RAISING THE STANDARD – THE NEW ISO RISK MANAGEMENT STANDARD

Grant Purdy
Associate Director, Broadleaf Capital International
Chair, Standards Australia and Standards New Zealand Risk Management Committee, OB7
Nominated Expert, ISO Technical Management Board Risk Management Working Group

1 The New Standard

It is 14 years since the first version of the Australian and New Zealand Risk Management Standards, AS/NZS 4360:1995, was published. It is now be replaced by a new international standard that in Australia will be called AS/NZS ISO 31000:2009 and will be published on 27th October.

AS/NZS 4360:2004 has been adopted throughout the world. Its widespread acceptance and the respect it has earned over the years are the main reasons that it was used as the first draft of the new ISO standard.

The definition of risk in the new Standard is:

the effect of uncertainty on objectives.

The change in definition shifts the emphasis from, in AS/NZS 4360, 'the event' (something happens) to 'the effect' and, in particular, the effect on objectives. By way of illustration, risk isn't the chance of the share market crashing but the chance that a crash will disrupt or affect you or your organisation's objectives by, for example, limiting capital for expansion.

Both the old and new definitions clearly place risk in the context of what an organisation wishes to achieve: its objectives. Risk arises because those objectives are pursued against an uncertain background. An organisation may set its objectives, but to achieve them it often has to contend with internal and external factors and influences it may not control and which generate uncertainty and thus risk. These factors might assist or speed up the achievement of objectives; they might also prevent or delay the organisation achieving its objectives.

Risk has, in the past, been regarded solely as a negative concept that organisations should try to avoid or transfer to others. However it is now recognised that risk is simply a fact of life that cannot be avoided or denied. If we understand risk and how it is caused and influenced, we can change it (we call this risk treatment) so that we are more likely to achieve our objectives and might even perform faster, more efficiently or with improved results.

Risk is implicit in all decisions we make: how we make those decisions will affect how successful we are in achieving our objectives. Decision making is, in turn, an integral part of day to day existence and nowhere more prominent in an organisation than at times of change and when responding to external developments. This is why risk management is so closely linked to the management of change and to decision-making.

2 Characterising Risk

We characterise and describe risk in terms of both the consequences of what could happen and the likelihood of those consequences. In the past some standards only described risks as sudden or 'acute' events. However, we now appreciate that risk can also arise because of

slowly changing or 'chronic' situations and circumstances, not just because of a sudden event. Climate change is an example of a changing situation that poses a great risk to organisations, and indeed to the planet, yet it is not described by a single event.

There are challenges in characterising both consequences and likelihoods. One simple way of describing potential consequences is to say what could happen and what could it lead to. The consequences we use to describe risk may involve loss, harm and detrimental effects but often they involve benefit and advantage as well. In many cases, whether we describe consequences in a negative or positive frame depends on our point of view. For example, often our loss will be someone else's gain.

Importantly and fundamentally, risk is characterised and 'measured' by considering consequences and the likelihoods *of those consequences*, not the abstract likelihoods of events that might be detached from your organisation's objectives. Consequences and their likelihoods are often combined to define a level of risk. Some standards still suggest that a level of risk can be estimated by considering the probability of an event and the consequences that will flow from it – this is generally unhelpful and most often produces unrealistic estimates of the level of risk, sometimes called 'phantom risks' because the predicted likelihood is overstated.

3 Differences Between AS/NZS 4360:2004 and ISO 310000:2009

From the beginning of the process to develop the new standard, it was obvious that a great deal of respect exists for AS/NZS 4360 throughout the world. Although other countries wanted the new standard to reflect what they believed to represent best practice in risk management, no one wanted to deviate significantly from the systematic and straightforward risk management process we had developed in Australia and New Zealand. That is why, when you read the new standard, you will find that the well known risk management process remains largely intact. Similarly, many of the definitions are the same or similar to those in AS/NZS 4360:2004.

After some heated debate, even the diagram representing the risk management process remains the same.

The major differences between the old and the new standards are:

- Making explicit the principles of effective management. These were only really implicit in AS/NZS 4360:2004;
- Giving some aspirational goals for Enterprise Risk Management in terms of a set of attributes in an Annex;
- Providing a lot more guidance on how risk management should sit within an organisational framework to be effective – and how that framework can be created, maintained and improved.

4 The Principles of Effective Risk Management

The principles of effective risk management consist of eleven statements that are explained in terms of performance criteria.

1. **Risk management creates and protects value.** It contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.

2. **Risk management is an integral part of all organizational processes**. It is not a stand-alone activity that is separate from the main activities of the organization. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes.
3. **Risk management is part of decision making.** It helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action.
4. **Risk management explicitly addresses uncertainty**, the nature of that uncertainty, and how it can be handled.
5. **Risk management is systematic, structured and timely,** so as to contribute to efficiency and to consistent, comparable and reliable results.
6. **Risk management is based on the best available information.** The inputs are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.
7. **Risk management is tailored,** by aligning it with the organization's external and internal context and risk profile.
8. **Risk management takes human and cultural factors into account,** by recognizing the capabilities, perceptions and intentions of external and internal people who can enhance or hinder achievement of the organization's objectives.
9. **Risk management is transparent and inclusive.** Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organization, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.
10. **Risk management is dynamic, iterative and responsive to change,** so that as external and internal events occur, context and knowledge change, monitoring and review take place, new risks emerge, some change, and others disappear. Therefore, risk management continually senses and responds to change.
11. **Risk management facilitates continual improvement of the organization,** so that organizations can develop and implement strategies to improve their risk management maturity alongside all other aspects of their organization.

5 Putting it into Practice – the Framework

Some organisations have adopted the narrow view that risk management is primarily concerned with the production of reports for senior management and the Board, so that risk assessment only needs to take place once or twice a year to provide an update on previous reports. Unfortunately this limited approach has been supported by legislation and governance codes in some countries. As we have seen over the last 18 months, this approach often fails to deliver the potential benefits of sound risk management and can leave its proponents severely exposed to uncontrolled uncertainty.

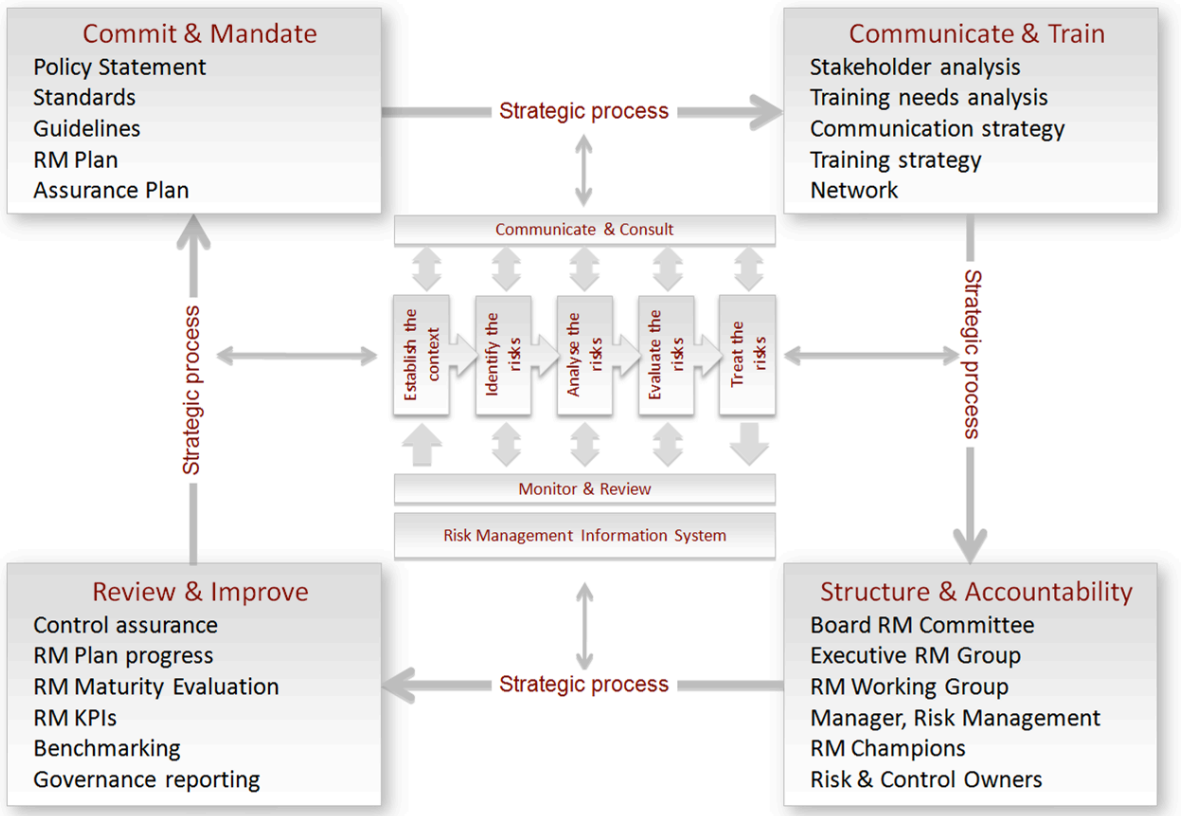
As risk is very much concerned with the strategic objectives of an organisation, risk management should be closely linked to the creation of strategic, business and project plans and the setting of organisational or project objectives. The normal yearly cycle of these strategic and business planning processes provides an annual ‘anchor’ for the risk management process. However, decisions are made throughout the year: these may lead to changes in the structure of the organisation, its processes, systems and projects, with implications for the organisation and its objectives. Risk assessment needs to take place whenever such decisions are made, as part of the management of the associated changes.

From time to time, organisations make profound and important strategic decisions that can have a significant impact on future success or failure. These often involve major investments of capital for expansion through organic growth, mergers or acquisitions, or major divestment decisions. Clearly, the significance of the decisions requires a full appreciation of the risks surrounding them and how the risks might best be treated to ensure successful outcomes.

Risk management should be a continuous process that supports internal changes and decisions and allows the organisation to respond well to external changes. For this to take place effectively the new standard requires that organisations must embed or integrate risk management with their normal business processes. The way risk management is set within the organisational context is normally called a 'risk management framework' – the policies, arrangements and organisational structures to implement, sustain and improve the risk management process. The new standard gives some considerable guidance on how such a framework can be created, stimulated and promoted and improved.

Figure 1 shows a typical framework and its components.

Figure 1: A risk management framework



Each organisation needs to design its risk management framework to suit its business processes, structure, risk profile and risk appetite. The example in Figure 1 is only a generic description – once the organisation has defined its framework it should plan how the framework will be implemented. This is the purpose of the risk management plan.

Introducing sound risk management processes usually requires changes to the organisation's culture and processes. A risk management framework cannot be introduced overnight, so the risk management plan may extend over a considerable time period.

Large or complex organisations may require a hierarchy of risk management plans. It is essential to have a risk management plan for the whole organisation that describes the broad

strategies to be pursued. However, accountability for risk management within an organisation can be encouraged by requiring departments or divisions to develop their own risk management plans, showing how they will integrate and embed risk management processes into their own processes and practices. Requiring divisions and departments to report on progress with their own risk management plans is also a useful form of governance reporting.

6 Going Forward

Even though we have succeeded in convinced the rest of the world to adopt our approach to risk management, the work of the Standard Australia and Standards New Zealand Joint Technical Committee (OB7) continues. In addition to updating all the existing handbooks to align them to AS/NZS ISO 31000, OB7 is working on a number of new or substantially re-written handbooks. These include the following handbooks that will be published over the next 12 months:

- Managing Risks in Not for Profit Organisations;
- Risk Communication;
- Risk Financing;
- Managing Risks in Sports and Recreation;
- Managing Safety Risks;
- Managing Environmental Risks;
- Risk Criteria.

OB7 has just produced a new business continuity management standard, called AS/NZS 5050. That is currently in draft and subject to public consultation. It is based on ISO 31000 and is three-part, management system standard.

Also early next year we will adopt the joint ISO/IEC standard 31010 on risk assessment methodology. This explains how the correct risk identification, risk analysis and risk evaluation tools can be selected and applied and is a supporting standard for ISO 31000.

While we in Australia and New Zealand may feel some pride that the rest of the world has decided to base its standard on the way we have managed risk here for 15 years, we should not be complacent. The new standard does contain requirements that are greater and more exacting than AS/NZS 4360:2004. All Australian and New Zealand organisations would benefit from conducting a gap analysis against the new standard and in developing or revising their risk management plans.

It is clear that the new ISO standard is a worthy successor to AS/NZS 4360:2004. It has already gained a considerable measure of acceptance, world-wide, as a practical, straightforward guide that can be adopted by all kinds of organisations.