Broadleaf

Resource material /

# A simple guide to risk and its management

June 2012, published under Managing risk in organisations

## Introduction

The publication of ISO 31000, the international standard for risk management, provided an opportunity to clarify what we mean by risk and how it should be managed. The standard supports a simple way of thinking about risk that helps remove the inconsistency and ambiguity that has existed between the many different approaches and definitions in the past.

## The definition of risk

Mankind has actively managed risk throughout its existence. However, it is only in the last few hundred years that we have been conscious that we could influence the future by learning lessons from the past. In the last century this knowledge has been turned into a science associated with decision-making.

During the last two decades, many standards and pieces of legislation have attempted to define risk. In most cases, definitions have been in terms of harm and harmful events. Nearly 20 years ago, a joint committee of Standards Australia and Standards New Zealand developed a standard for risk management that defined risk not only in terms of something that might happen, but also in terms of its impact on an organisation's objectives. It did not confine itself to just harmful events – risk and its consequences could be positive or negative. In its third edition, published in 2004, AS/NZS 4360 defines risk as:

> *the chance of something happening that will have an impact on objectives.*

AS/NZS 4360:2004 and its two predecessors were adopted in many countries. Its widespread acceptance led to the development of the first global risk management standard, ISO 31000:2009, Risk management – Principles and guidelines. This was published in 2009, together with a revised set of definitions that are contained in ISO/IEC Guide 73:2009, Risk management –Vocabulary.

The definition of risk in ISO 31000 and Guide 73 is:

> *the effect of uncertainty on objectives.*

The change in definition shifts the emphasis from '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.

In the past, risk has 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 modify it (we call this risk treatment) so that we are more likely to achieve our objectives, and we might even do this more quickly, 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 and should be an integral part of the management of change and decision-making.

## 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 '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 likelihood 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.

## The process for managing risk

AS/NZS 4360 first defined the systematic process we now use for managing all forms of risk. ISO 31000 has adopted the same process, shown in Figure 1.

## Figure 1: The process for managing risk


The risk management process

### Establishing the context

The risk management process must start by defining what we want to achieve and attempting to understand the external and internal factors that may influence our success in achieving our objectives. This step, called 'establishing the context', is an essential precursor to risk identification. An important part of establishing the context is identifying our stakeholders and understanding their objectives, so that we can appreciate how to involve them and take their objectives into account in setting risk criteria. Stakeholder analysis is often seen as part of the 'communicate and consult' step, an activity that continues throughout the risk management process.

## Risk assessment

The next three elements of the process, risk identification, risk analysis and risk evaluation, comprise what is commonly called risk assessment.

### Risk identification

Risk identification involves the application of a systematic process to understand a range of examples of what could happen, how, when and why. Understanding these example 'scenarios' is vital to inform risk treatment.

Failure to employ a systematic process for risk identification can lead to organisations missing some risks and only concentrating their attention on the 'known known' risks, and hence miss those that are 'known unknowns' or 'unknown unknowns' that may then never be treated adequately.

Risk identification should also identify the existing controls that aim to modify the consequences or their likelihood.

### Risk analysis

Risk analysis is concerned with developing an understanding of each risk, its consequences and the likelihood of those consequences. This involves much more than the simple application of a matrix, which is as far as some organisations go in rating risks. For example, understanding the effectiveness of existing controls and any control gaps is a vital part of risk analysis and must be explored before making decisions about risk treatment. We normally determine the level of risk as it is at present, taking into account existing controls and their level of effectiveness.

### Risk evaluation

Risk evaluation involves making a decision about the level or priority of each risk through the application of the criteria developed when the context was established. Risks are prioritised for attention, and cost benefit analysis is used to determine whether risk treatment is worthwhile.

## Risk treatment

Risk treatment is the process by which we improve existing controls or develop and implement new controls. If the risk management process is followed, the systematic way in which the risks have been identified and analysed means that risk treatment can proceed with confidence.

Controls are the means by which we seek to modify risks. They can be thought of as 'enablers' for our objectives. Risk treatment normally involves activities that aim to change either the likelihood of the consequences or the type, magnitude or timing of those consequences. Risk treatment might involve increasing the exposure of the organisation to the risks it prefers and from which it can benefit, as well as limiting exposure to those it dislikes (see risk appetite and risk tolerance below).

The traditional view of risk treatment involved the transfer of risk or its retention. Risk transfer is now more generally known as risk sharing, in recognition of the fact that a risk cannot be completely transferred without other risks being incurred. For example, purchasing insurance is often cited as a form of risk transfer. However, this involves the insured accepting some of the risk (the deductable) as well as tolerating the risk associated with restrictive wordings and a general reluctance of the insurer to pay claims. Insured parties also take on the risk that the insurer may fail (as has happened in the past few decades) and their premium will be lost and claims will not be paid. Similar considerations apply to risk sharing through other forms of contract.

Options for risk treatment should always be considered. Through the application of cost benefit analysis, decisions can be made about the most appropriate ones for the organisation to pursue. These should then be translated into specific actions or tasks that form a risk treatment plan, and assigned to 'task owners'.

## Monitoring and review

New risks emerge and existing risks change as an organisation's internal and external environment changes. Sometimes these changes arise because of what we do in risk treatment. Often, we find that risks have changed because controls we may have relied upon for many years have become inadequate or ineffective. Unless an organisation monitors how its internal and external context changes and reviews whether its controls remain effective, then its appreciation of the risks it faces and the levels of those risks may be incorrect.

One of the most effective ways to monitor risks is through environmental scanning by individuals charged with ensuring the assessment and treatment of each risk is up to date and appropriate. Such individuals are called 'risk owners'. Similarly, 'control owners' are accountable for ensuring that the most important, key controls remain

effective. Control owners do this through continuous monitoring, backed-up by planned programs of assurance based on approaches such as control self-assessment.

Another very effective means to monitor and review risks and controls is for the organisation to seek to learn from successes and failures, and to do so actively. Normally, this is addressed using root cause analysis to ensure that causes of events are identified systematically. It is critical that this leads to lessons being learned and actions being taken that enable the recurrence of successes and the prevention of failures.

## Risk appetite and risk tolerance

Risk appetite and risk tolerance are often confused. Many organisations struggle to define their risk appetite and to apply it within the risk management process. Risk appetite is defined by ISO/IEC Guide 73:2009 as:

> *the amount and type of risk that an organisation is prepared to pursue, retain or take.*

It can be seen that risk appetite is concerned with both the kinds of risks the organisation prefers as well as the level at which it wants to expose itself. Indeed, for many organisations, the risks they face day-by-day are the source of their income and the foundation of their business model.

While the concept of risk appetite seems simple, in practice it is very difficult to determine and efforts to define it rarely contribute meaningful value to an organisation. This often occurs because those who are required to define the risk appetite do not have a full understanding of what risk is or how it influences the achievement of their organisation's objectives. In addition, and compounding this lack of understanding, risk appetite changes with time and often reflects the personal experience and perceptions of individual directors and managers.

Making an outright and explicit description of risk appetite is problematic and the search for a simple definitive statement is often unhelpful. For this reason we normally represent an organisation's risk appetite using risk criteria that are developed on a case by case basis as part of the 'establishing the context' step of the risk management process. The criteria reflect the organisation's objectives and the outcomes in each case. They are therefore unique to an organisation and should not be copied from others.

Risk tolerance is not the same as risk appetite but the concepts are linked through the risk evaluation step. Risk tolerance is defined as:

*an organisation's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives.*

While risk appetite is implicit in the criteria that are applied during risk evaluation, risk tolerance is concerned with an organisation's willingness to tolerate or retain risk after risk treatment has taken place. This implies the application of some form of cost benefit analysis as part of risk evaluation and as the means of differentiating between and selecting options for risk treatment.

In practice, while we may use 'risk appetite' colloquially to describe the amount and types of risks we prefer (or not), it is better to not to attempt to define it explicitly. Similarly, 'risk tolerance' is best left to the decision-making processes within risk evaluation. The simplest approach, in keeping with the ISO 31000 risk management process, is to ensure that appropriate risk criteria are defined during 'establishing the context' and then applied during risk evaluation.

## Putting it into practice

### Supporting decisions

While the previous discussion on the risk management process can be thought of as concerning what risk management involves, organisations also need to consider and plan how risk management will actually take place, when required, to support decision-making.

Some organisations have adopted the narrow view that risk management is primarily concerned with the production of reports for senior managers 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. This will fail to deliver the full benefits of sound risk management and it can leave its proponents severely exposed to uncontrolled and unexpected uncertainty.

As risk is very much concerned with the objectives of an organisation, the process for the management of risk should be closely integrated into the creation of strategic, business and project plans and the setting and re-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 that are made throughout the year, not just as part of an annual planning cycle, can 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.

Organisations are also affected by changes that take place continually in the external environment. Government policies shift, laws are enacted and enforced, competitors and markets change, communities' and external stakeholders' views evolve. Not all these changes may be material to the organisation's objectives, but many will – and the organisation should appreciate their ramifications, act to reduce their negative impacts on objectives and exploit them where possible. Regular environmental scanning, attention to risk and the undertaking of risk assessment are therefore required to ensure the organisation keeps pace with external changes and responds as well as it can.

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 framework and plan

An organisation's ability to manage risk effectively depends on its intentions and its capacity to achieve those intentions. This intent and capacity is referred to as its risk management framework, which is part of its system of governance and management.

The quality of the framework is important because effective risk management requires:

- Clear expectations from 'the top'
- Appropriate capability (skills, resources, support)
- Sound relationships with stakeholders
- Integration of necessary risk management practices into the day-to-day activities and accountabilities of the management team
- A commitment to continually learn and improve.

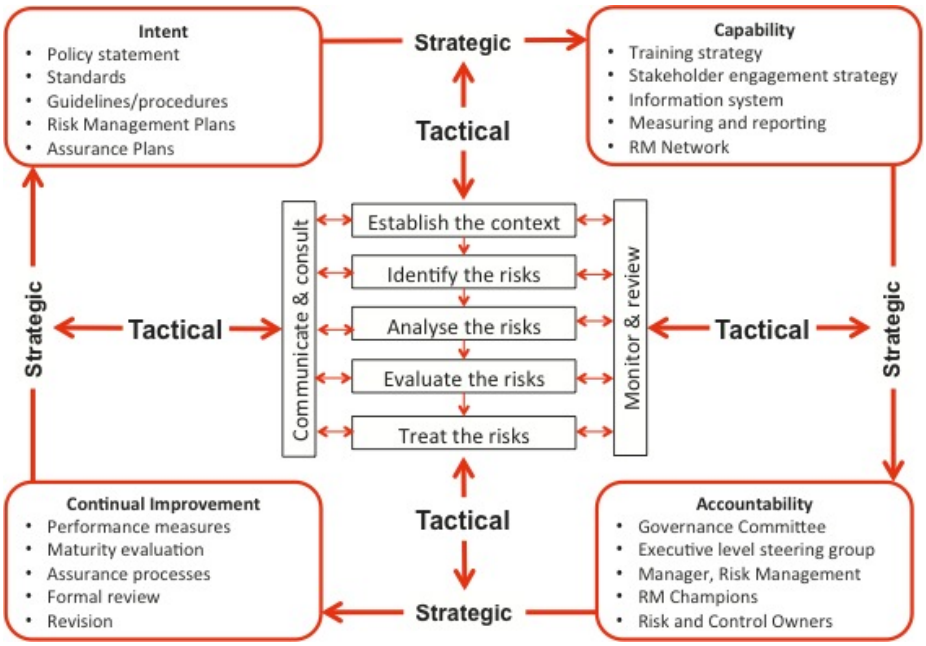
The risk management framework should not attempt to replace the natural capability of people to manage risk; rather it should enhance good practices so that the process is reliable, comprehensive and consistent. For this to occur and for the required capability to be achieved, the organisation requires:

1. A set of suitable 'tools'
2. A coherent approach to training and communicating to people so they can use those tools in a competent and consistent manner

3. An approach that signals and reinforces the correct behaviour and way of thinking.

Figure 2 shows the structure of a framework and its components.

## Figure 2: The architecture of a risk management framework




The framework for risk management

Each organisation needs to enhance and optimise its risk management framework to suit its business processes, structure, risk profile and risk appetite. The example in Figure 2 is only a generic description – once the organisation has defined its framework it should plan how the framework will be implemented or enhanced. This is the purpose of the risk management plan.

### Top-down process

Although ISO 31000 explains how to manage risk effectively, it does not explain how to make the changes that are needed to ensure the organisation's approach to managing risk improves, becomes all-encompassing and fully integrated. Even though organisations are different and their starting points may differ widely, a generic and systematic process is applicable in all cases.

Our experience is that only approaches that are 'top down' and driven by top management are successful. These signal the clear mandate for change and help ensure the necessary resources are available to make the transition as efficient and effective as possible.

This transition can take place across all of an organisation or in one or more of its parts, such as within a subsidiary business. However, even if the implementation takes place in part of the organisation, the approach should still be top down.

### Application to projects

The framework described here can also be adapted and applied to projects. Projects often require a different timescale and specialised criteria, but project risk management must be set within the organisational risk management of the owners to ensure that projects deliver the value for which they are being undertaken.

## Broadleaf's services

Broadleaf is working with many large organisations to develop and enhance risk management frameworks that are compatible with ISO 31000. We help organisations to achieve and sustain tailored approaches to risk management that suit them and that adapt as the organisation and its strategic objectives change.

We are particularly conversant with current risk management thinking as three of our team were members of the committee that wrote AS/NZS 4360 and one was a nominated expert to the ISO Working Group that wrote ISO 31000:2009 and ISO/IEC Guide 73:2009 and the implementation guide, HB 436:2013.

Our practical experience base is unique and our many service offerings include:

- Risk management planning
- Gap and effectiveness evaluation against ISO 31000
- Risk management framework development and enhancement
- Drafting of risk management policies, standards and guidelines
- Risk management information system specification, procurement and deployment
- Risk assessment facilitation
- Development and delivery of tailored risk management training

- Training and mentoring of risk management specialists in all aspects of risk management and its implementation
- Risk-based audit and assurance planning
- Risk management performance management
- Governance reporting and assurance
- Risk management framework benchmarking and review
- Extending the standard approach into quantitative analysis of uncertainty in budgets, cash flows, schedules and other measures of organisational and project performance.

Resource material /

A simple guide to risk and its management (http://broadleaf.com.au/resource-material/a-simple-guide-to-risk-and-its-management/)

**Broadleaf Capital International**
ABN 24 054 021 117
PO Box 607
Cammeray NSW 2062 Australia
Contact@Broadleaf.com.au
+61 2 9488 8477
+61 419 433 184

**Creating value from uncertainty**
Specialists in managing strategic, enterprise and project risk
Visit out website at www.Broadleaf.com.au