



## Risk Management Policy Statement

Campbell Brothers Limited (CBL) is committed to establishing enterprise wide risk management systems and processes to ensure its strategic goals and corporate governance responsibilities are met. This policy recognises risk management is integral to good management practice and effective corporate governance and is necessary to ensure decisions are made with sufficient information about risks and opportunities.

**The objectives of the CBL Risk Management Policy and Framework are to:**

- Maximise the value from our assets, projects and other business opportunities
- Provide a consistent and systematic approach to identify, analyse, evaluate, treat, monitor and report on both material business risks and operational risks across CBL
- Provide a framework that encourages enterprise and innovation, and assists management to make decisions that are appropriate
- Ensure the risk profile is maintained to depict current risks in each area of its business operations
- Ensure activities are undertaken within approved risk tolerance levels and with sufficient independent oversight to protect the profitability, assets and reputation of CBL.

The CBL Risk Management Framework is based on AS/NZ ISO31000-2009 "Risk Management Principles and Guidelines" and meets or exceeds Principle 7 – Risk Management of the Australian Securities Exchange (ASX) Corporate Governance Council guidelines.

### **Application**

This policy applies to all Campbell Brothers Limited businesses.

### **Resources**

Campbell Brothers Limited will provide the necessary resources and support mechanisms to ensure its commitment toward risk management is achieved.

### **Implementation**

Each Campbell Brothers Limited business is responsible for implementing the requirements of this policy in consultation with their employees. The effective management of risk is vital to the continued growth and success of our Group.

**Greg Kilmister**  
Chief Executive Officer

**Date: 28 September, 2010**



# Risk Management Framework

**Introduction**

Campbell Brothers Limited (CBL) is committed to demonstrating a high standard of safety, quality and risk management. CBL views risk management as a key component of its corporate governance responsibilities and an essential process in achieving and maintaining a viable organisation. Subsequently, CBL believe that effective integrated management of risk is central to its continued growth and long-term success.

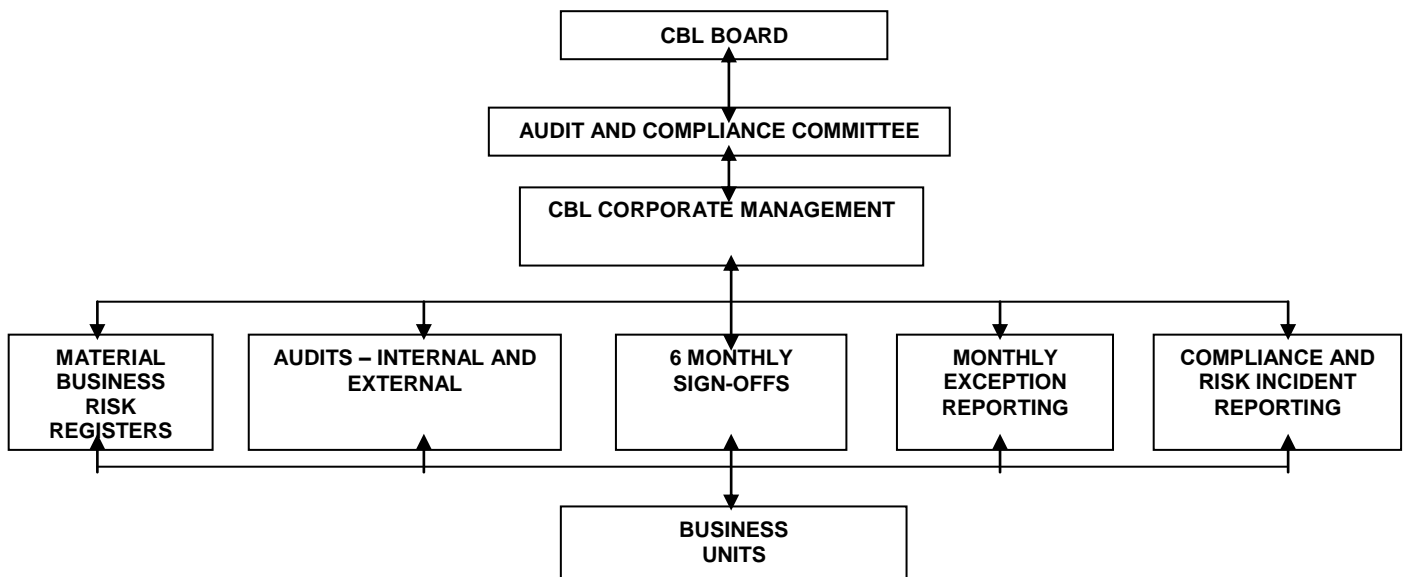
The objective of the risk management framework is to provide CBL businesses with guidance in how to apply consistent and comprehensive risk management systems. The framework provides information on how to identify, analyse, evaluate and treat risks as well as communication requirements to provide assurance that risks are being effectively managed.

The risk management process contained in this framework aligns with the Australian/New Zealand Standard for Risk Management AS/NZS ISO 31000-2009 “Risk management –Principles and guidelines”.

**Risk reporting**

The risk reporting structure set out in figure one below provides a simplified view of the communication of risk information from a business unit level to the CBL corporate level.

Figure 1 CBL - Risk Communication Structure



CBL will commit to the following reporting schedule to monitor and report on its risks:

Report	To Who	Schedule
CBL Material Business Risk Review - Update on the material business risk (MBR) registers and the controls in place to manage MBR's.	Audit and Compliance Committee	March Audit Committee Meeting
Compliance and Risk Reports - Summary of key operational compliance and risk issues that are reported from each business.	Board (via monthly Board Report)	Each Month
Compliance, Risk and Internal Audit Reports - Update report of key operational risks identified each quarter.	Audit and Compliance Committee	Quarterly
Key Risk Briefings/Reports - Specific management attend and report to the Audit Committee to provide details on key risks such as Health Safety and Environment, IT governance; Finance, Tax and Accounting; Human Resources; Insurable Risk; and Security.	Audit and Compliance Committee	Annually as scheduled by the Audit Committee Program
Reviews of Corporate Policies - Review of policies including Securities Trading, Code of Conduct, Continuous Disclosure.	Audit and Compliance Committee	Annually as scheduled by the Audit Committee Program
Six Monthly Sign-Offs - Report on performance of businesses against corporate policies, internal accounting controls, statutory risks and corporate governance procedures.	Audit and Compliance Committee	Each May and November Audit Committee Meeting

### **The Risk Management Process**

The risk management process has been adopted from AS/NZS ISO 31000:2009 "Risk Management Principles and Guidelines". CBL have interpreted the steps of the standard in the following way:

#### **Establish the Context**

Before formally assessing risks, each business division should ensure they detail their context in relation to their specific business including:

- Governance/management structure
- Services provided
- Physical environment (property and location details)
- Service dependencies (internal & external)
- Competition

#### **Risk Identification**

The organisation has processes in place to identify actual or potential risks. Risks can be identified in a multitude of ways through day-to-day activities, proactively through formal risk management workshops, or reactively as a result of certain events occurring.

The following risk identification processes are relied upon within CBL to ensure risks are reported:

Risk Identification Group	Examples
<b>Structured Workshops</b>	<ul style="list-style-type: none"> <li>• Business strategic planning reviews</li> <li>• Material Business Risk workshops incorporating techniques such as ‘strengths, weaknesses, opportunities, threats’ (SWOT) analysis; brainstorming; analysis of systems or scenarios</li> </ul>
<b>Normal Organisation Activities</b>	<ul style="list-style-type: none"> <li>• Monthly Team meetings</li> <li>• Business and Operations Managers forums</li> <li>• Capital expenditure risk assessments</li> <li>• Routine data collection and business data analysis</li> </ul>
<b>Assessment against Standards</b>	<ul style="list-style-type: none"> <li>• Financial reviews and external audits</li> <li>• Six monthly compliance process, incorporating compliance against company policy, key risk controls, and legal compliance</li> <li>• Internal audit and peer reviews</li> <li>• Third Party Accreditation reviews (ISO, NATA)</li> <li>• Corporate Compliance and Risk Audits</li> <li>• Health Safety and Environment (HSE) and Injury Management (IM) inspections/audits</li> </ul>
<b>Incident or Event Logging</b>	<ul style="list-style-type: none"> <li>• Internal incident or complaint reporting via Compliance and Risk portal incorporating health, safety, environment and property incidents.</li> <li>• Faircall Whistleblower Hotline</li> </ul>
<b>Exception Reporting</b>	<ul style="list-style-type: none"> <li>• Monthly exception reporting incorporating Legal, Information Technology, Employment Practices, Insurance, Trade Practices, Environmental, HSE, Tax and Corporations Law risks.</li> </ul>

## Risk Assessment

The risk assessment step involves the calculation of the risk based on the consequence of the event and likelihood of the identified event occurring. For the majority of risks that take the form of incidents, events, or non-compliances, risk assessment is built into the reporting requirements i.e. CBL standard incident report forms require investigation and corrective actions. A risk assessment matrix has been developed to be used across CBL for Material Business Risks and for Operational Risks. Consequences are grouped under the areas of Financial, Legal, Reputation, HSE, and Operational. A five by five consequence and likelihood risk matrix is used to apply a rating to each identified risk.

To ensure a consistent approach is taken for the assessment of material business risks CBL has implemented a standard register to record all identified material business risks. Risk management workshops are held by the Corporate Compliance and Risk Group with senior management teams from each CBL Division to identify and record material business risks. The outcomes of the risk workshops are recorded on the CBL MBR Risk Register.

## Evaluate Risks

The risk rating calculated from the Risk Management Matrix establishes the priority of the identified risk. CBL have established guidelines for required actions associated with the level of risk and the communication of the risk within the organisation.

## Risk Treatment

All Extreme, High and Medium risks identified require controls to be implemented to treat the risk to an acceptable level. The CBL MBR Risk Register includes identified responsibilities and timeframes for each risk treatment, and how the risk will be further analysed and evaluated. For

operational risks, the CBL Compliance and Risk Portal will record a register (Central Compliance and Risk Log) of identified risks and allocate corrective actions and responsibilities to each risk.

### **Monitor & Review**

As a minimum the CBL MBR Risk Register will be reviewed every 12 months. The monitoring and review process will examine how robust the selected risk controls and management strategies are, as well as monitor the effectiveness of all steps in the risk management process.

For operational risks, the frequency of review of the Central Compliance and Risk Log will be in accordance with the allocated corrective actions for each item.

### **Communication and Consultation**

Communication to stakeholders, both internally and externally, will not only assist in establishing a positive culture of risk management but ensure all potential and actual risks are identified and reported as part of the risk management process. Businesses are required to escalate significant risks through to their executive management and the CBL corporate office in line with the risk matrix and reporting processes contained in this framework.

### **Roles and Responsibilities**

The Board is responsible for reviewing and approving the overall risk management strategy including the risk appetite of the Group. The Audit and Compliance Committee assists the Board to monitor the Group's obligations in relation to financial reporting, internal control and audit, and compliance and risk management systems. Directors also monitor risks and controls through the Remuneration Committee, Nomination Committee, and other Sub-Committees of the Board that may be formed from time to time.

The CEO and executive management team are responsible for implementing the risk management strategy and for developing policies, controls and processes to identify and manage risk across CBL. The Board receives regular reports from management about the Groups financial position and operational results for each controlled entity. The CEO and CFO provide certification to the Board each reporting period that:

- The financial statements are founded on a sound system of risk management and internal compliance and control which implements the policies adopted by the Board, and
- The company's risk management and internal compliance and control system is operating efficiently and effectively in all material respects.

A number of key management controls are in place to ensure risk management is integrated into the business operations in a consistent manner in line with Board expectations. These include:

- Code of Conduct
- Authority Limit Guidelines
- Capital Expenditure Risk Assessment Guidelines
- HSE Minimum Standards
- Business Continuity and Disaster Recovery Guidelines
- Whistleblower Program

The Group Compliance and Risk Manager is independent from the business units and reports to the Chief Executive Officer. The role is responsible for assisting each CBL business meets their obligations under the risk management policy and this framework, and to report to the Audit and Compliance Committee on the effectiveness of the controls in place for compliance and risk.

The Compliance and Risk Group provides the following support:

- Infrastructure to facilitate compliance and risk reporting (the Compliance and Risk Portal)
- Specialist advice to businesses in implementing regulatory policies and establishing compliance programs
- Analytical tools and advice for areas of operational risk (including HSE)
- Management of Global insurances to adequately protect key business assets.

## Appendix 1 Risk management tools

**Table 1 Consequence matrix**

Consequence	Financial	Legal	Reputation	HSE	Operational
<b>Insignificant</b>	Low level loss/ cost to business / Division/ CBL <1% budget/ed revenue /EBIT	Event unlikely to attract regulatory response or claim. Notification of authorities unlikely to result in action.	Isolated complaint / event. No media inquiry	Employee/ contractor or environmental incident with limited harm, i.e. first aid	No material damage to property or disruption to continuity of services. Negligible affect on project.
<b>Minor</b>	Minor level loss / cost to business / Division/ CBL 1%- 5% budgeted revenue / EBIT	A minor breach, which may incur a non compliance or improvement notice. Notification necessary and visit likely.	Number of complaints and /or clients affected. Receiving local adverse publicity	Medical treatment required. Localised environmental clean up or remediation.	Minor damage to property. Services/ business disrupted for less than 12 hours. Project impact minor
<b>Moderate</b>	Moderate level loss / cost to business / Division/ CBL 5%- 10% budgeted/ revenue	A breach of regulations, or negligence. Notices/ claim issued with the likelihood of limited prosecution or civil action.	Multiple wide spread complaints and /or clients affected. Adverse media interest / exposure is likely to be limited in duration	Serious compensable injury, Extended time off >4 days. Moderate local environmental impact, contained to site but clean up required	Damage or disruption to services / or a business for 24 hours. E.g. minor fire, disruption to utilities, IT system down. Project delayed or compromised impacting on objectives
<b>Major</b>	Major level loss / cost to business / Division/ CBL 10%- 15% budgeted/ revenue. Corporate support needed	A major breach of regulations, or negligent act. Investigation by authorities Likelihood of prosecution or civil action.	Complaints across country. Significant or sustained adverse publicity effecting client confidence.	Permanent impairment due to injury. Off site environmental impact. Requiring significant cleanup and on going remediation	Major damage or closure of a business or service for more than 30 days. Inability to achieve project objectives.
<b>Catastrophic</b>	Extreme level loss/ cost to business / Division/ CBL >15% budget/ revenue	A serious wilful breach of regulations, or negligence. Likelihood of suspension of business. Directors / officers likely to be prosecuted or named in civil action.	Sustained nation-wide media exposure with significant and lasting public/ client outrage / dissatisfaction. ASX notification necessary.	Fatality or numerous serious injuries. Serious environmental impact, off site impact. Extensive cleanup and on -going remediation necessary	Major damage or closure of a hub lab or major site. Resulting in inability to service customers. Project failure with broader impact to business

**Table 2 Likelihood guide**

Likelihood classification	Description
5 Frequent	Expected to occur again either immediately or within a short period of time (likely to occur most weeks or months)
4 Likely	Will probably occur in most circumstances (several times a year)
Possible	Possibly will occur, might occur at sometime (may happen every one to two years)
2 Unlikely	Possibly will recur, could occur at sometime (may happen every two to five years)
1 Rare	Unlikely to recur, may occur only in exceptional circumstances (may happen every five to thirty years)

**Appendix 1 Cont**  
**Table 3 Risk matrix**

Likelihood ↑	Frequent 5	5 Medium	10 High	15 High	20 Extreme	25 Extreme
	Likely 4	4 Low	8 Medium	12 High	16 Extreme	20 Extreme
	Possible 3	3 Low	6 Medium	9 Medium	12 High	15 High
	Unlikely 2	3 Low	4 Low	6 Medium	8 Medium	10 High
	Rare 1	1 Low	2 Low	3 Low	4 Low	5 Medium
		Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
	Consequence →					

**Table 4 Risk actions**

Risk Score	Risk Rating	Actions	Reporting Requirements
16 - 25	Extreme	<p>Immediate Action is required by Senior Executive.</p> <p>Detailed investigation / analysis and response to be undertaken.</p> <p>CEO to be notified, preparation of media briefing considered if required.</p>	<ul style="list-style-type: none"> <li>○ The incident / risk must be reported to the Executive GM, and CBL Compliance &amp; Risk Manager within 24 hours.</li> <li>○ Business to provide CBL Compliance &amp; Risk Manager with a Risk report within 48 hours.</li> <li>○ Summary of incident / risks and controls / outcomes reported to the Board and Audit and Compliance Committee.</li> <li>○ A detailed Risk Investigation to be completed for identified risks</li> </ul>
10 - 15	High	<p>Senior Management attention needed.</p> <p>Investigation / analysis and response to be undertaken at the discretion of Business senior management and / or Divisional GM.</p> <p>CBL corporate Compliance and Risk Unit to be notified.</p>	<ul style="list-style-type: none"> <li>○ The incident / risk must be reported to the Business Executive, Divisional GM and Compliance &amp; Risk Manager within 48 hours.</li> <li>○ Business management to consider need for regulatory reporting requirements; i.e. Environmental authorities, Workcover, ASX, or other regulatory body if required.</li> <li>○ Business to provide CBL Compliance &amp; Risk Manager with a Risk report within 5 days.</li> <li>○ Summary of incident / risks and controls / outcomes reported to the Board and Audit and Compliance Committee.</li> <li>○ A detailed Risk Investigation Form to be completed for identified risks</li> </ul>
5 - 9	Medium	<p>Senior Management responsibility and actions must be specified.</p> <p>Data should be aggregated and provide opportunity for business improvement, addressed at Business / local level.</p>	<ul style="list-style-type: none"> <li>○ The Business Manager to notify GM if required after consideration of the circumstances of the incident / risk.</li> <li>○ Business management to consider need for regulatory reporting requirements; i.e. Environmental authorities, Workcover, ASX, or other regulatory body if required.</li> <li>○ Aggregated data reported and analysed via CBL Compliance portal and reported to Divisional GM's and Audit and Compliance Committee.</li> </ul>
1 - 4	Low	<p>Managed by routine procedures, aggregate data, then undertake business improvement project.</p>	<ul style="list-style-type: none"> <li>○ Business to enter information on Compliance Portal – incident report/ compliance reporting / exception reports / monthly sign off, etc.</li> <li>○ An incident that rates as Low Risk should only be reported to Compliance &amp; Risk Group if it is likely to attract external attention (media) or requires notification under existing legislative reporting requirements.</li> <li>○ Data collected in Compliance portal and information extracted as needed by businesses or CBL corporate.</li> </ul>

## Appendix 2

### Campbell Brothers Limited Material Business Risk Register

RISK NO.	Business objective / function	RISK (A brief description of the risk under investigation, include Event, Causes, Impacts)	CAUSATION (Identify the key contributing factors / drivers associated with the risk)	CONSEQUENCE (Risk category = Finance, Operations, HSE, Legal, Reputation)	CONSEQUENCE LEVEL (1-5)	LIKELIHOOD LEVEL (1-5)	EXISTING CONTROLS (What is in place to prevent, manage risk?)	CURRENT RISK SCORE (with controls)	CONTROL EFFECTIVENESS SCORE / RATING	RISK OWNER (Job Title)	RISK STRATEGY (Avoid, Reduce, Transfer, Do nothing)	RISK TREATMENT	TREATMENT DUE DATE (MM/DD/YYYY)