Broadleaf

Creating value from uncertainty

Broadleaf Capital International Pty Ltd

ABN 24 054 021 117

www.Broadleaf.com.au

Case study:
Evaluating and enhancing risk management in an international business

At the request of the board, Broadleaf carried out an independent review of the current framework, strategy and process for managing risk in a major international commercial organisation. We were asked to provide our professional opinion on the current situation and to give advice on any further steps that should be taken to enhance and improve the foundations for risk management.

Version 1, 2015

Broadleaf

Contents

Figures

1 Background

Our client, a major international business, has a mature framework for risk management that is aligned with ISO 31000:2009.

To satisfy national corporate governance requirements, the board adopts an active role in reviewing the company's policies on risk oversight and management to satisfy itself that the company has developed and implemented a sound system of risk management.

While the board believed the company's approach to risk management was generally satisfactory, previous audits were regarded as superficial and had not provided it with the degree of assurance it required. As leading experts in this field, Broadleaf was commissioned to conduct an independent review of the current framework, strategy and process for managing risk and to compare these to best practice. The board requested our professional opinion on the current situation and that we give the company advice on any further steps that should be taken now to enhance and improve the foundations for risk management.

After many years of practical experience in evaluating and enhancing risk management, we believe that success depends as much on the manner in which any changes to a framework are developed and implemented as it does on the detail of the tools and written materials generated. This is why we adopted an approach here that sought the views of key internal stakeholders on the current ways of managing risk and then involved them in the development and approval of the enhancement strategy, to ensure they accepted the review and owned its outcomes.

It was also important for us to continually interact with the company risk management team, so that our advice was framed in a manner that supported the improvements they had planned already. We met the team throughout the review to explain and demonstrate practical options for any enhancements or additions we recommended, before we finalised our report.

2 Approach

Our approach involved a structured, interactive review and gap analysis of the existing risk management framework and applications of the process, from both a technical and practical perspective, so as to understand whether the company's current approach reflected good practice, whether it was suitable

for the organisation and whether it could be adapted and enhanced to make it more effective if that was necessary.

We used ISO 31000:2009 as a basis for the review, supplemented by our own experience of what represents good practice in organisations of the size and nature of the company. Throughout the initiative we worked closely with members of the company Group Audit and Risk function, transferring knowledge.

Figure 1 shows an outline of the approach we followed, as described below.

2.1 Preparation

The study started with a meeting where the detailed arrangements for the study were agreed, including the schedule of activities and delivery dates, the documents needed for review and those managers we wanted to interview.

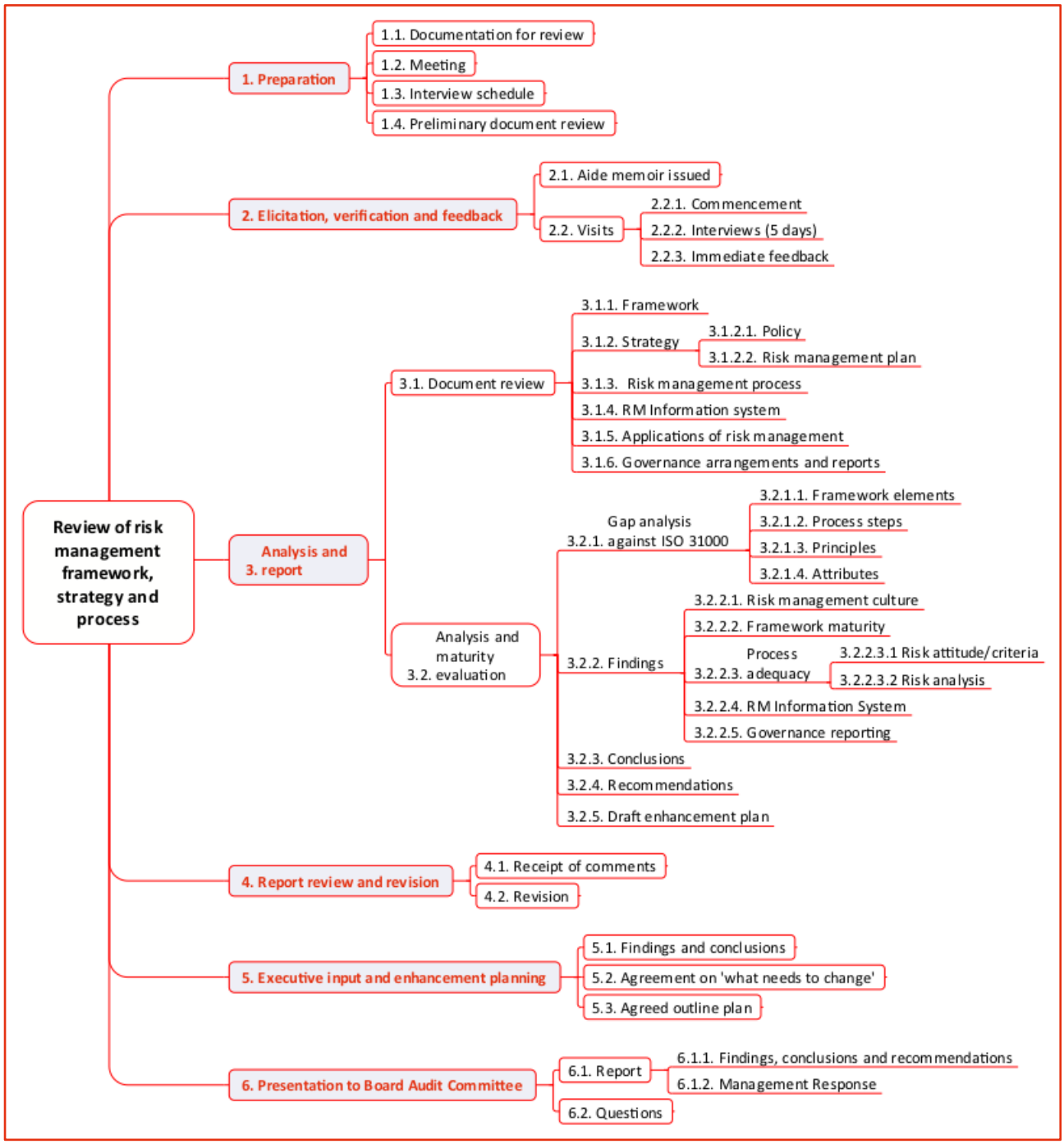
Prior to the initial meeting we issued a list of background documentation we needed for the review and opened up a secure Internet portal for the uploading of the documents. The list included:

- Relevant policy statements, framework descriptions, internal standards and procedures, with a particular focus on decision support and controls assurance;
- Internal standards, procedures or guidelines that deal with particular applications of risk management. For example in the areas of safety, procurement, security, operations, maintenance, BCM, compliance and project management;
- The current strategic plan and objectives;
- Examples of risk management plans and control assurance plans;
- Extracts from the risk management information system including risk registers and risk treatment plans;
- Methodology for and outputs from any quantitative risk analysis studies (range analyses);
- Copies of recent reports to any risk management steering committees or review groups and the Audit Committee that show risk management performance;
- Copies of any existing training and briefing materials that deal with risk management.

We conducted a preliminary review of the materials supplied and, from this, developed an *aide memoire* of sample questions that would be asked during

interviews. This document was supplied to the company so that it could be passed on to those who were to be interviewed to allow them to prepare.

Figure 1: Our approach to the review



2.2 Elicitation, verification and feedback

In our experience it is vital to observe and review how risk management takes place in practice. This is particularly true if there might be any discontinuity of practice across an organisation or inconsistent processes and systems. It is also important to test management's perceptions of the current approach to risk management to see if it is currently viewed as effective and is likely to satisfy their future needs.

In this case we undertook this observation through a series of structured interviews with senior managers from which we drew conclusions on:

- The suitability of the current framework and tools to manage risk associated with an organisation of its size and complexity, its risk profile and risk attitude (appetite);
- The drivers of that attitude, based on what are recognised as the 'key success factors' and growth objectives for the organisation;
- The perceived usefulness of the current risk management process and its degree of integration into key decision-making processes;
- The strengths and limitations of the other approaches to risk management specific to particular kinds of risks that co-exist in the organisation;
- Whether the tools and methods currently being used are capable of providing a current, correct and comprehensive understanding of its risks and inform it whether the risks are within its risk criteria;
- The level of understanding of senior managers about aspects of the risk management culture;
- An outline of the perceived risk profile of the organisation and whether this varies from accepted and reported risk profiles.

At the conclusion of the interviews we provided immediate feedback to Audit and Risk staff on:

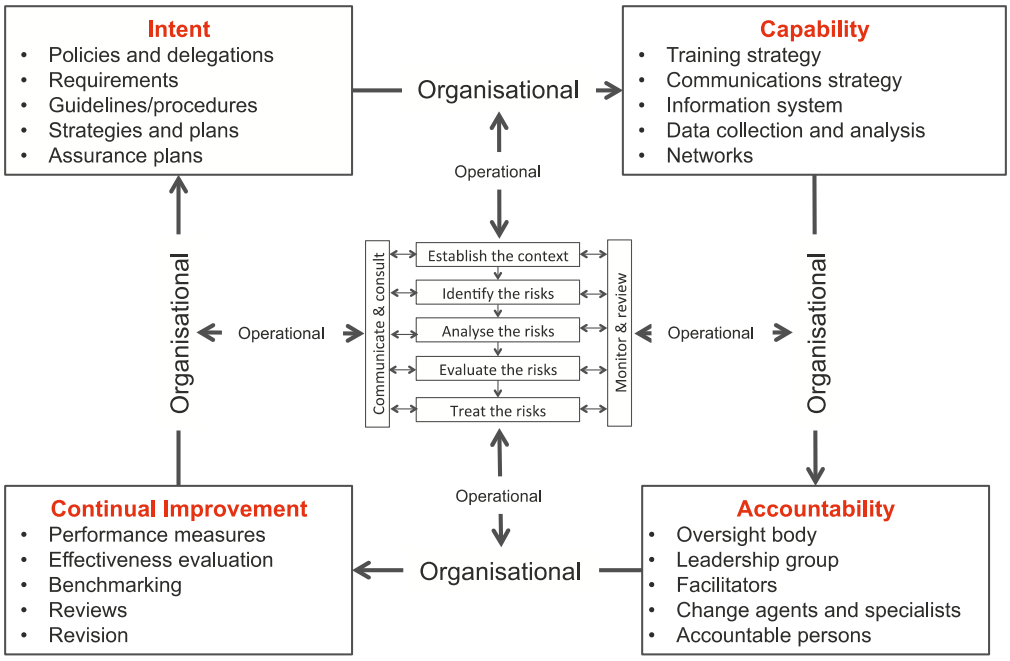
- Our major findings;
- Our conclusions on the level of maturity, the strengths and weaknesses;
- Our initial thoughts on where the company could enhance the management of risk and the steps that should be taken.

2.3 Analysis and report

Figure 2 shows the generic architecture of a risk management framework. This is a collection of *elements* 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

Figure 2: Architecture of a risk management framework



Our interviews concentrated on understanding how the risk management process was applied in practice and, in particular, how managers identified risks and made decisions on whether levels were acceptable. To do this we had to understand if the existing risk criteria accurately reflected the company's risk attitude. We also looked at the current qualitative risk analysis system and the instructions on its application to see if they were clear, unambiguous and technically valid. The existing consequence criteria and scales were compared with the company's critical success factors, and we assessed if the likelihood scales were useful and relevant.

Assessments of the effectiveness of existing controls and estimation of potential exposures are also vital components in risk analysis. We therefore

compared the current approach to the guidance in the Institute of Internal Auditors/Standards Australia handbook HB 158:2010.

Using all the information gathered we conducted a gap analysis and maturity evaluation using ISO 31000:2009 and what we understand is world's best practice as a basis for comparison. An example of output is shown in Figure 3.

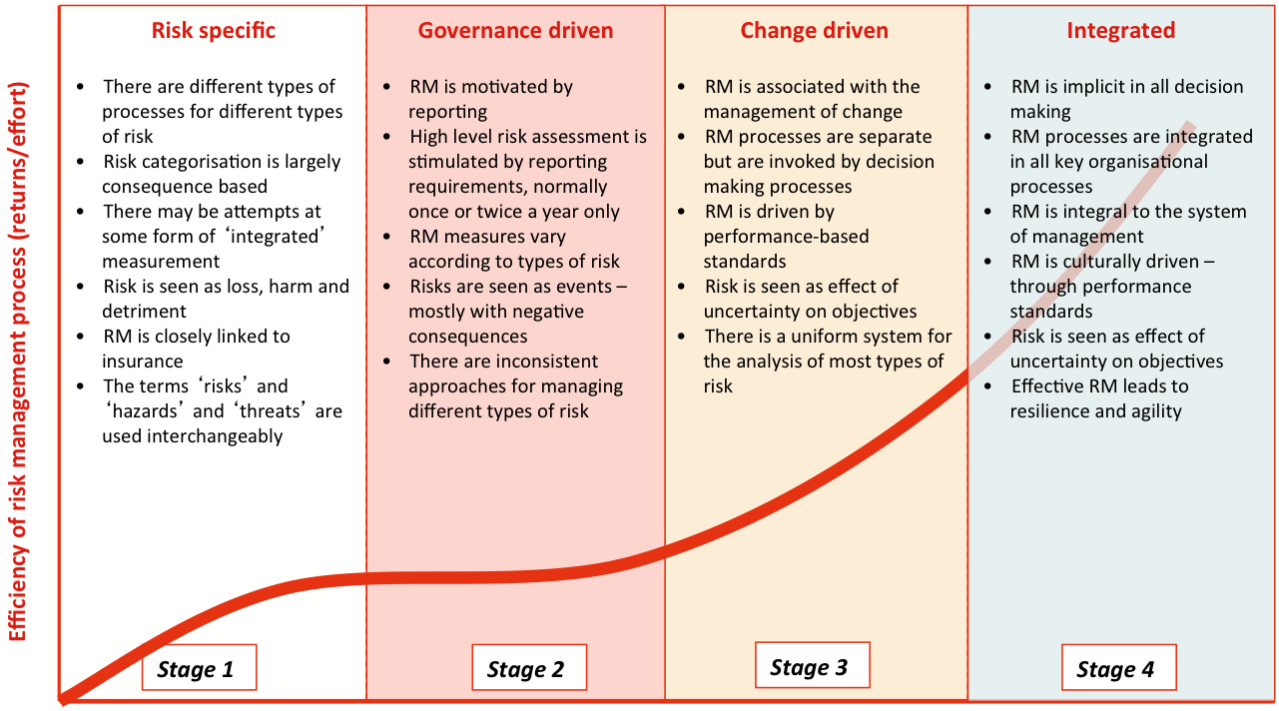
In general, we found the company's approach to risk management did not contain all the elements of a fully effective risk management framework as described in ISO 31000:2009. It also did not fully satisfy the principles for effective risk management and the attributes of enhanced risk management given in the standard.

Following the maturity scheme shown in Figure 3 we found that, in practice, the company's approach to risk management fell generally in Stage 2 with some instances in Stage 1 and others in Stage 3.

Figure 3 reflects the way organisations normally advance in risk management as they implement a risk management framework that aligns with Clause 4 of the ISO standard and adopt the principles of effective risk management and the attributes of advanced risk management given there. While the risk management process can be applied in isolation to specific risk types (Stage 1) and risk management can be used purely to generate occasional governance reports (Stage 2), ISO 31000:2009 makes it clear that the management of risks will not be truly effective until it becomes dynamic and is fully integrated into the organisation's processes for decision making.

In this case we found that while clearly managers in the company did consider risks when they made decisions this was rarely a structured and comprehensive process.

Figure 3: Risk management maturity scale



Our report made findings on:

- The framework and how it facilitated the integration of risk management into decision making, including risk management plans and the strategy for their implementation;
- How risk management was applied in strategy development and during all forms of planning, for decision-making and change management;
- The reliability of each element of the risk management process;
- How the overall risk profile of the company was obtained and evaluated through aggregation and roll-up and how risks were treated at a corporate level;
- The form and content of governance reporting;
- How risk treatments were closed out and the monitoring and review of risks, controls and risk treatments;
- The company culture as it pertained to the management of risks in terms of both intent and practice;
- The adequacy and effectiveness of the systems and resources available to support the management of risk, including human resources.

We also identified opportunities for improvement to the company's current approach for risk management including its implementation strategy and the

resources and systems available. In all cases, where the current approach varied from best practice, we made practical suggestions about how improvements could be made.

Our report contained a draft enhancement plan where the timings in the plan reflect the necessary critical path to be followed for the implementation of framework enhancements and the activities and actions required to bring risk management at the company to a best practice standard in a reasonable and practical time period.

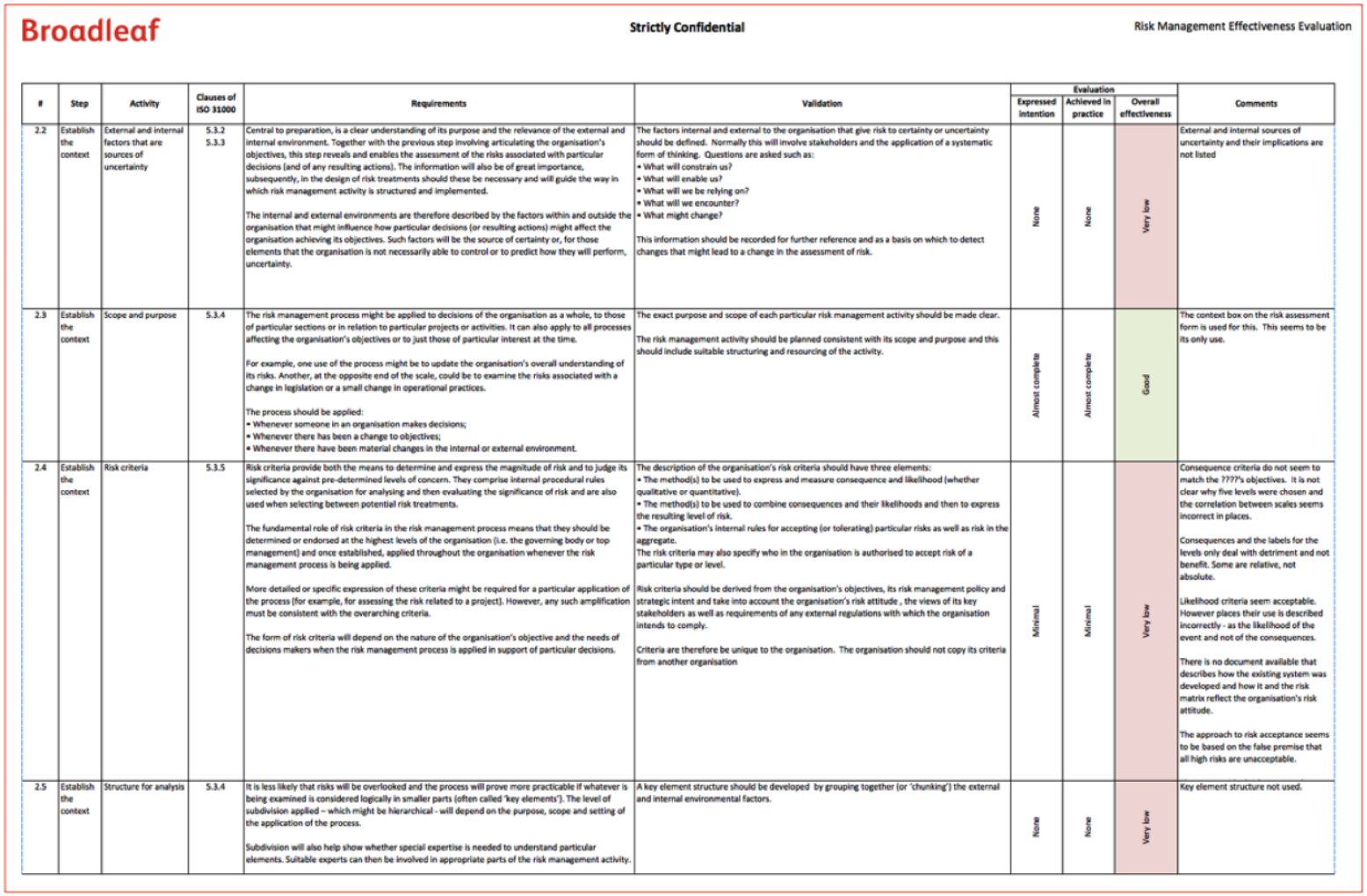
2.4 Senior management input and enhancement planning

It is important that senior managers appreciate and can comment on the findings and conclusions from such reviews as this leads to support for an enhancement plan. It is important that this takes place before any report is made available to the board so that the company can indicate its response.

We therefore presented our findings and recommendations at a short meeting with senior managers. The draft agenda was:

1. Fundamentals of risk and best practice risk management;
2. Overall findings and assessment of the review;
3. Suggested improvements and enhancement strategies;
4. Draft enhancement plan.

Figure 4: Example extract from evaluation report

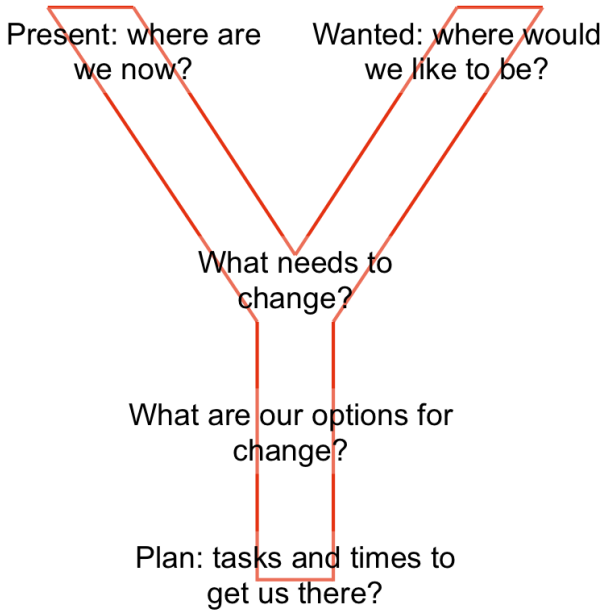


Broadleaf — Strictly Confidential — Risk Management Effectiveness Evaluation

#	Step	Activity	Clauses of ISO 31000	Requirements	Validation	Evaluation: Expressed intention	Evaluation: Achieved in practice	Evaluation: Overall effectiveness	Comments
2.2	Establish the context	External and internal factors that are sources of uncertainty	5.3.2 5.3.3	Central to preparation, is a clear understanding of its purpose and the relevance of the external and internal environment. Together with the previous step involving articulating the organisation's objectives, this step reveals and enables the assessment of the risks associated with particular decisions (and of any resulting actions). The information will also be of great importance, subsequently, in the design of risk treatments should these be necessary and will guide the way in which risk management activity is structured and implemented. The internal and external environments are therefore described by the factors within and outside the organisation that might influence how particular decisions (or resulting actions) might affect the organisation achieving its objectives. Such factors will be the source of certainty or, for those elements that the organisation is not necessarily able to control or to predict how they will perform, uncertainty.	The factors internal and external to the organisation that give risk to certainty or uncertainty should be defined. Normally this will involve stakeholders and the application of a systematic form of thinking. Questions are asked such as: • What will constrain us? • What will enable us? • What will we be relying on? • What will we encounter? • What might change? This information should be recorded for further reference and as a basis on which to detect changes that might lead to a change in the assessment of risk.	None	None	Very low	External and internal sources of uncertainty and their implications are not listed
2.3	Establish the context	Scope and purpose	5.3.4	The risk management process might be applied to decisions of the organisation as a whole, to those of particular sections or in relation to particular projects or activities. It can also apply to all processes affecting the organisation's objectives or to just those of particular interest at the time. For example, one use of the process might be to update the organisation's overall understanding of its risks. Another, at the opposite end of the scale, could be to examine the risks associated with a change in legislation or a small change in operational practices. The process should be applied: • Whenever someone in an organisation makes decisions; • Whenever there has been a change to objectives; • Whenever there have been material changes in the internal or external environment.	The exact purpose and scope of each particular risk management activity should be made clear. The risk management activity should be planned consistent with its scope and purpose and this should include suitable structuring and resourcing of the activity.	Almost complete	Almost complete	Good	The context box on the risk assessment form is used for this. This seems to be its only use.
2.4	Establish the context	Risk criteria	5.3.5	Risk criteria provide both the means to determine and express the magnitude of risk and to judge its significance against pre-determined levels of concern. They comprise internal procedural rules selected by the organisation for analysing and then evaluating the significance of risk and are also used when selecting between potential risk treatments. The fundamental role of risk criteria in the risk management process means that they should be determined or endorsed at the highest levels of the organisation (i.e. the governing body or top management) and once established, applied throughout the organisation whenever the risk management process is being applied. More detailed or specific expression of these criteria might be required for a particular application of the process (for example, for assessing the risk related to a project). However, any such amplification must be consistent with the overarching criteria. The form of risk criteria will depend on the nature of the organisation's objective and the needs of decisions makers when the risk management process is applied in support of particular decisions.	The description of the organisation's risk criteria should have three elements: • The method(s) to be used to express and measure consequence and likelihood (whether qualitative or quantitative). • The method(s) to be used to combine consequences and their likelihoods and then to express the resulting level of risk. • The organisation's internal rules for accepting (or tolerating) particular risks as well as risk in the aggregate. The risk criteria may also specify who in the organisation is authorised to accept risk of a particular type or level. Risk criteria should be derived from the organisation's objectives, its risk management policy and strategic intent and take into account the organisation's risk attitude , the views of its key stakeholders as well as requirements of any external regulations with which the organisation intends to comply. Criteria are therefore be unique to the organisation. The organisation should not copy its criteria from another organisation	Minimal	Minimal	Very low	Consequence criteria do not seem to match the ????'s objectives. It is not clear why five levels were chosen and the correlation between scales seems incorrect in places. Consequences and the labels for the levels only deal with detriment and not benefit. Some are relative, not absolute. Likelihood criteria seem acceptable. However places their use is described incorrectly - as the likelihood of the event and not of the consequences. There is no document available that describes how the existing system was developed and how it and the risk matrix reflect the organisation's risk attitude. The approach to risk acceptance seems to be based on the false premise that all high risks are unacceptable.
2.5	Establish the context	Structure for analysis	5.3.4	It is less likely that risks will be overlooked and the process will prove more practicable if whatever is being examined is considered logically in smaller parts (often called 'key elements'). The level of subdivision applied – which might be hierarchical - will depend on the purpose, scope and setting of the application of the process. Subdivision will also help show whether special expertise is needed to understand particular elements. Suitable experts can then be involved in appropriate parts of the risk management activity.	A key element structure should be developed by grouping together (or 'chunking') the external and internal environmental factors.	None	None	Very low	Key element structure not used.

For the planning component of the session we used the 'Y model' (see Figure 5) to elicit feedback and ownership of the current situation, the wanted situation and what needed to change. The management team was encouraged to discuss and compare options and then to finalise the enhancement plan actions and agree timelines. These agreements were recorded and included in our final report.

Figure 5: Y model process



2.5 Report to the Board and Audit Committee

We supported the company in presenting the review findings, conclusions and the agreed enhancement plan to the board and its audit committee. Figure 6 shows an example of the form of summary plan that was presented to the board.

Broadleaf

Figure 6: Summary enhancement plan

3 Lessons

This review arose because the company and its board did not have confidence in the reviews conducted previously by generalist audit companies. Reviewing the approach to risk management in a complex organisation requires special skills and considerable experience. As an important part of the review must involve interviews with senior managers, the credibility of the interviewer is paramount if useful responses are to be obtained and if those are to be interpreted properly.

While it is important to follow a structured approach to the gap analysis and evaluation, the resulting conclusions and recommendations must be both customised and practical. Most importantly, they must reflect credible ways that similar organisation manage risk in the 'real world'.

Although the request for this review came from the board, it was fully supported by the company's risk management team. They worked closely with Broadleaf to understand our conclusions and recommendations and requested examples of best practice on which they could base their own solutions.

Broadleaf

4 Contact

If you would like further information about this topic please contact us. We will endeavour to reply promptly.

Dr Dale F Cooper
Cooper@Broadleaf.com.au

Pauline Bosnich
Bosnich@Broadleaf.com.au

Dr Stephen Grey
Grey@Broadleaf.com.au

Grant Purdy
Purdy@Broadleaf.com.au

Geoff Raymond
Raymond@Broadleaf.com.au

Phil Walker
Walker@Broadleaf.com.au

Mike Wood
Wood@Broadleaf.co.nz

For further information visit www.Broadleaf.com.au