Hearing over the cacophony

Grant Purdy

Associate Director, Broadleaf Capital International

Grant has worked in risk management for over 38 years, in over 25 countries, as a government inspector, business manager, consultant and a manager of risk management. Currently an Associate Director of Broadleaf, he was previously Group Manager of Risk Management at BHP Billiton, the world's largest resource sector company.

Grant was a member of the Standards Australia and Standards New Zealand Joint Technical Committee on Risk Management for 14 years and its chair for seven. He co-authored the 2004 version of AS/NZS 4360 and has also helped write many other risk management handbooks and guides. He was the nominated expert for Australia on the Working Group that prepared ISO 31000 and Guide 73 and Head of Delegation for Australia on ISO TC 262.
purdy@broadleaf.com.au

Cacophonists are doing their darnedest to create the impression that they are building a new (management) art, far nobler than the (management) of the past, into which so puerile a thing as (clarity and simplicity) cannot be allowed to enter[1]

This article is based on the keynote speech given at the Risk NZ Conference in October. It challenges the value of the ever-expanding multitude of artefacts, encumbrances, concocted expressions and three letter acronyms that obscure the core concepts for managing risk and *clog up* current risk management practice.

The article demonstrates that the central concepts of successful risk management can be explained without resorting to such devices, deals with half a dozen *myths* and draws conclusions on the virtues of keeping an organisation's general approach to managing risk as simple (but not simplistic) as possible and recommends how RiskNZ should support that aim.

1 Central concepts

So often, papers and articles about risk management fail to explain specifically and in plain language exactly what is being managed – in other words the meaning of risk on which the paper or article is based is not explained. This not only means that their central thesis is fuzzy but typically, results in a lack of rigour in the thinking that follows.

Similarly, there is a failure to specifically articulate what *management* means, what are the parameters of good risk management and what empirical process of management is being assumed.

Risk

One well-accepted definition is that risk is the effect of uncertainty on what we want to achieve, our objectives. There is an inexorable logic to this definition because it is just labelling reality. Organisations pursue their objectives by taking and implementing decisions but they must do so in external and internal environments in which there is uncertainty. Whether this is called risk or has some other label doesn't change the reality.

On this basis, it makes sense that the purpose of managing risk is to improve decision-making so as to make it more likely that the subsequent actions will contribute as much as possible to the achievement of the organisation's ultimate purpose – the realisation of its objectives. It has no other purpose.

[1] Adapted from "The Noble Contempt for Melody, Henry T Finck, Philadelphia, 1914.

And it further makes sense that to achieve this purpose, risks associated with the proposed decision must be first detected and the nature and magnitude of the risk understood. Then, as necessary, the decision can be varied to ensure that the risk is acceptable - according to criteria selected by the organisation.

This is exactly the process that we all intuitively follow as we make our decision to cross the road – we understand the risk, decide if it is OK and either cross now or delay until the risk is more acceptable.

Risk is ultimately an abstract concept and so as part of an organisation's capability the nature of risk must be understood – particularly because it is a word with many colloquial and intuitive meanings.

Risk is neither inherently good nor inherently bad (in other words it is a neutral concept). However, if it is only viewed as bad, then this can lead organisations to not expose themselves to the risk that is necessary for their objectives. Similarly, unless risk is always seen as being inseparably associated with objectives there will be confusion as to what is or is not risky. For example, there is a marked difference between how an approaching cyclone is viewed by a homeowner in its path and a company that repairs storm damage.

Process for managing risk

So to be successful, the process for managing risk must enable risk to be detected and understood and then modified as necessary in the most efficient way possible. Logically, this means it must take into account the views and knowledge of interested people, consider options and be able to detect and respond to change because the real world is not static.

Describing risk

Somewhat confusingly, we use the plural form of the word, risk – i.e. risks - to characterise risk. Risks are statements that describe what could happen or be present and what that could lead to, expressed in terms of our objectives. Risks are just illustrations of risk.

The magnitude of risk

Intuitively, some risks are more important for our objectives than others and in order to understand the significance of any particular risk, we need to express its magnitude. Clearly the expression of magnitude must include both the magnitude of the consequence as well as the likelihood of that magnitude of consequence being experienced. In other words, to establish the level of risk – either quantitatively or qualitatively - the two considerations must be combined.

Modifying risk

Once understood, risk can be modified so that the magnitude is acceptable. We call the things that modify risk *controls*. These are best thought of as enablers because they provide greater certainty we will achieve our objectives.

Why be more systematic?

We try to be more systematic and structured in the way we consider and tackle risk to counter some of the normal tendencies humans display when faced with a decision that will affect their future. Being more systematic allows us to:

- Challenge our assumptions and preconceptions before decisions are made, particularly whether the actions we decide to take will lead to success and will contribute to the achievement of our overall goals
- Take appropriate actions to lower uncertainty that outcomes will be successful and that overall objectives will be achieved
- See early warning signs that the most important controls we rely on for success and to achieve our objectives are not in place or are not fully effective, so that we can take early and pre-emptive action
- Learn systematically from successes and failures in such a way we can understand how to create or improve controls.

2 Decision support

Risk management is therefore, quite simply, a form of decision support – something that humans practice instinctively whenever they have to decide how to act and respond. The thoughts that go through our heads (to some extent) when we are faced with making decisions (implicit or explicit) are:

1. What am I trying to achieve and why?
2. How might I go about it?
3. Do I need to involve others?
4. What might help me or impede me?
5. What lessons from the past are relevant?
6. What I need to do to make sure I am successful?
7. How do I know if I will be successful?

Not surprisingly these are, in fact, the seven steps in the ISO 31000 risk management process which emulates how we naturally manage risk every time we are faced with a decision: we are inevitably mindful of the related uncertainties and whether we realize it or not, we judge the importance and effect of the uncertainties in relation to our overall objectives - which also frame how we might deal with it.

Following a sound risk management process just ensures this normal, intuitive approach to decision making is more complete and effective and ensures the involvement of interested parties.

As discovering, understanding and responding to risk is already a natural, integrated part of how we think and act, it follows that it is unhelpful to do anything that de-integrates that from decision making or which makes it unnatural. For this reason, using phrases such as “implement risk management” are not helpful because it implies that it is not already happening and is somehow optional. We should always ensure the primary focus is on the decision-making and acting processes within the organisation because that is how we achieve objectives: the most efficient way to enhance the way we manage risk must be *in situ* not *in vitro*.

Risk management is, quite naturally, a dynamic process that is triggered by the need to make a decision or review a previous decision because something of significance might have changed. It is not a static activity that is meant to occur because of a calendar or some committee meeting cycle.

Unless the process is seen to and used to support decisions, little real value is created. Worse still, these other uses (particularly if framed as *compliance*) distract from, dilute and confuse the natural risk management process.

Unfortunately, in too many organisations, the only rationale given for applying the risk management process is to produce retrospective information which is duly recorded in registers and databases and solemnly reported - but is not actually used by anyone to make decisions.

3 Artefacts, Confections, Encumbrances and Three Letter Acronyms

Unfortunately, the risk management profession seems determined to make the simple and useful concepts and processes described above much more complex and opaque. It seems that almost every month we hear of a new adjective-noun combination that has been invented to explain the subject and which, in the process, confuses people more. Many of these seem to fall within the category of *solutions seeking problems* and few pass muster on any test of intellectual rigour.

The terms given below were all found in just one edition of a published journal from one of the larger and more respected professional bodies.

Risk velocity	Risk universe
Risk clock speed	Risk intelligence
Risk maturity	Risk tone
Risk culture	Risk appetite statements
Risk governance	Risk complexity

We also seem to want to continually re-invent the management of risk by ascribing to it a new three-letter acronym. The following are just some of the current commonly used acronyms that, despite their popularity, stand little scrutiny:

ERM	ORM

CRM	PRM
GRC	BCM
SRM	BRM
IRM	RBT

The last of these, RBT (risk based thinking), has only just been coined by a committee that is revising ISO 9001 (the quality management standard). Irrespective of the fact ISO 9001 is fundamentally dealing with quality-related risk and that decisions taken to manage quality (as with all decisions) involve risk, it seems that the committee felt it could protect this paradigm by using a new, undefined expression to fudge the fact that these risks need to be competently managed. Eager to make money, some bodies are already offering courses and qualifications in RBT; which does seem analogous to offering training and certificates in breathing!

Unfortunately all these artefacts, encumbrances, confections and acronyms further externalise risk management from decision-making and create great confusion and complexity along the way.

They effectively disenfranchise those who are faced with decisions who need to manage risk most effectively and who need simple-to-understand support. However, not all in the risk management profession seem to share the view that risk management should be explained in the simple terms that are meaningful to decision makers. For example, the lead for the project to revise the 2004 COSO ERM Framework document was recently quoted as saying: *We're dealing with much more complicated issues regarding risk complexity and risk velocity*[2]

The creation of much of this paraphernalia seems no accident. There is clear evidence that in some cases consultants and software companies set out to sell a new wrapping to the same basic box of contents. Often repeating this tactic again and again. But these confections - often pedalled at expensive conferences labelled with the new buzz phrase - seldom survive any scrutiny in terms of successful management of the effect of uncertainty on objectives.

The following six myths demonstrate how confused and confusing is the way many in our profession explain how we should manage risk.

4 Cracking a half dozen myths

Myth 1 – The integration of risk management into decision making means consulting a pre-existing risk register

Whether decision-making results in a single action or the implementation of many in a plan, there is really no good reason why last year's risk register should be relevant to the decisions being made now (or in the future). Risks are not inputs to decisions, they are formed by decisions.

We can only consider the risks of decisions being made *now* in relation to the effect of uncertainty on our organisation's objectives as things stand at present or at some time into the foreseeable future; i.e. in the context of the current objectives and the current internal and external environments. These may or may not be different to those that drove earlier analyses of other decisions.

This must mean we need to manage risk as an integral part of a planning process, when many decisions are made, not as an input or add on. **Figure 1** shows that, to be fully effective, the risk management process should be fully merged and blended with the decision making process, not parallel, overlapping or just an input as in **Figure 2**.

[2] http://www.complianceweek.com/blogs/grc-announcements-accounting-auditing-update/coso-launches-project-to-update-erm-framework#.VFLBWIgxmrV

Figure 1: What truly integrated risk management looks like

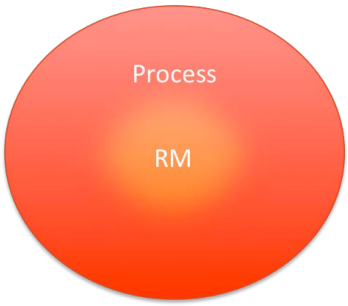
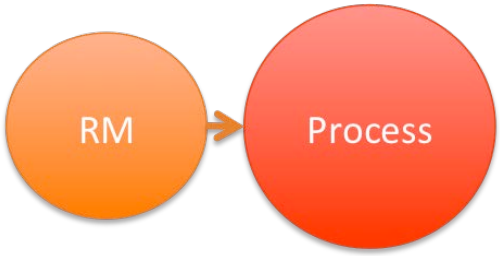


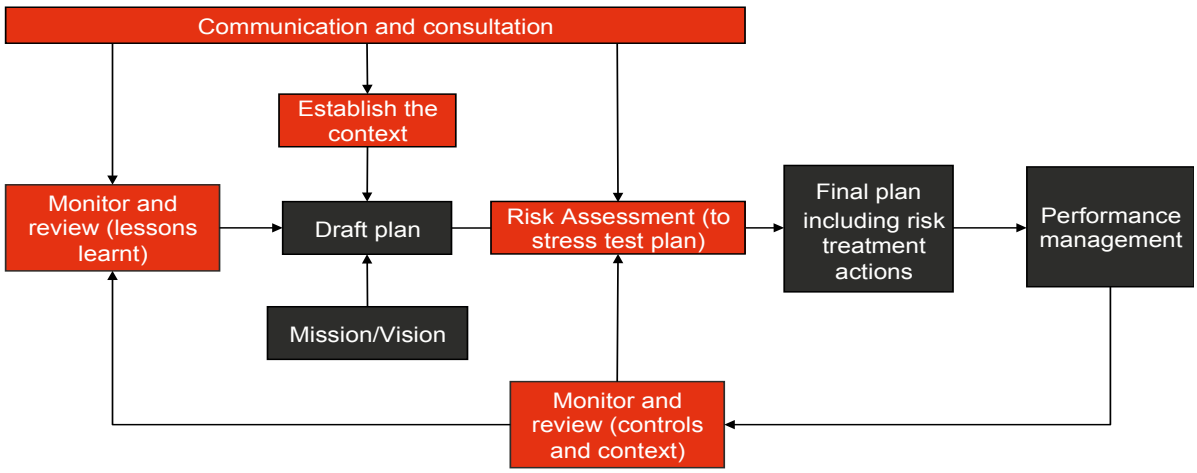
Figure 2: This is not integrated risk management



described using normal language.

Figure 3 depicts how the risk management process can be integrated into the process for the development and implementation of a strategic plan or business plan; both of which are just types of decision-making. Although this diagram uses the labels from ISO 31000 for the steps of the risk management process to illustrate this integration, in practice using such labels can be unhelpful. The purpose of the steps may be more readily understood if they are described using normal language.

Figure 3: Integration of the risk management process into the strategic planning process



Myth 2 - We can have different approaches and language for managing different types of risks

This myth underpins silo thinking that leads to confused and inconsistent decision-making. This is both inefficient and can lead to risks not being discovered, properly understood or correctly treated when required.

Even though we might sometimes find it useful to characterise risk by concentrating on one type of consequence, one type of risk source or one type of control, risk is just risk.

Silos defined by some type of classification of risk persist in organisations because:

- Those accustomed to running the silos can be protective of their sphere of influence, knowledge and status, and so resist change.

- The technical specialisation of the silo is defined by the expertise needed to understand the risks being managed by the silo.

There can be good reasons to group expertise but for the effective management of risk across all such clusters there should be a common language, common reporting mechanisms, and the same risk criteria.

Transitioning from a silo-based approach of managing some forms of risk to one involving a common system, or modifying the practices within an expertise group to conform to a common organization-wide approach, requires careful planning and execution. The change should be mandated by the governing body through senior management with clear communication and consultation around the benefits and implications of the change.

Myth 3 - The risk management framework is a document (that contains the risk rating system)

Apart from having a dependable *process* for managing risk, organisations also need to express their intentions that this process will be applied to all decision making. Of course, intentions mean nothing unless backed by organisational capacity – such as competency and relevant resources – and by arrangements that give confidence that the process is being applied correctly and consistently.

The risk management framework is just the collection of *stuff* that enables the risk management process to be applied to decision-making and risks to be modified as required. The framework has two parts – both of which are particular to an organisation:

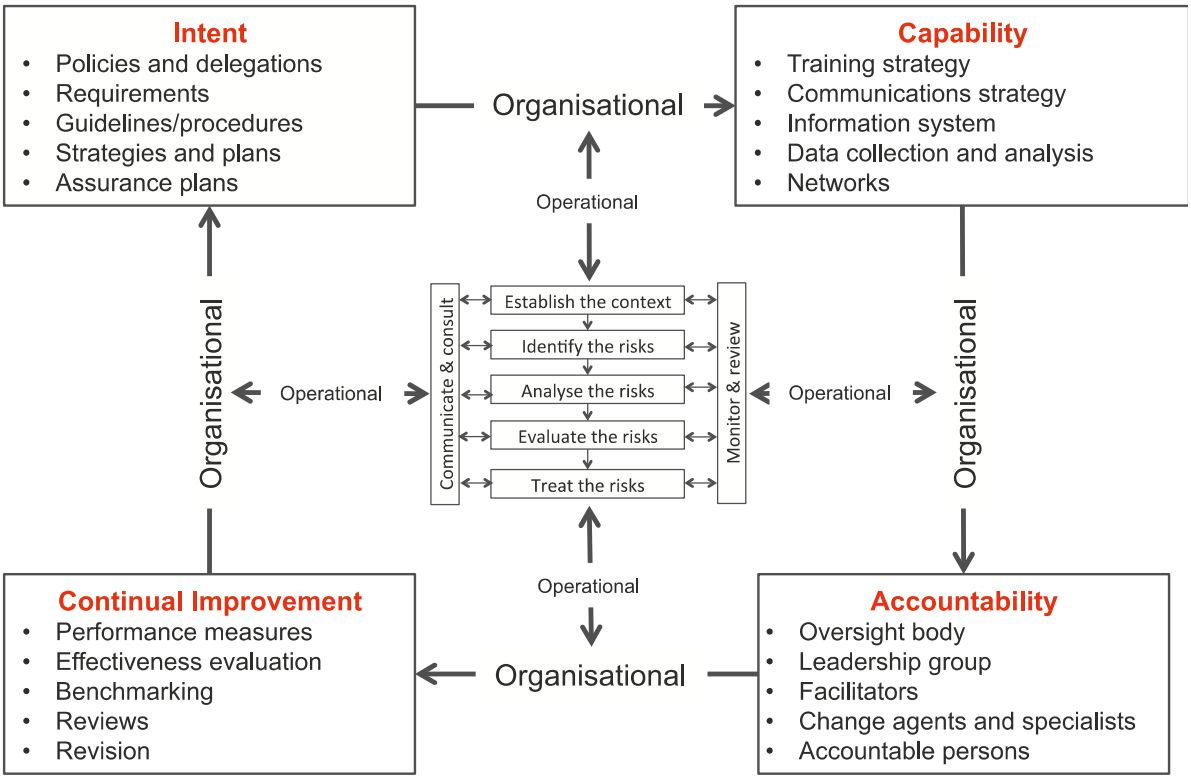
1. An expression of the organisation's intentions - how it signals what, why and how risk will be managed. This might be by policies, standards and other management practices;
2. The capacity it provides to manage risk in keeping with these intentions. This consists of:
    - Tools;
    - Capability to use them as part of decision making;
    - Arrangements to confirm that intentions are satisfied;
    - An ability to continuously adapt, respond to change and improve.

For the reasons given before, ideally we should not have elements of the organisation's system of management labelled as *risk something*. Managing risk is simply a way of understanding and dealing with the effect of uncertainty on the organisation's objectives in the course of decision-making and if we have separate artefacts labelled in terms of risk or risk management, this tends to externalise or dis-integrate the risk management process from decision-making.

While it is always a good idea to describe the elements of the framework and how they should perform to help us manage risk, the risk management framework is not a document.

Figure 4 illustrates one way of depicting the architecture of a risk management framework and its components

Figure 4: Architecture of a framework



Myth 4 - Risk registers are important

Some seem to believe that risk registers possess magic properties: just creating them is sufficient for an organisation to manage risk effectively. However, in reality, they are simply records of discussions that were held at a point in time: just *snapshots*. At most, risk registers are a means to an end – more effective controls and an acceptable level of risk.

Many organisations believe that good risk management means they must generate and store a large number of pieces of information in their risk registers even though there are no clear intentions as to the end use.

The tests that should be applied to these documents, that are supposed to be a record of the conversations that took place, are:

1. What management activity is the information required to support?
2. Is the information suited to these purposes?
3. Can those who should use the registers be able to read and understand the conversation that took place and draw the correct conclusions?

In practice risk registers only require a few pieces of information that is expressed using clear descriptions and avoiding acronyms or jargon.

While it is custom and practice to use landscape-orientated tables or spread sheets to record this information, the inevitably narrow columns lead to compromises in quality and *understanding*. It therefore seems preferable to create records of these conversations in other forms: for example, to describe one risk on each page and include more useful and meaningful information.

Many organisations spend a great deal of time and effort updating *the (only) risk register,* but rationally it is difficult to see the validity or value in this. If a risk register is the form of record we think we should make of the conversations we have on risk when we are faced by a decision, this must mean we should generate and keep numerous risk registers. However, more practically, maybe we should challenge this custom and rethink whether we need to record and keep the results of these conversations at all.

It is entirely possible that we don't need to create or preserve these long-winded, complex documents that, after all, are just a means to an end. Context statements, risk treatment plans and control assurance plans are much, much more important and valuable but, unfortunately, many organisations do not write these down or keep them.

Myth 5 - Risks (actually) occur

We use examples of things that might happen (because there is a source of uncertainty) and what they might lead to in terms of our objectives - to help us understand risk. Risks are therefore just examples, illustrations or hypotheses and it is entirely fortuitous if events occur exactly as we have predicted.

When something happens which has been contemplated in the characterisation of risk some people say: "the risk has happened". However, to say this is to fundamentally misunderstand risk. Firstly, for there to be risk, there must be uncertainty; i.e. a probability between 1 and 0. If something has happened, the probability is 1 so there is no risk so far as that particular source is concerned. Secondly, if risk exists, it exists as a result of the decision that generated it. It cannot also *happen*.

It is therefore not correct to say that a risk has *happened* or when there has been an event that a risk has *occurred*.

Myth 6 - We need to conduct risk reviews once a year to tell the board or audit committee what our risks are

A reporting requirement is never a good reason for the application of the risk management process. We manage risk to create value, through enhancing the decisions we make.

The role of an audit (or risk) committee is to be satisfied that things are occurring as the organisation intends. Therefore, so far as risk management is concerned, the committee needs to know that, when decisions are being made:

- The organisation will have a current, comprehensive and correct understanding of the risk it faces; and
- The magnitude of risk is at an acceptable level.

However, it is impossible for a committee to know that this has been achieved by looking only at a historical, probably out of date, list of risks in a risk register. The existence of a *red* or *orange* risk in the register, says nothing about the validity or competency of the process by which this was derived.

How does the committee know that those risks are current, comprehensive and correct? What evidence has it that the organisation has the capacity to manage risk on an ongoing basis, as part of everyday decision making? The committee can only answer these questions if it is provided with reliable evidence that the organisation's framework for managing risk is soundly based and continues to be effective.

The third edition of the Australian Securities Exchange (ASX) Corporate Governance Principles recognises this problem and this is the reason that Principle 7 now says that:

- "A listed entity should establish a sound risk management framework and periodically review the effectiveness of that framework."
- "Recognising and managing risk is a crucial part of the role of the board and management."
- "It is the role of management to design and implement that framework. It is the role of the board to oversee its risk management framework and to satisfy itself that the framework is sound."
- "The board or a committee of the board should review the entity's risk management framework at least annually to satisfy itself that it continues to be sound."

ASX Principle 7 references AS/NZS ISO 31000:2009 Risk management – Principles and guidelines to define risk management as "coordinated activities to direct and control an organization with regard to risk" and a "risk management framework" as a "set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization".

The implications of this for Australian listed companies are that:

- They have to demonstrate they have a sound framework for managing risk - otherwise any other risk information they supply to Boards and their committees does not have credibility;
- Reporting to a Board or its committees should focus on the framework and its soundness;
- Information on risks, controls and risk treatment can only be used to illustrate active conversations about managing risk; and
- Reports should also include performance management and effectiveness evaluations.

5 What does this mean for RiskNZ?

The stated purpose of RiskNZ is: *to improve the knowledge and practice of Risk Management in New Zealand.*

This requires RiskNZ to take an active role cracking these and similar myths, quelling fads and discouraging the use of the tide of mainly nonsensical jargon that currently bedevils our profession. If RiskNZ's role is to share and enhance skills and understanding amongst all sectors and disciplines about the management of risk then it should promote approaches that are clear, simple and useful.

It is therefore suggested that RiskNZ should avoid the proliferation of unnecessary and invalid jargon in what it publishes and what it allows to be presented in its name.

Furthermore it should promote in all that it does, that managing risk is a process whose principal purpose is to support better decisions and thus MUST occur as an integral part of decision making in all organisations.