Broadleaf

Creating value from uncertainty

Broadleaf Capital International Pty Ltd

ABN 24 054 021 117

www.Broadleaf.com.au

Keynote speech: Hearing over the cacophony

RiskNZ

Prepared by:

Grant Purdy

Associate Director

Version 2, October 2014

Copyright

ABN 24 054 021 117

www.Broadleaf.com.au

PO Box 607, Cammeray, NSW 2073
Tel: +61 2 9488 8477
Cooper@Broadleaf.com.au

Broadleaf

Today

Challenge the value of the multitude of artifacts, encumbrances and three letter acronyms that clog up risk management practice

Smash a half dozen myths

Draw some conclusions on keeping it simple (but not simplistic)

Hearing over the Cacophony
3

Broadleaf

Central concepts

Hearing over the Cacophony
4

Broadleaf

The simple creed

Risk is the *effect of uncertainty* on what we want to achieve, our objectives

It arises from factors in the external and internal environment that create uncertainty - risk sources

It's neither positive not negative - the way we describe it depends on whether we view the potential consequences as advantageous or not

We use risk**s** to describe risk. These are simply statements that describe examples of things that might happen or are present and what they might lead in to in terms of effects on our objectives

Controls are the things we already have in place that *are modifying* risk. They enable us to achieve our objectives

Hearing over the Cacophony
5

Broadleaf

What does managing risk really involve?

1. Challenging assumptions and preconceptions before decisions are made
2. Taking appropriate actions to reduce the uncertainty that our objectives will be achieved
3. Providing early warning that key controls are not in place or are not be fully effective, so that pre-emptive actions can be taken
4. Enabling the organisation to learn from its successes and failures – at a fundamental level

Hearing over the Cacophony
6

Broadleaf

Risk management is decision support

The things you automatically consider (to some extent) when making a decision (implicit or explicit)

1. What do I want to achieve?
2. How shall I go about it?
3. Who do I need to involve?

4. What might help me or impede me?
5. What lessons can I learn from the past?
6. What I need to do to make sure I am successful?
7. How do I know if I will be successful?

Hearing over the Cacophony
7

Broadleaf

We already manage risk – naturally

Every time we are faced with a decision, we are inevitably mindful of the related uncertainties

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 the risk management process just ensures this normal, intuitive approach is more complete and effective

Risk management is already integrated and natural, we should not attempt to de-integrate it and make it unnatural

Enhancement should be *in situ* not *in vitro*

Hearing over the Cacophony
8

Broadleaf

Risk management is a dynamic, not static process

Its triggered by the need to make a decision, not by a calendar

There is little point in doing it for its own sake

Periodic risk register reviews create little value and often send the wrong message

Hearing over the Cacophony
9

Broadleaf

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

After Henry Finck, writing about modern atonal music in 1914

Hearing over the Cacophony
10

Broadleaf

Fads
Artefacts, Encumbrances and Three Letter Acronyms

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

- ERM
- CRM (collaborative risk management)
- GRC
- SRM
- IRM
- ORM
- PRM
- BCM
- BRM
- oh, and 'Resilience'

Hearing over the Cacophony
11

Broadleaf

These artifacts, encumbrances and acronyms, oppose the natural integration of risk management with decision making

They disenfranchise those who are faced with decisions, who need to manage risk effectively and who need support

They seem to be normally created as a marketing ploy by consultants or software producers

Hearing over the Cacophony
12


Broadleaf
A half dozen myths to crack
Hearing over the Cacophony
13


Broadleaf
Myth 1
Integration of risk management means consulting a pre-existing risk register
Hearing over the Cacophony
14

Broadleaf

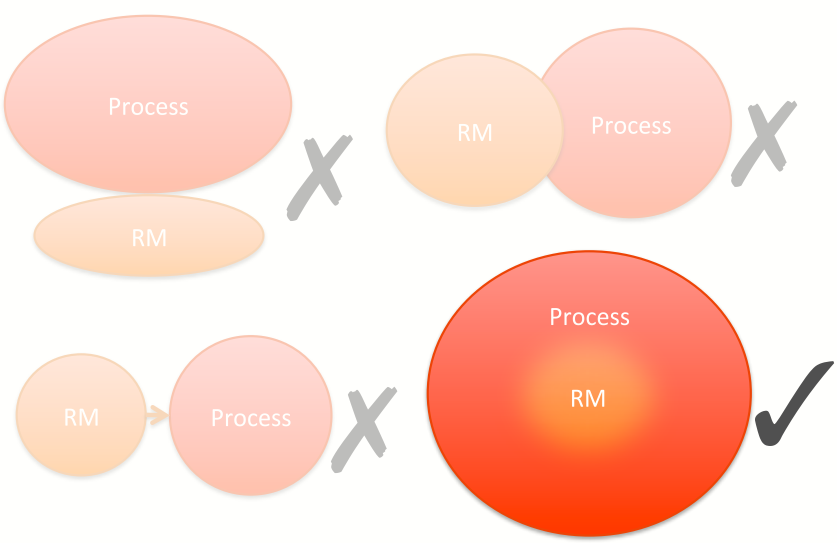
Risk management and planning

- Why is last year's risk register relevant for the decision we face now?
- Surely we need to consider the implications of the decision we face in relation to the effect of uncertainty on the organisation's objectives
- We need to consider both the uncertainties in achieving successful outcomes from the decision and also the uncertainties for our overall objectives
- This means we need to manage risk as an integral part of the planning process – not as an input or add on

Hearing over the Cacophony
15

Broadleaf

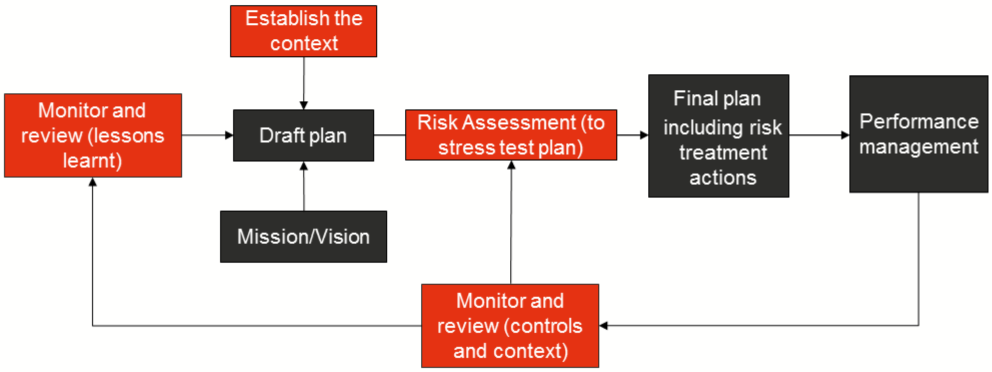
Merged and blended, not parallel, overlapping or just an input



Hearing over the Cacophony
16

Broadleaf

Development and implementation of the strategic plan (or any plan)

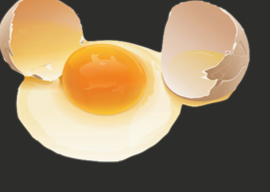


Hearing over the Cacophony
17

Broadleaf

Myth 2

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



Hearing over the Cacophony
18

Silo thinking

Risk is risk! There are not different types of risk.

However, we sometimes try to characterise risk by concentrating on one type of consequence, one type of source or one type of control

Silos persist because:

1. Those accustomed to running the silos can be protective of their sphere of influence and status, and so resist change
2. Technical specialization of the silo being defined by the expertise needed to understand the risks being managed by the silo

Solution

There can be good reasons to preserve clusters of expertise.

However, across all such silos 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 fully common system, or modifying the practices within silos 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.

Broadleaf

Myth 3

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

Hearing over the Cacophony
21

Broadleaf

What is a framework?

It's a collection of 'stuff' that makes risk management 'happen' in an organisation

It consists of two parts:

1. An expression of the organisation's intentions - how it signals what, why and how risk will be managed
2. The capacity it provides to manage risk in keeping with its intentions:
    - Tools
    - Capability to use them as part of decision making
    - Ability to continuously adapt and improve

Hearing over the Cacophony
22

Broadleaf

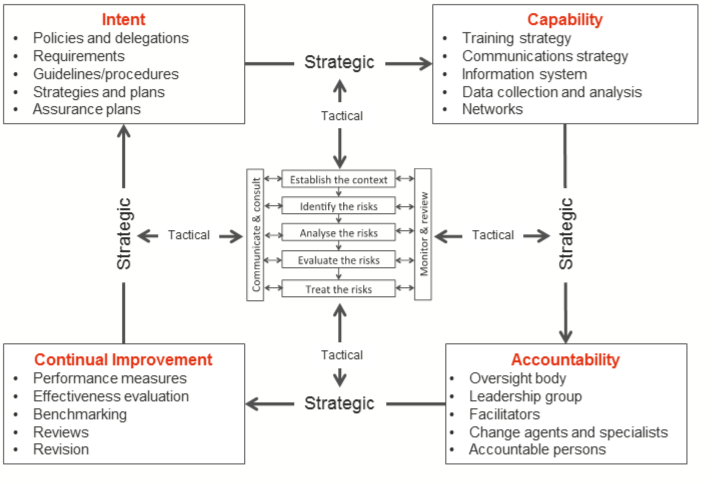
Implications

- Ideally we should not have elements of the organisation's system of management badged as *risk* ...
- The management of risk is simply a way of understanding and dealing with the effect of uncertainty on the organisation's objectives
- If we have separate artefacts described in terms of risk or risk management, we are defeating the primary purpose of managing risk
- To manage risk we need to access and use most of the elements of a normal management system
- This is the way we avoid *de-integration*
- Oh, and the framework is not a document!

Hearing over the Cacophony
23

Broadleaf

Architecture of a framework



Hearing over the Cacophony
24

Broadleaf

Myth 4

Risk registers are important

Hearing over the Cacophony
25

Broadleaf

Risk registers

They are not magic - just records of discussions that were held at a point in time: snapshots!

At most, a means to an end

The tests:

- Is the information collected really useful and useable?
- Can a normal person read and understand it?

This requires:

- Only a few columns
- Full descriptions, avoiding acronyms or jargon

Could we avoid the limitations of using a table or spreadsheet with narrow columns?

Hearing over the Cacophony
26

Broadleaf

The context statement, risk treatment plan and the control assurance plan are much, much more important documents than the risk register

Do you preserve these?

Hearing over the Cacophony
27

Broadleaf

Myth 5

Risks (actually) occur

Hearing over the Cacophony
28

Broadleaf

Risks

We use examples of things that might happen (because there is a risk source) and what they might lead to in terms of our objectives - to help us understand risk

Risks are just examples, illustrations, scenarios or hypotheses

We use them to estimate the level of risk, expressed as the likelihood that particular consequences will be experienced

NB. - consequences should relate directly to objectives

We sometime use events for this illustration or, often, a situation or circumstance that is present now or might occur at some point in the future

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

Hearing over the Cacophony
29

Broadleaf

Myth 6

We need to conduct risk reviews once a year to tell the audit committee what our risks are

Hearing over the Cacophony
30

Broadleaf

Risk management for reporting

A reporting requirement is never a good reason for risk management

We manage risk to create value – through supporting decisions

What do your audit/risk committee really need to know?

- That you have an current, comprehensive and correct understanding of the risk your organisation faces
- And that those risk are within your risk criteria

But how do they know if these are true just by looking at a historical, probably out of date, list of risks? How do they know that those risks are current, comprehensive and correct?

So the committee's primary responsibility should be to ensure that the framework is working correctly

Hearing over the Cacophony
31

Broadleaf

ASX Principle 7 (Ver. 3)

- 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 and to ensure that the entity operates within the risk appetite set by the board. It is the role of the board to set the risk appetite for the entity, 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

Australian/New Zealand Standard AS/NZS ISO 31000:2009 *Risk management – Principles and guidelines* defines "risk management" as "coordinated activities to direct and control an organization with regard to risk" and "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".

Hearing over the Cacophony
32

Broadleaf

Broadleaf

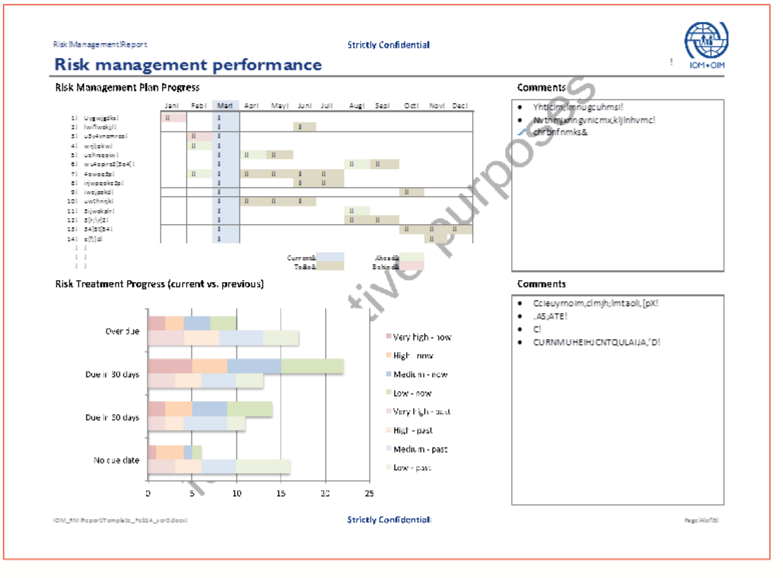
Implications

- Organisations have to be able to demonstrate they have a sound framework for managing risk
- Otherwise any risk information does not have any credibility
- This means that any reporting to a Board has to focus on the framework and its performance
- Information on risks, controls and risk treatment just illustrate we are actively managing risk
- This requires performance management, effectiveness evaluation and reporting

Hearing over the Cacophony
33

Broadleaf

Performance part of a report



Hearing over the Cacophony
34

Broadleaf

Some more myths that need cracking …

1) The level of risk is probability of the event x impact
2) We should categorise risks according to consequence type
3) We need a risk appetite statement
4) We need to measure inherent risk or target risk
5) Key risk indicators pick up emerging risks
6) Auditors should focus on high risks

Hearing over the Cacophony
35

Broadleaf

Summary

To improve the knowledge and practice of Risk Management in New Zealand

Should the Society be doing more to crack the myths, quell the fads and discard the jargon that bedevil our profession?

If the Society's role is to share and enhance skills and understanding amongst all sectors and disciplines about the management of risk then, surely, we should promote approaches that are clear, simple and useful?

The Society should promote in all it does that:
risk management is a process whose principal purpose is to support better decisions and thus MUST be integral to decision making in all organisations

Hearing over the Cacophony
36

Broadleaf

Contact

Grant Purdy
Associate Director

Purdy@Broadleaf.com.au
+61 412 121 631
+61 3 9893 0011

PO Box 1098
Mitcham North, VIC 3123
Australia

For further information visit www.Broadleaf.com.au