	Present (✓)	Effectiveness (%)
2	Communicate and Train	Stakeholder analysis.	- To identify who should be consulted	Important		
		Communication plan	- To plan the ongoing consultation and information exchange - In keeping with the normal organs and culture of communication	Important		
		Training strategy	- To build skills - On risk management generally - On tools and processes - Competency based	Important		
		Network/ Community of Practice	- For Champions - To support and mentor - To distribute best practice - To engender ownership within the business	Desirable		
3	Organise and Allocate	Risk Management Committee of the Board	- Board - Charter clearly defined - More than just Financial risks - Assurance role	Essential		
		Executive Risk Management Group	- Executive level - Steering of strategy and plan - Monitoring performance - Allocation of resources	Important		
		Risk Management Working Group	- Concentrates on application - Comprises the RM Champions of the organisation - Spreads best practice.	Important		

Figure 5: Example of a maturity evaluation protocol

Attribute	Indicators	???? Response
1 An emphasis on continual improvement in risk management through the setting of organizational performance goals, measurement, review and the subsequent modification of processes, systems, resources, capability and skills.	This would be indicated by the existence of explicit performance goals against which the organization's and individual manager's performance is measured. The organization's performance could be published and communicated. Normally, there would be at least an annual review of performance and then a revision of processes systems, and the setting of revised performance objectives for the following period. This risk management performance assessment is an integral part of the overall organization's performance assessment and measurement system for departments and individuals.	- With the exception of safety lag indicators used to set KPIs we could not find any evidence of performance management being applied to risk management.
2 Comprehensive, fully defined and fully accepted accountability for risks, risk controls and risk treatment tasks. Designated individuals fully accept, are appropriately skilled and have adequate resources to check risk controls, monitor risks, improve risk controls and communicate effectively about risks and their management to internal and external stakeholders.	This would be indicated by all members of an organization being fully aware of the risks, risk controls and tasks for which they are accountable. Normally this will be recorded in job/position descriptions, database or information system. The definition of risk management roles, accountabilities and responsibilities should be part of all the organization's introduction programs. The organization ensures that those who are accountable are equipped to fulfil that role by providing them with the authority, time, resources and skills sufficient to assume their accountabilities.	- Risk owners are defined in most systems but their role is not defined. - Controls owners are not defined in the Business Risk Management system or given in risk registers. - In general, task owners are the risk owners. - Managers generally do not have defined responsibilities with respect to Business Risk Management. - Risk specialists such as the Manager Risk Systems have responsibilities that include implementation of risk management. - Current governance requirements do not place the accountability for Business Risk Management implementation on managers

3.4 Step 4 Develop Your Plan – To Start

We would recommend that the person or team who are leading the risk management activity should create a plan that shows the actions that will be taken initially to 'start up' risk management according to ISO 31000. This plan should be carefully developed as it will provide the foundations for effective risk management and will become the guide that the whole organisation follows. The plan should include:

– Conducting a gap analysis and maturity evaluation;

- Getting a sponsor and receiving a clear mandate;
- Setting a realistic timetable (years);
- Getting a budget (and some help?);
- Spending enough time getting ready and decide when you will be ready to roll (down);
- Bleeding in the processes (one a year?);
- Deciding on the 'early adopters' with credibility and start with them;
- Deciding on the 'blockers' and take them on later;
- Looking out for opportunity to 'showcase' risk management.

In particular, the plan should include the strategy to be adopted to 'engage' management at successive layers of the organisation, as the risk management framework is rolled down.

3.5 Step 5 – Develop Your Plan – To Keep it Going

Often organisations start risk management well but after the first few months the process can falter and momentum is lost. This can arise from a change in staff or leadership but often occur because senior management assume that risk management no longer needs their attention which is then diverted towards some other initiative or project.

Fundamentally such problems arise because risk management is been treated as a short term 'initiative' or a 'project' and there is no understanding that implementing ERM requires and is part of a significant culture change. Often there is an unrealistic understanding of how long it takes an organisation to change culture, to embrace and embed risk management. Some changes can happen quickly but it does require prolonged effort and management focus to make risk management become self-sustaining.

For these reasons we think it is essential for organisations also to plan for how they will maintain, sustain, improve and adapt their approaches to risk management – as their organisation and its external context changes.

Key actions to make a risk management framework self sustaining include:

1. Embedding risk management processes into key business processes. For example using risk assessment as part of the management of change, integrating strategic plan development with risk assessment and root cause analysis, building accountability and skills in line management review and assurance of controls.
2. Applying performance management processes to risk management at both a personal and organisation levels. This will involve making line management accountable for their own risk management plans, reinforcing accountability for risks and controls through performance monitoring and reporting using a risk management information system and setting up a system of periodic management 'self evaluation' and reporting with internal audit validation and corroboration. An example of this is shown in Figure 6.

Valuable momentum can also be achieved by allowing the detailed direction of risk management to lie with a 'community of practice' of risk champions who represent all parts of the organisation. This transfers ownership of the framework and its enhancement to the business as a whole and away from the Risk Management department.

There has been a lot of interest recently on reporting about risks and risk management. This has been stimulated by the ERM Framework produced by the COSO organisation in the USA[6], the Sarbanes Oxley legislation and similar requirements including our own ASX Corporate Governance Guidelines[7]. Much of this reporting has focussed on systems to escalate the notification of risks identified up the management chain in the belief that 'big risks' must be notified to senior people. However, this 'risk reporting' activity has sometimes served to distract attention away from the main purpose of risk management, to treat risk.

Somehow, some organisations have become so caught up with the reporting frenzy that risk treatment becomes a secondary consideration. Some software systems encourage this imbalance and the linking of compliance and risk management has sought to re-frame risk management into just risk reporting.

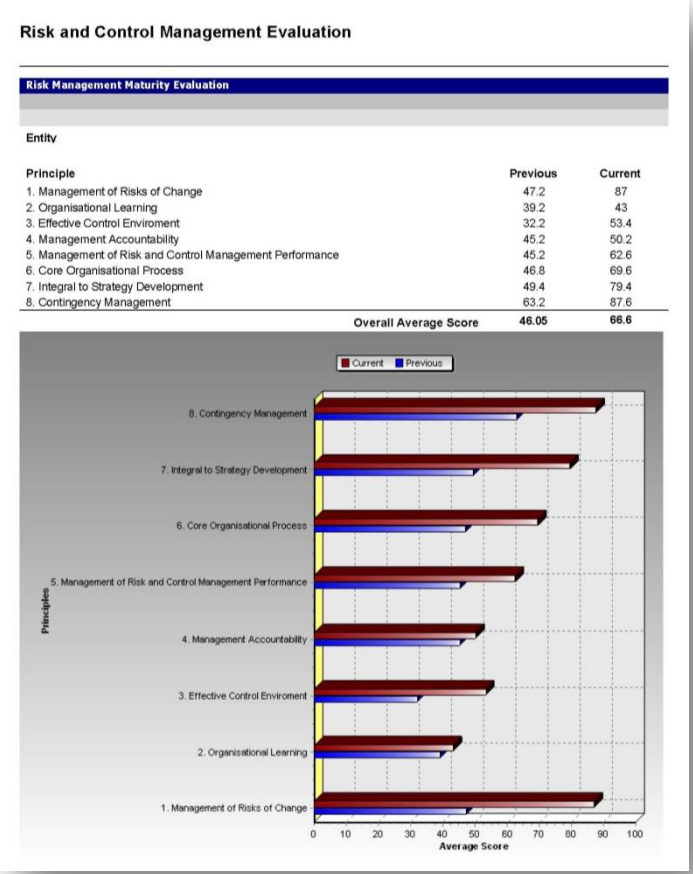


Figure 6: example Management Self-evaluation

We believe that reporting is just one part of risk management and that, in practice, it should be incidental to good risk management, not the sole purpose for it to occur. Fortunately the revised Principle 7 of the ASX Guidelines now require reporting on 'risk management' not on risks. After all, if an organisation's approach to risk management is defective, any report of the risks it faces must be treated with suspicion.

4 The Future of Risk Management

AS/NZS 4360 has been applied and adopted by many hundreds of thousands of organisations in Australia, New Zealand and across the world over the last 13 years. They have generally found it provides a very practical approach to the management of risks which can be widely applied.

On the other hand are many signs now that organisations who have attempted to implement the COSO ERM framework are dissatisfied with the progress they have made and are seeking an approach which is more relevant to the strategic management of their businesses. Several

[6] COSO: The Committee of Sponsoring Organizations of the Treadway Commission (http://www.coso.org/publications.htm

[7] Corporate Governance Principles and Recommendations, 2nd edition, ASX Corporate Governance Council, August 2007, ISBN 1 875262 42 3.

authors have pointed out that the COSO Framework possesses many technical and practical weaknesses. For example the well known commentator, Felix Kloman[8] has said:

> *"Most efforts improve the breed, although the COSO II (Committee of Sponsoring Organizations) monster in the United States set us back several years. The Australian/New Zealand effort should be the bellwether, if risk management is to continue to evolve and flourish"*

Ali Samad-Khan[9] has pointed technical weaknesses in that way COSO requires risk analysis to be conducted. He has said:

> *"COSO not only fails to help a firm assess its risks, it actually obfuscates the risk assessment process"*

And a full review last year by Michael Rasmussen of Forrester Research[10] concluded that:

> "*Many organizations look first to The Committee of Sponsoring Organizations of the Treadway Commission (COSO) enterprise risk management (ERM), only to discover that it is poorly written and difficult to implement. The Australia/New Zealand 4360:2004 Risk Management Standard (AS/NZ 4360) is more mature, straightforward, and flexible with a wealth of implementation resources for different risk scenarios."*

The Institute of Internal Auditors was one of the authors of the COSO ERM Framework. Their Australian Branch, in a letter[11] containing comments on the latest draft of ISO 31000:2009 has suggested that:

> *"While those responsible for setting the ISO standard may not agree with everything in the COSO ERM document, they need to be cognisant that a very significant number of organisations around the world have invested significant effort into developing risk management frameworks which are based on COSO and that a competing standard is likely to cause significant frustration and confusion by users.*
>
> *As such the IIA-Australia would contend that if ISO is to go ahead with this standard then a harmonisation project would be appropriate to ensure that these two documents are compatible and/or complementary. This may require an update to COSO, an update to the draft ISO 31000 or both."*

It seems almost certain now that ISO 31000 will become a global standard early next year and that it will become the paramount standard for risk management for all countries. It also seems likely that the COSO ERM standard will need to change as it currently does not comply with ISO 31000: the approach to risk management it advocates does not satisfy the principles of good risk management under clause 4 of the ISO standard. It also omits certain key elements of the risk management process (Clause 6), does not contain practical guidance on implementation (Clause 5) and does not lead to approaches to risk management that meet

[8] H. Felix Kloman, Risk Management Reports, Volume 33, Number 10, October 2006. Additionally, Risk Management Reports December 2004 provides further reflections on challenges with COSO ERM.
[9] Operational Risk, January 2005 (http://www.opriskadvisory.com/docs/Why_COSO_is_flawed_(Jan_2005).pdf
[10] AS/NZ 4360 — A Practical Choice Over COSO ERM, Michael Rasmussen, Forrester Research, January 3, 2007
[11] Private communication.

the attributes of excellence (Annex). Importantly, under COSO risk is still about events with negative consequences and is not associated with the achievement of an organisation's broad objectives and the uncertainty faced in that.

5 Conclusions

We would strongly advocate the use of ISO 31000 itself as the guide to implementing the standard. This should involve a carefully planned process starting with 'taking stock of the existing approaches using a gap analysis followed by maturity evaluation.

The development of a plan is then essential. This should not only to address the immediate steps to be taken but also deal with how effective risk management can be sustained over time.

We are also confident that ISO 31000 will quickly receive universal acceptance and will lead to the rectification of the deficiencies in some other standards like that from COSO. In time we expect to see that risk management implemented according to ISO 31000 will be seen to be adding much value to many organisations and that it will become a worthy successor to the our own, very successful standard, AS/NZS 4360:2004.

In summary, we think that ISO 31000 will treat the risk in risk management.

