

BROADLEAF CAPITAL INTERNATIONAL PTY LTD

ABN 24 054 021 117

23 Bettowind Road
Pymble
NSW 2073
Australia

www.Broadleaf.com.au

Tel: +61 2 9488 8477
Mobile: 0419 433 184
Fax: + 61 2 9488 9685
Cooper@Broadleaf.com.au

Specialists in Strategic, Enterprise and Project Risk Management

Risk Management Reporting and Governance

1 Background

This note gives practical advice on the nature of risk management reporting for governance purposes and contains a summary of what we regard as best practice. This is based on what we have observed in companies and organisations in Australia and other countries that are subject to similar governance regimes.

While governance reporting is a major output from a risk management process and, in particular Enterprise Risk Management, it should not be the primary or sole focus. Indeed, if the risk management framework is properly defined and implemented, reporting should be incidental to the application of the risk management process. Often this is facilitated through a risk management information system.

It is normal that organisations submit to their Board reports that show:

- The risk profile for the organisation;
- The changes in that risk profile since the last report;
- The performance of the risk management ‘system’ or framework.

Practically this means that most organisations require their divisions to prepare reports for submission to an Audit or Risk Management Committee of a Board twice a year. Some organisations just submit one summary report or reports that cover all divisions in the organisation.

2 Risk Profile Report

This normally is a high level risk register that contains strategic and consolidated risks from divisions. It is desirable to preface this with an Executive Summary that gives commentary and which explains:

- What are the most significant risks and why;
- How these are being controlled;
- Any particular control gaps and how these are proposed to be filled.

While it is normal to rank risks according to residual risk rating, often Directors like to see those risks with the greatest potential impact – as measured by Potential Exposure¹ under an

¹ Potential Exposure represents the plausible worst case consequence of an event. It is estimated by considering the consequences from an event if all existing controls are ineffective or missing. It can be defined as equal to

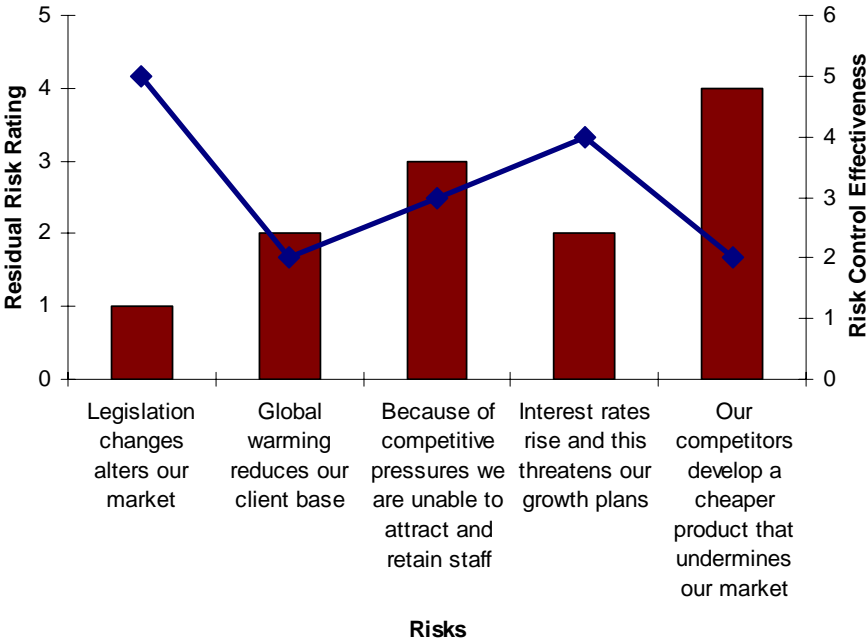
organisation-wide system – and to be assured that these in particular are being well controlled.

The risk register is best simplified from that recorded in the risk management information system and typically risks are grouped into categories preferably based according to cause. The risk register is likely to contain up to twenty or so risks described in terms of:

- Risk description;
- Causes;
- Nature and extent of potential consequences;
- Key controls;
- Risk control effectiveness²;
- Residual risk rating;
- Potential exposure;
- Key treatment tasks (if relevant).

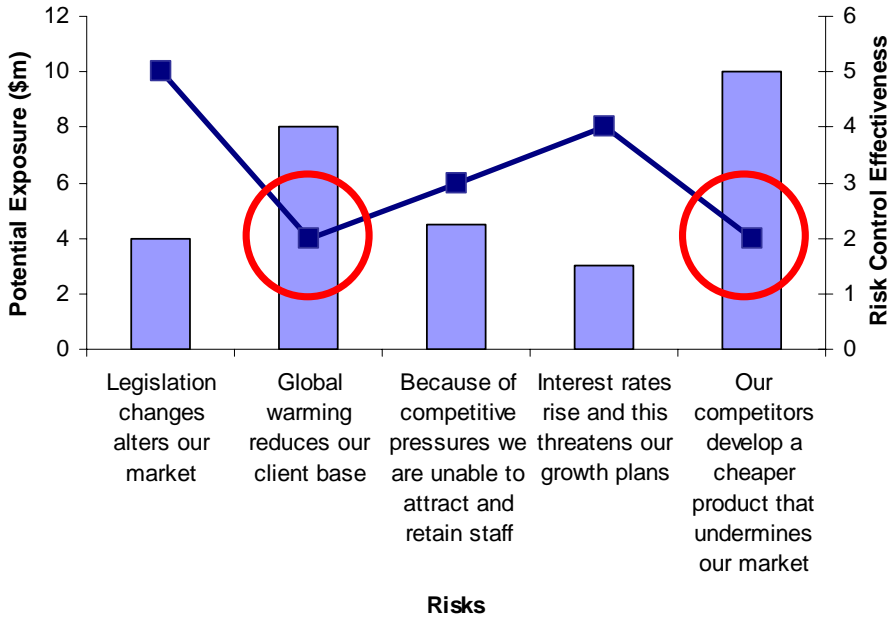
A graphical analysis can also be very informative. These include separate graphs where risks are plotted showing risk rating against risk control effectiveness, potential exposure against risk control effectiveness and risk rating against potential exposure. Examples are shown in Figures 1 and 2.

Figure 1: Example risk rating vs. risk control effectiveness graph



the EBITDA lost, plus the legal liability or compensation payments made plus any opportunity costs.
² Risk Control Effectiveness (RCE) is based on a relative assessment of the actual level of control that is currently present and effective compared with that reasonably achievable for that particular risk. RCE will therefore be an indicator of whether the organisation is doing all that it could or should to manage the risk issue.

Figure 2: Example potential exposure vs. risk control effectiveness graph



Most of this report and the graphical analysis can normally be produced ‘automatically’ by the organisation’s risk management information system.

3 Changes in Risks Report

The changes in risks report can be separate from or part of the risk profile report. The intention here is to show Directors how the risk profile has changed since the last report and to explain why. Often this is more useful and important than just the simple risk profile. The report explains:

- Those risks that have decreased in risk level or potential exposure, possibly because of control activity;
- Those risks that have increased in level or potential exposure;
- Those risks where there has been a significant change (either positive or negative) in risk control effectiveness.

There is also benefit in noting ‘emerging risks’ that are on the organisation’s watch list – often caused by external factors such as Government or market forces.

Again a graphical analysis can aid understanding. Most risk management information systems can produce reports based on ‘snapshots’ that allow this kind of comparative reporting. An example is shown in Table 1.

Table 1: Example Change in Risk report

Risk	Change in Risk Rating	Change in RCE	Change in PE (\$m)	Reason for Change
Legislation changes alters our market	↑	↔	↑	We expect new legislation after the current state elections
Global warming reduces our client base	↑	↑	↑	We have discovered that we are much more vulnerable to global warming than we expected. We have few valid controls in place
Because of competitive pressures we are unable to attract and retain staff	↔	↑	↔	A recent audit showed that our current staff retention strategies are deficient
Interest rates rise and this threatens our growth plans	↓	↔	↔	Although we are highly geared, the reserve bank is not expected to raise rates in the near future
Our competitors develop a cheaper product that undermines our market	↑	↔	↑	The market is getting bigger but we are maintaining our product development programme.

4 Risk Management Performance Report

The organisation will also need to produce reports that explain and describe the quality and maturity of risk management in its various departments and areas. This reporting on risk management performance to the Board will allow it to attest that the company's risk management and internal compliance and control systems are 'operating efficiently and effectively in all material respects' as required by the 2003 Australian Stock Exchange Corporate Governance Guidelines and similar requirement under other such governance codes.

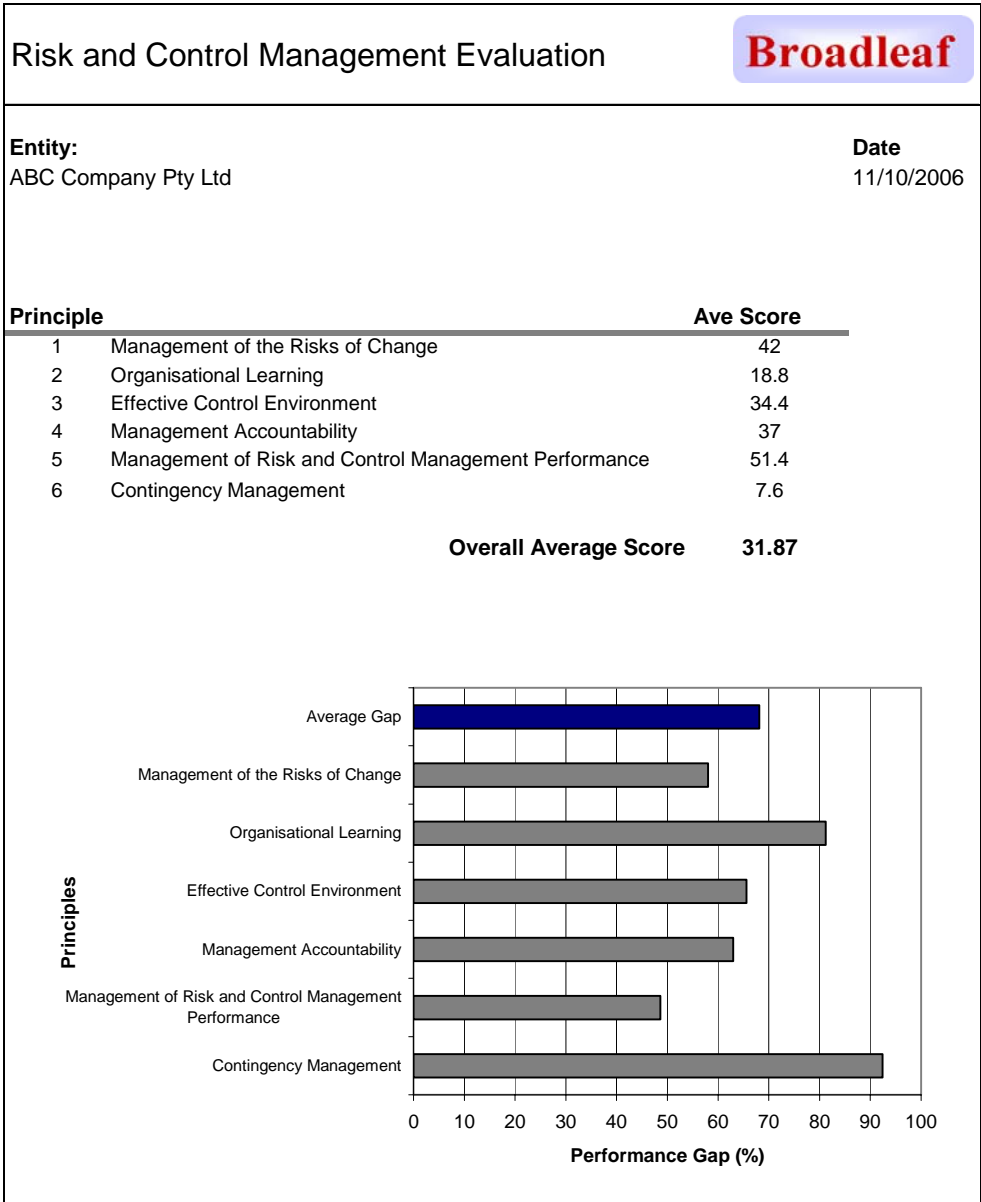
Normally these reports contain:

- The up-to-date risk management plan for the company, division or area;
- A description of the progress in implementing the risk management plan since the last report;
- An objective and structured assessment of the level of risk management maturity and the change since the last report;
- Performance against risk management performance indicators where these are used.

Any decline in performance or lack of progress should be noted and explained.

Again the risk management information system is normally used to produce these reports. An example from a risk management maturity evaluation is shown in Figure 3.

Figure 3: Example output from a risk management maturity evaluation



5 Broadleaf’s Services

Broadleaf is working with many large organisations in the commencement and continuation of risk management. We help organisations to achieve and sustain tailored approaches to risk management that suit them and which adapt as the organisation and its strategic objectives change.

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

- Risk management strategy planning;
- Gap and maturity analysis;
- Framework development;
- Policy, standard and guideline drafting;
- Risk management information system specification, procurement and deployment;
- Risk assessment facilitation;

- Risk based audit and assurance planning;
- Governance reporting and assurance;
- Risk management performance management;
- Risk management framework benchmarking and review;
- Development and delivery of general risk management training;
- Training and mentoring of risk management specialists in all aspects of risk management and its implementation.

6 Contacts

If you would like further information about risk management reporting and governance, please either contact one of the members of Broadleaf shown below or visit our web site at www.Broadleaf.com.au.

Grant Purdy
Purdy@Broadleaf.com.au

Dr Dale F Cooper
Cooper@Broadleaf.com.au

Dr Stephen Grey
Grey@Broadleaf.com.au

Geoff Raymond
Raymond@Broadleaf.com.au

Mike Wood
Wood@broadleaf.co.nz

Phil Walker
Walker@Broadleaf.com.au