

**Section 11
Risk Management
Part A**



RISK MANAGEMENT MANUAL

Version 1.1 (July 2003)

Risk Management Manual

Document Control Form

Distribution: List of the people who will receive the document, and their required action (ie. signoff, review, for information only). Include the section(s) to be reviewed or signed off for all people with review / signoff responsibility.

Name	Title	Action (ie Sign off, Review, Information)	Section(s) to be reviewed
Craig Dunstan	Chief Executive Officer	Sign off	Entire Document
Chris Nunn	Head of Operations	Review	Entire document
Chris Calvert	Head of Property	Review	Entire document

Version History:

Date	Version	Name	Description
15/05/02	1.0	Craig Dunstan	Document created
21/07/03	1.1	Chris Nunn	On establishment of business

Approval:

Approval of the document indicates that the signatory has read the document and understands and agrees with the content of the document.

Craig Dunstan Managing Director MacarthurCook Investment Managers Limited	Signature: Date:/...../.....
---	---

CONTENTS

1.	INTRODUCTION	4
2.	RISK MANAGEMENT GUIDELINES	4
3.	RISK ASSESSMENT PROCESS.....	6
5.	COMPLIANCE & CORPORATE GOVERNANCE	6
6.	FINANCIAL RISK.....	8
7.	OPERATIONS RISK MANAGEMENT POLICY	8
8.	TRANSACTION AND TECHNOLOGY RISK MANAGEMENT POLICY.....	12
9.	HUMAN RESOURCES MANAGEMENT	14
10.	MACARTHURCOOK FUNDS	14
11.	SERVICE PROVIDERS.....	15
12.	PRIVACY ACT	15
13.	LICENCES AND REGISTRATIONS	15
14.	OTHER STATUTORY RETURNS.....	16
15.	FINANCIAL CONTROLS	16
16.	PHYSICAL ENVIRONMENT.....	16

1. INTRODUCTION

The purpose of this paper is to identify all areas of compliance responsibility and potential risk, and to report against nominated requirements and benchmarks.

All exceptions are to be noted.

2. RISK MANAGEMENT GUIDELINES

2.1 Risk

Risk can be defined as the expectation of something occurring that will have an impact on the company's objectives. It is the possibility of:

- Something adverse happening (risk of loss)
- Something uncertain happening (risk of volatility)
- Something positive not happening (risk of lost opportunity)

Risk can be categorised into:

- Market risk – non-diversifiable risk.
- Basis risk – relative pricing of securities
- Liquidity risk – the ability to liquidate a security with minimum delay.
- Counter party risk, (Credit Risk including Pre-Settlement and Settlement Risk)
- risk that a party to a contract will not perform to the terms of the contract.
- Business Risk - risk that the business model is unsustainable.
- Investment Risk - risk that investments in underlying assets are unsound, arising from poor investment processes or poor execution of those processes.
- Operations Risk - deficiencies in internal procedures and controls to leading to financial loss.
- Legal Risk – that contracts are not legally enforceable or documented incorrectly.
- Fiduciary Risk – risk that poor compliance and/or monitoring procedures will result in litigation from clients, investors and/or investee companies.
- Human Resources risk – failure to provide adequate or insufficiently trained specialists to undertake the required tasks and/or failure to appropriately segregate duties amongst staff and/or failure to assign appropriate accountabilities.

Derivatives can be used to mitigate market, basis and/or liquidity risk. A culture of process management, compliance and corporate governance should assist in mitigating the prospect of business, investment, operations, fiduciary and human resource risk.

2.2 Risk Management

Risk management is the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects. It is a tool that should assist in systematically identifying, measuring and controlling risk.

2.3 Allocation of Responsibilities

The Board of MacarthurCook retains the following decisions:

- Investment in property assets and approval of mortgages with a loan advance exceeding \$1 million.
- Approval of business plans and budgets.
- Creation of Constitutions and appointment of MacarthurCook as Responsible Entity of funds.
- All other significant policy decisions which affect the MacarthurCook business

The Board is also to be made aware of all material risks to the business, as reflected in the annual risk assessment matrix review (refer Section 3); receiving advices on all exceptions (including mandate breaches) and actions taken by way of a quarterly report. The Board will also be provided with a semi annual précis of the MacarthurCook Executive Self Assessment Questionnaire as enunciated in the MacarthurCook Compliance Plan.

The MacarthurCook Board has delegated authority to the Chief Executive, the authority to establish risk tolerances, fund objectives and investment criteria for excluded offer funds promoted by MacarthurCook. No such delegation exists for registered schemes.

MacarthurCook performs systematic checks on portfolios to ensure that they conform to Constitutions and investment management mandate requirements. Each portfolio manager is required to provide the Compliance Officer with a quarterly Compliance Report relating to funds managed by them.

With respect to all other facets of the business, clearly defined responsibilities and accountabilities have been established. Responsibilities have also been assigned based on MacarthurCook's key performance indicators to ensure that as far as possible the corporations' business objectives can be attained.

The Senior Executive Team will undertake an assessment of the risk matrix (enunciated in Section 3) of the business to be provided to the Board.

3. RISK ASSESSMENT PROCESS

The Risk Assessment Matrix is to be completed on an annual basis by all senior managers and forwarded to the MacarthurCook Board for review. The following risks will be specifically reviewed in this matrix.

- Compliance Risk
- Operations Risk
- Transaction and Technology Risk
- Human Resources Risk
- Investment Risk
- Fiduciary Risk
- Business Continuity Risk

Six months after becoming a Responsible Entity (i.e. approximately November 2003) a detailed risk assessment will be completed.

Once the business has been established the risks as identified above and addressed in this Manual will be fully reviewed and this Manual updated as necessary.

The priority for review will be:

- Compliance Risk
- Human Resources Risk
- Investment Risk

5. COMPLIANCE & CORPORATE GOVERNANCE

5.1 Purpose

As part of its on-going corporate governance program, MacarthurCook has developed a comprehensive suite of compliance documentation and procedures.

The broad purpose of these documents is to establish and maintain a diligent regime which:

- Aims to prevent, and where necessary, identify and respond to any breaches of the relevant laws, regulations, codes, industry standards or other prudential obligations within which MacarthurCook operates;

-
- Promotes a permanent culture of risk management and compliance;
 - Assists MacarthurCook in becoming and remaining a responsible corporate citizen.

5.2 Compliance Documents

MacarthurCook has developed the following compliance documents:

- MacarthurCook Compliance Plan - details all operational aspects of MacarthurCook's business, including amendments to the Constitution, Information Memoranda, promotion of the funds, continuous disclosure, complaints handling procedures, etc;
- MacarthurCook Controls Matrix – details the legal & regulatory compliance obligations of the company and the controls in place to ensure adherence to the obligations;
- MacarthurCook Investment Process Guidelines - outlines the process adopted by MacarthurCook in identifying, assessing and ultimately investing on behalf of funds for which it is the responsible entity and/or manager;
- MacarthurCook Corporate Governance Policy - details MacarthurCook's policy with respect to staff performance, its Code of Conduct; Insider Trading; and Privacy;
- MacarthurCook Human Resources Manual;
- Business Recovery Plan.

6. FINANCIAL RISK

Financial Risk refers to the risk that MacarthurCook is unable to meet the financial requirements of PS 166 and accordingly its AFS licence.

The financial position MacarthurCook is to be monitored on a monthly basis and its compliance with the obligations under PS 166 verified to the Board at each meeting.

Should MacarthurCook be in breach of its obligations or is likely to be in breach in the next three months, the Chief Executive is to be notified immediately.

The Chief Executive is to notify the directors within 48 hours and put forward to the directors a contingency plan which may include measures such as:

- sale of assets
- borrowing from shareholders
- raising additional capital from shareholders
- reduction in drawings or salaries
- deferment of expenses

7. OPERATIONS RISK MANAGEMENT POLICY

Operations risk arises from being in business and is a catch-all heading designed to cover those risks which are not specifically covered by other risk management policies.

Operations risk can be minimised by employing experienced personnel who are well versed in business risk identification, who are constantly vigilant on behalf of the organisation, together with strong internal controls and effective procedures.

OBJECTIVES

- To identify the areas of risk of financial loss through the occurrence of an event whether outside the control of the company or within its day-to-day operations;
- To ensure that measures are in place to minimise potential losses that may arise from the identified risk areas.
- To ensure appropriate insurance cover is maintained at all times;
- To ensure that the insurance cover meets the minimum requirements imposed by ASIC;

CHANGES TO POLICY

No changes to the operations risk policy are to be made without the approval of the Board.

SECTION A: MANAGEMENT OF RISKS

1. Insurance Brokers

- (i) The company has utilised the services of Miller & Associates, a reputable insurance broker, to obtain adequate insurance to protect the company's personnel, operations and physical assets.
- (ii) The Head of Operations is to review the broker's service annually to determine whether the service provided was satisfactory.
- (iii) Subject to satisfactory review of performance in the interim, after 3 years, the Head of Operations is to put the insurance broking service out to tender.

2. Annual Review

The Head of Operations is to assess and monitor annually the extent to which cost effective insurance can be purchased to cover those aspects of the operations of the company for which policies and procedures do not provide sufficient risk minimisation. This will involve an examination of the assets of the company and assessing the potential risks which may cause a diminution in the value of those assets.

The company is also exposed to risks which may result in liabilities. These liabilities may arise from claims by customers and members of the public who suffer loss or injury as a result of the company's operations. Other sources of potential liability include failure by directors and officers to properly carry out their duties, breach of professional duty by professional advisers, and loss of income due to interrupted business operations. The review is to include assessment of these areas.

3. Insurance Cover

The Head of Operations is to ensure the following covers are in place.

- (i) **Asset Protection**
The company's assets (buildings, office equipment/furniture, motor vehicles etc) are to be insured for their replacement/market value against loss, destruction or damage from fire, burglary and other perils.
- (ii) **Fidelity Guarantee**
The company is to insure itself against fraudulent misappropriation or embezzlement by employees.

-
- (iii) **Business Interruption**
The company is to insure itself against the consequential loss of profits, during the period following the loss or damage from an insured peril when business is interrupted. The sum insured is to cover gross rentals and the additional increase in cost of working.
 - (iv) **Public Liability**
The company is to insure itself against legal liability to the public in respect of bodily injury or property damage arising from the operation of the company's business.
 - (v) **Professional Indemnity**
The company is to insure itself against legal liability to third parties for financial loss arising out of a negligent act or breach of duty.
 - (vi) **Director's and Officers' Liability**
The company is to insure its Directors' and Officers' against any legal liability which may arise from a wrongful act.

4. Staff

- (i) The Chief Executive is to ensure the company retains management expertise and resources appropriate to its activities.
- (ii) The Chief Executive is to ensure that position descriptions detailing minimum experience and qualifications are maintained for all key positions.
- (iii) The Chief Executive is to maintain and regularly review business plans which identify business objectives, performance targets and developmental activities required by staff.

5. Controls

The Head of Operations is to ensure that appropriate financial and internal controls are in place. These controls are to be reviewed annually by the external auditors.

6. Security

The Head of Operations is responsible for minimising the risk of loss by implementing appropriate preventive measures to which may include:

- (i) **Premises security**
Premises to be protected by: video surveillance, button-activated alarms linked to a security company or the equivalent. Premises

considered to be in higher risk areas are to be additionally protected by security patrols.

- (ii) Emergency procedures are to be documented and staff are to be trained regularly in dealing with these contingencies.
- (iii) Cash Handling
No cash other than petty cash is to be kept on the premises.

7. Documentation Risk

All documentation provided to clients and external parties is to be subject to a due diligence process to ensure accuracy and compliance with relevant legislation. Procedures detailing preparation, review and appropriate sign-off are to be reviewed by the Head of Operations annually.

8. Compliance with Legislation

The Chief Executive is to ensure processes are in place to ensure that all statutory and legal obligations of the company are met.

9. Business Resumption Plan

A Disaster Recovery Strategy/Business Continuity Plan is to be maintained and tested annually.

SECTION B: DEFINITION OF ROLES AND RESPONSIBILITIES

The Heads of relevant business units are responsible for developing, documenting and implementing relevant procedures that ensure compliance with these policies.

In the event of any occurrence which may give rise to a claim under any of the company's insurance policies, the Head of Operations is responsible for ensuring that notice is given to the relevant insurers and brokers.

In addition, the Head of Operations is responsible for ensuring compliance with the terms and conditions of insurance policies.

The Head of Operations is responsible for ensuring that the companies operations risk management policy and procedures are reviewed annually and to report to the Board annually as to the effectiveness of the policies.

SECTION C: REPORTING

Reporting to the Board

Any substantial claims (as determined by the Head of Operations) made against the insurance policies are to be reported to the Board as soon as practicable.

The Heads of relevant business units are to report to the Board any breach of this policy, together with any strategies to rectify the problem.

The Board is to consider annually as to the effectiveness of this policy.

8. TRANSACTION AND TECHNOLOGY RISK MANAGEMENT POLICY

INTRODUCTION

Transaction and technology risk relates to the security and integrity of the company's data bases, both automated and non-automated.

OBJECTIVES

- To ensure the security and integrity of financial information.
- To ensure timely and frequent backups are carried out for computerised records.
- To ensure adequate controls are in place to prevent/detect data corruption.
- To ensure disaster recovery procedures are documented and operational.

CHANGES TO POLICY

No changes to the Transaction and Technology Risk Policy are to be made without the approval of the Board.

SECTION A: MANAGEMENT OF RISKS

1. Purchases

Purchase of all computer hardware and software is to be centralised through the Head of Operations who is to maintain a recommended set of standards for such equipment, have in place a supply and support agreement with major suppliers, and co-ordinate all purchasing and installation.

2. Back-ups

Financial and client data maintenance on computer files are to be backed up daily and stored off-site. Procedures are to be documented and subject to an annual audit.

3. IT Controls

- (i) The Head of Operations is responsible for ensuring backups are performed in accordance with documented procedures.
- (ii) The Head of Operations is responsible for the provision of controls to prevent the introduction of computer viruses or other corruptive programs.
- (iii) Change control procedures are to be maintained by the Head of Operations to ensure an appropriate level of control over modification of programs and program access controls.

4. Other Controls

- (i) All source documents are to be stored in secure and lockable cabinets.
- (ii) Security documents are to be kept in a secure fire proof area.
- (iii) Only authorised staff are to have access to computer systems.
- (iv) Staff are to attend appropriate training courses to be authorised to access the system.
- (v) Computer output is to be checked against input documents.
- (vi) Formulate and document procedures aimed at preventing data corruption and fraud.
- (vii) Ensure that appropriate systems and controls are in place and supported by appropriate technology before expanding into new areas of financial investments or products.

5. Disaster Recovery

The Head of Operations is to document and keep up-to-date a Business Continuity Plan/Disaster Recovery Plan (DRP). The Head of Operations is responsible for the execution of the plan which will be tested annually to ensure its adequacy. The DRP will set guidelines for the continuation of business based on the scale of the disaster. The magnitude of the disaster will determine the services that will be provided initially. As action is taken as documented in the plan, service levels will continue to increase until all service can once again be provided. The plan will contain procedures to establish full operational activities within 48-72 hours.

SECTION B: DEFINITION OF ROLES & RESPONSIBILITIES

The Head of Operations is responsible for developing, documenting and implementing relevant procedures that ensure compliance with these policies.

The Head of Operations is responsible for ensuring that the company's Transaction & Technology risk management policy and procedures are reviewed annually and to report to the Board annually as to the effectiveness of the policies.

SECTION C: REPORTING

Reports to the Board

Heads of relevant business units are to report any breach of this policy to the Board, together with any strategies to rectify the problem.

The Board is to consider annually the effectiveness of this policy.

9. HUMAN RESOURCES MANAGEMENT

MacarthurCook's human resources policy is designed to ensure that we maximise our intellectual capital by employing and developing high calibre individuals within all areas of our business.

In recruiting new staff, MacarthurCook pays particular attention to the professional skills and experience of the position. Each position is supported by a Position Description document, outlining the key job requirements and the essential skills and qualities of each position.

Performance appraisals are conducted on all staff on a regular basis – with a minimum of quarterly and preferably monthly, reviews of all colleagues.

Individual remuneration arrangements are tied to the individual's personal performance as well as MacarthurCook's business performance. Annual reviews incorporate performance plans for the forthcoming twelve months, incorporating mutually agreed personal development programs as appropriate.

MacarthurCook has developed and maintains a Personnel Manual and a Training Manual. Representatives are required to maintain registers of security holdings and continuing education registers. All such holders are also required to complete a Compliance Certificate on a semi annual basis.

10. MACARTHURCOOK FUNDS

10.1 Compliance Plan

Compliance Plan acknowledgement sign-offs are to be received from all relevant executives.

10.2 Complaints

A register of customer complaints is to be maintained as per the Compliance Plan.

10.3 Marketing Material Compliance

Due diligence checklists are to be completed for all marketing material and offer documents. A copy of a sample form is enclosed (Form 23).

10.4 Investment Mandate Compliance

Portfolio Managers are to complete a compliance certificate for each portfolio quarterly report (Form 33) verifying that investment guidelines have been adhered to.

11. SERVICE PROVIDERS

Due diligence will be conducted on all significant service providers prior to their appointment. Appropriate contracts will also be entered into which detail the service obligations of the provider.

Service providers are required to provide regular compliance sign-offs related to their operations. Compliance to standards is to be regularly monitored.

Details of external service providers are contained in the register.

12. PRIVACY ACT

Matters or actions contravening or likely to contravene the provisions of the Privacy Act are to be reported.

12.1 Documentation Issued to the Public

The impact of the Act is to be considered with respect to all documentation eliciting information from individuals.

12.2 Investor Personal Information

Security measures will be implemented to ensure that access to personal information is limited.

13. LICENCES AND REGISTRATIONS

13.1 Australian Taxation Office

All funds are to be registered with the ATO.

PINs to enable electronic access for lodgement of GST data are to be sought.

13.2 Australian Financial Services Licence

Conditions of the licence are to be adhered to and relevant fees paid.

13.3 FICS Membership

FICS membership is to be maintained.

14. OTHER STATUTORY RETURNS

14.1 Business Activity Statements

Business Activity Statement (BAS) forms are to be completed for all funds.

14.2 Australian Bureau of Statistics

Returns are to be completed when required.

15. FINANCIAL CONTROLS

15.1 Income Items

Management fees related to MacarthurCook funds will be accrued for the relevant month.

15.2 Expenditure Control

The following controls will be implemented over expenditure:

- (i) An annual budget will be established and approved by the Board;
- (ii) Monthly reports of expenditure vs budget will be prepared and included in Board papers;
- (iii) Authorisation procedures will be adopted after approval by the Board and implemented immediately;
- (iv) A copy of the authorisation procedures will be maintained in the Compliance Manual (see Board memo attached)

16. PHYSICAL ENVIRONMENT

16.1 Emergency Training

A MacarthurCook nominee (Office Manager) will participate in all emergency training sessions conducted on the premises occupied by MacarthurCook. Staff will be issued with an emergency procedures guide.

16.2 Evacuation Drills

MacarthurCook staff will participate in any emergency evacuation drills conducted.

16.3 Incidents

Incidents requiring medical or emergency attention will be reported to the Chief Executive Officer.

Sign Off Certification – Prescribed Documents

Project Name:	Date:
Owner/Person Responsible:	

Phase 1: Due Diligence Sign Off	Return by:
--	-------------------

Purpose of the Due Diligence Checklist:

The purpose of this checklist is to assist in ensuring that all statements included in this document are; True, Not Misleading and that there are No Material Omissions.

It is believed that this due diligence procedure would assist favourable as a Corporations Law defence in any proceeding against MacarthurCook and provides a model process for all of our documents. The defence commonly known as the “due diligence” defence, may be available to MacarthurCook if it can be proven that reasonable precautions were taken and that due diligence was exercised to ensure that all statements to be included were true and not misleading and that there were no material omissions from it. In addition, a defence may be available to MacarthurCook if it can be proved that reliance on information supplied by another person was reasonable in the circumstances or that any mistake was reasonable in the circumstances.

All persons involved in completing this checklist must keep in mind that reliance will be placed on statements made by them in relation to the document attached and named above.

There may be both criminal and civil liability for those who authorise, or cause the issue of, or are involved in a contravention of the Corporations Act.

Function	Key	Copies to (tick)	Signature, Date, Comments
Chief Executive Officer	CEO		Function: Name:
Head of Operations	HO		
Head of Property	HP		
Head of Mortgages	HM		
Product Manager	PM		Comments/Conditions: <input type="checkbox"/> No comments <input type="checkbox"/> Comments as follows:

RISK ASSESSMENT MATRIX

Form 51

- ¹ **Inherent Risk:** The chance of something happening that will have an impact upon objectives assuming there is no control processes or other risk treatments implemented.
- ² **Risk Management:** Assessment of the adequacy and effectiveness of the control processes and other risk treatments, rated as follows:
 Effective: The management of the risk is considered appropriate.
 Qualified: There is a degree of risk management applied however further improvements are considered appropriate.
 Ineffective: Significant issues identified requiring management attention to ensure risk is adequately managed.
- ³ **Current Risk:** The remaining level of risk after control and other risk treatment measures have been taken.

Likelihood and Consequence Matrix

Likelihood	Consequence				
	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Catastrophic
A Almost Certain	H	H	E	E	E
B Likely	M	H	H	E	E
C Possible	L	M	H	E	E
D Unlikely	L	L	M	H	E
E Rare	L	L	M	H	H

Legend

E	extreme risk; immediate action required.
H	high risk; senior management attention needed.
M	moderate risk; management responsibility must be specified.
L	low risk; manage by routine procedures.

Likelihood

Level	Descriptor	Description
A	Almost Certain	Is expected to occur in most circumstances.
B	Likely	Will probably occur in most circumstances.
C	Possible	Might occur at some time.
D	Unlikely	Could occur at some time.
E	Rare	May occur only in exceptional circumstances.

Consequences

Level	Descriptor	Description
1	Insignificant	Low financial loss, minimal customer impact, processing slightly delayed.
2	Minor	Medium financial loss, some customer impact, processing delayed
3	Moderate	High financial loss, medium customer impact, possible customer attrition.
4	Major	Major financial loss, high customer impact, loss of customers
5	Catastrophic	Financial loss > \$500K, processing unable to be continued.

