Risk Management Policy

Approved by the Board	**26 August 2019**
Previously Approved	September 2017
Next Review Date	August 2020

Table of Contents

1. Introduction

1.1 Purpose of this Policy

Readcloud Limited (**RCL**) and any controlled companies together are referred to as the **Group** in this Policy.

This Policy aims to provide a framework and process for managing risk within the Group and its activities.

This Policy is intended to:

a) facilitate a formal process to identify and analyse the key financial, strategic, operational and compliance risks relevant to RCL and it business activities;

b) allows the necessary controls and policies to be implemented to deliver appropriate governance and best practice; and

c) provide assurance to management that the process is functioning effectively.

A Risk Management Policy is intended to be an assurance that a company is actively integrating and embedding risk management in all activities undertaken. This assurance can be achieved by:

a) establishing a Risk Management Framework which provides an operational and administrative structure;

b) giving guidance to personnel on acceptable levels of risks;

c) allocating resources to identified significant risk areas;

d) reinforcing the importance of effective risk management with personnel in their everyday activities; and

e) monitoring and reviewing processes and arrangements on an on-going basis.

1.2 Application of this Policy

This Policy applies to the Group and its representatives (directors, employees).

1.3 Review and amendment of Policy

The Risk Management Policy and the risk management framework will be reviewed on an annual basis. The scope of the review will include whether the implementation of risk management processes are in accordance with this Policy, the consistency of risk management practices and opportunities to improve risk management within the group.

2. Background

Organisations face 'internal and external factors and influences that make it uncertain whether, when and the extent to which they will achieve or exceed their objectives. The

effect this uncertainty has on an organisation's objectives is 'risk'. All activities of an organisation involve risk.'[1]

In AS/NZS ISO 31000:2009 Risk Management – Principles and guidelines, 'Risk' is defined as the chance of something happening that will have an impact on the objectives. Risk may have a positive or negative impact.

A risk is often characterised in terms of an event or circumstance and the consequences that may flow from it. Risk is often measured in terms of a combination of the consequences of an event and the associated likelihood.

'Every business takes risks to operate and grow, and needs to managed those risks to do so. Risk management is not about eliminating risk. It is about controlling risks to increase the likelihood of meeting business objectives.'[2]

Risk management is the process of systematically identifying, analysing, assessing, treating, monitoring and communicating risks associated with business activities in a way that will avoid or minimise losses and maximise opportunities.

This Risk Management Policy is based on the approach outlined in AS/NZS ISO 31000:2009 Risk Management Principles and Guidelines. It sets out the processes, responsibilities and accountability for risk management.

The Board acknowledges that a structured approach to risk management generally delivers numerous benefits. These include increased likelihood of achieving objectives, more effective decision-making, improved operational effectiveness and efficiency, efficient allocation and use of resources, improved loss prevention and incident management, improved governance, enhanced health, safety and organisational morale and better accountability.

3. Responsibilities

3.1 The Board

The Board of Directors ('the Board') believe the management of risk is a continual process and an integral part of good business management and corporate governance.

Risk management is considered by the Board to mean the identification and management of those risks which could harm the Group. Such risks may be classified as strategic, operational, financial, legal, contractual and technological.

In terms of risk management the Board is responsible for:

a) ensuring that the Group has effective systems in place to identify, assess, monitor and manage risks to the Group;

b) informing stakeholders of any material change in the risk profile of the Group (in accordance with the RCL's disclosure obligations); and

c) ensuring internal controls and arrangements are adequate for monitoring compliance with laws and regulations, as applicable to the Group.

[1] AS/NZS ISO 31000:2009

[2] CP 204: Risk management systems for responsible entities

To assist them, the Board has established:

a) an Audit and Risk Committee, structured in consideration of the ASX Corporate Governance Council's Guidelines;

b) reporting mechanisms from management responsible for the financial and administrative operations of the Group (as part of the Risk Management Framework).

3.2 Board Audit and Risk Committee

The Audit and Risk Committee ('ARC') plays a key role in assisting the Board with responsibilities relating to accounting, internal control systems, reporting practices and risk management and ensuring the independence of the external auditors.

The Audit and Risk Committee operates in accordance with a Charter, which outlines its structures and responsibilities.

3.3 Risk Manager

The Risk Manager is responsible for the co-ordination and continued improvement of the Risk Framework. Due to the Company's relatively small size, the CIO will also act as the Risk Manager.

Risk profiles are reviewed annually by the Risk Manager, in conjunction with management.

The responsibility for the risk management arrangements within RCL is summarised in the following table:

Risks/Processes	**Responsibility**
Overall risk management framework and policy	Board
Management of strategic risks	Board
Management of operational risks	CEO Manager of the functional areas
Effective operation of internal control structures/ risk treatments	CEO Risk Manager
Review and monitoring of effectiveness of risk management	AR Committee Risk Manager
Maintenance of Risk Profiles	Manager of the functional areas Risk Manager

4. Risk Management Framework

The Group has implemented a Risk Management Framework based on the standard AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines to ensure risks are identified,

assessed and managed with the purpose of minimising loss to business and maximising opportunities. [3]

In developing the Framework, management have taken into consideration the Group's internal and external context, factors such as its objectives and strategies, the nature of its business, the social, economic, regulatory, technological and competitive environment in which it operates and the stakeholders involved.

The Framework comprises:

a) a systematic process for the identification, assessment, treatment and monitoring of risks;

b) communication and consultation to ensure management are involved in the development and maintenance of Risk Profiles;

c) integrated risk management in business planning and day to day operational management; and

d) training to improve staff awareness of risks and management techniques.

Risk Profiles are maintained for the Group, which describes the risks facing the business activities within the Group and the key controls surrounding those risks.

The profiles are reviewed at least annually and presented to the Audit and Risk Committee.

The Group has the following in place to ensure a strong control environment:

a) clearly defined management responsibilities and organisational structure;

b) delegated limits of authority;

c) policies and procedures that are available to and understood by employees;

d) regular internal review, and

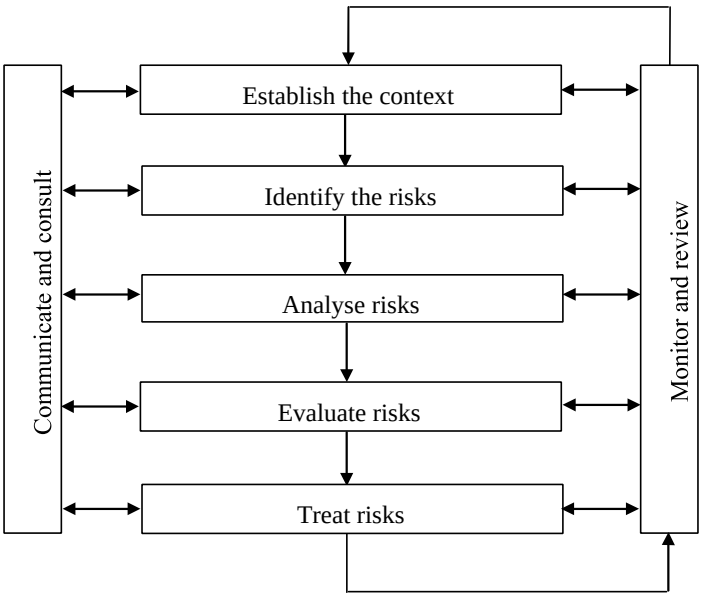
e) a Business Recovery Plan, aimed at preventing significant disruption to the business.

The Framework is intended to assist an organisation to integrate risk management into its overall management system.

5. The Risk Management Process

The risk management process can be illustrated as follows:

[3] Section 4 of AS/NZS ISO 31000:2009



Communication and consultation should address the risks, the causes, the consequences (if known) and the measures taken to treat them. Effective internal and external communication and consultation should occur, as appropriate, to ensure those accountable for implementing the risk management process and stakeholders are fully informed.

Communication and consultation should encourage open, relevant and accurate exchanges of information.

The risk management process comprises the following activities:

5.1 Establish the context

By establishing context the organisation defines its objectives, outlines the internal and external parameters to be taken into account in managing risk and sets the scope and risk criteria for the remaining process.

Establishing the internal and external context

The Group's risk management process takes place within the context of its capabilities, goals and objectives. It should be aligned with the culture, structure and objectives of the organisation.

The external context ie the strategic context is the relationship between the Group and its environment and involves the identification of the Groups' strengths, weaknesses, opportunities and threats.

This involves consideration of the social, economic, regulatory, financial, technological, competitive, geographic environment in which it operates and the stakeholders involved.

These parameters are similar to those considered in the design of the Risk Management Framework; however they need to be considered in more detail as part of this process.

Establishing the context of the risk management process

The scope, objectives and parameters of activities within organisation where the risk management process is being applied should be established. The management of risk should occur with consideration of the resources needed to carry out risk management.

Defining risk criteria

An organisation should define criteria used to evaluate the significance of risk. Some criteria will be imposed by legal and regulatory requirements while some will reflect the organisation's values, objectives and resources.

5.2 Identify Risks

Risks at both the company and functional level are identified.

The primary mechanism for risk identification is reviews of:

a) business processes,

b) regulatory environment,

c) technology arrangements,

d) company financials, and

e) operational risks.

The CEO and Manager of the functional area and compliance specialists generally work through the activities and processes conducted within a functional area to identify the risks within that area.

Generic examples of risks for RCL's business are:

a) Political circumstances,

b) Technology and technical issues,

c) Economic – interest rates, share market,

d) Human – error, sabotage,

e) Financial – fraud, misappropriation of funds,

f) Professional liability – wrong advice or negligence, and

g) Contractual risks.

5.3 Analysis of Risks

Risks may be analysed using a variety of methods, including:

a) Qualitative analysis – using words or a descriptive scale to describe the magnitude of the potential consequences and the likelihood that those consequences will occur;

b) Semi-qualitative analysis – in this type of analysis the qualitative scales are given values – which allows a more detailed prioritisation to occur;

c) Quantitative analysis – using numerical values for both potential consequences and the likelihood that those consequences using data from a variety of sources.

Risk Analysis Matrix (Risk Rating)

The Consequences and Likelihood ratings are detailed in the following tables. The result of combining estimates of consequences and likelihood produces a Risk Rating Matrix.

Qualitative measure of Consequence

Descriptor	Rating	Financial Value	Legal/ Reputation
Insignificant	1	Low financial loss – under $5k	Insignificant impact, no disruption to capability, no impact on reputation, no impact on clients
Minor	2	Minor financial loss – $10k - $50k	Minor non-compliance (possibly of a technical nature) Some attention
Moderate	3	Financial loss – $50k - $ 250k	Non-compliance with regulation, perhaps with fine/ enforcement Adverse attention
Major	4	Financial loss – $250k - $1 m	Serious non-compliance with regulation, with fine/ enforcement Serious adverse public attention
Catastrophic	5	Financial loss – over $1m	Regulator action, serious (or threatened) litigation (including class action

Qualitative measure of Likelihood

Descriptor	Rating	Description	Expected frequency
Almost certain	5	Has occurred many times before and is expected to occur in most circumstances	Greater than once 6 months
Likely	4	Will probably occur in most circumstances 50-75% chance of occurring	Between once every 6 months and once a year
Possible	3	Might occur at some time 20- 50% chance of occurring	Between once a year and once every 5 years
Unlikely	2	Could occur at some time 5-20% chance of occurring	More than 5 years but less than 10 years
Remote	1	Less than 5% chance of occurring, only in exceptional circumstances	Less than once every 10 years

Risk Rating Matrix

Medium 5	High 10	High 15	Very High 20	Very High 25
Low 4	Medium 8	High 12	Very High 16	Very High 20
Low 3	Medium 6	Medium 9	High 12	High 15
Low 2	Low 4	Medium 6	Medium 8	High 10
Low 1	Low 2	Low 3	Medium 4	High 5

5.4 Evaluation of Risks

Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. The outcome of this process is a prioritised list of risks for further action.

Risk evaluation can lead to the decision to:

a) treat the risk by maintaining the existing controls,

b) undertake further analysis,

c) introduce further controls.

5.5 Treating Risks

This involves identifying a range of options for treating risk, assessing those options, preparing a plan to treat the risk and implementing it.

The options for treating risk include:

a) Avoiding the risk – (where this is possible) by deciding not to proceed with the activity because it could generate an unacceptable level of risk;

b) Reducing the likelihood of the occurrence – through (for example) contract conditions, preventative maintenance, technological development, supervision, structured training, audit and compliance programmes;

c) Reducing the consequences – by using (for example) contingency planning, disaster recovery plans, separation or relocation of an activity and resources, public relations, ex-gratia payments;

d) Transferring the risk – through contracts, insurance arrangements; and

e) Retaining the risk – some risk is inevitable (ie the residual or inherent risk).

In assessing the risk treatment options, consideration is given to cost versus benefit of any action to ensure the “pay-off” to the business is acceptable.

5.6 Recording, monitoring and reviewing

"Both monitoring and review should be planned as part of the risk management process and involve regular checking and surveillance. It can be periodic or ad-hoc.

Responsibilities for monitoring and review should be clearly defined"[4]

The Group has established Risk Profiles for its business activities, based on function. Refer to Appendix 2.

The Risk Profiles contain details of key processes, the associated risks, a risk assessment (Consequences and Likelihood) the controls that have been implemented and residual risk (post the risk control).

The Risk Profiles are maintained by the Risk Manager. The Profiles are reviewed by the Risk Manager, in conjunction with the Manager and others from within the functional area, annually and also when:

a) a new activity or process is introduced;

b) an existing activity or process changes.

The Board reviews the Risk Profiles at least annually.

6. Risk Awareness and Training

The Board has responsibility for ensuring that management and employees understand the importance of risk management within the business. Risk management is incorporated in the training programs for management and employees.

[4] Section 5.6 of AS/NZS ISO 31000:2009

Appendix 1

ASIC provided the following guidance to assist with designing and testing measures.

Your risk management systems	
Risk management framework	• Have you documented your risk management systems? • Do your documented measures show who is responsible for risk management? • Has your governing body signed off on your risk management measures and made a commitment to ongoing risk management? • Have you appointed senior managers to oversee risk management measures? • Are there clear risk management reporting lines? Do your staff understand what they are required to report on, and when? • Do you annually review your risk management measures to ensure they are effective? Does this include external review? • Do you have a business continuity plan?
Implementing risk management	• How do you ensure that staff understand and comply with risk management measures? • Are risk management staff adequately trained and qualified in risk management responsibilities?
Identifying risks	• How do you identify risks to your business? • How do you identify risks to consumers and market integrity? • Have you considered all your obligations under the Corporations Act (including the regulations and licence conditions) and identified the risks of non-compliance with them? • How do you ensure you identify new risks as they arise (e.g. because of new products or technology)? • Do you document the risks you identify?
Evaluating risks	• How do you establish the probability of a risk event occurring and the impact of the problem if the risk occurs? • How do you combine the probability and impact factors to determine the overall risk? • How do you prioritise the risks and establish which ones need to be addressed? • Do you document the risks you evaluate and how you arrive at your evaluation?
Addressing risks	• How do you address those risks with appropriate measures and controls? • Do you document your measures and controls for addressing risk and the reasons behind them?

Appendix 2

Risk Profiles

The risk categories are intended to help RCL to organise its risk identification and assessment activities. This will include all sources of risk from the perspective of all stakeholders – internal and external.

Company Assets

This collection of risks addresses the Company's ability to protect its assets. This includes corporate reputation, physical access to premises, physical assets (such as computers, blank cheques) as well as data representations of assets (books and records, electronic funds transfer applications).

People

This collection of risks relates to RCL's ability to attract, retain and adequately manage/monitor its employees, and also manage risks relating to employee conduct.

Continuity

This collection of risks relate to RCL's ability to continue its operations in the event of a loss or failing. These can include business continuity planning, disaster recovery planning, key personnel and external/internal service level agreements for standard operational service and delivery.

Financial

This collection of risks addresses RCL's exposure to loss if transactions are not processed in accordance with service levels and acceptable standards.

This also includes liquidity risks that result from any inability to meet obligations as they come due without incurring unacceptable costs or losses.

Information Technology

This collection of risks relate to RCL's information technology capabilities and can included web access (both internal/external), reliability (i.e. service levels), data integrity, reliance on spreadsheets/databases and access to local area network (i.e. email, intranet, files).

Legal/Commercial and Compliance

This collection of risks relate to conformity with internal policies and procedures, as well as external commercial transactions and applicable laws and regulations. Management should ensure that appropriate personnel are versed in the pertinent procedures, laws and regulatory principles and requirements.

Market

This collection of risks relate to non-financial market risks and can include changes in financial market conditions (domestic and international equity market movements, economic changes), regulation, competitors, etc.

Resellers

This collection of risks is in recognition of the Reseller's contribution to the revenue and reputation of RCL.

External Service Providers

This collection of risks relate to the provision of services by external parties to RCL.

Product

This collection of risks relate to demand for new products and services, representations and marketing materials, and competitors.

Group Company & ASX Listing

These various risks relate to, and recognise, the complexities and difficulties, that arise following the consolidation of various entities into one operating business.