



# **RISK MANAGEMENT POLICY**

**May 2017**

# TABLE OF CONTENTS

|  |           |
|--|-----------|
| <b>1. OVERVIEW .....</b>                                     | <b>4</b>  |
| 1.1. PURPOSE.....  | 4         |
| 1.2. INTRODUCTION.....                                       | 4         |
| 1.3. AMENDMENT AND APPROVAL .....                            | 4         |
| 1.4. DEFINITIONS.....  | 4         |
| <b>2. AIMS RISK MANAGEMENT METHODOLOGY AND APPROACH.....</b> | <b>6</b>  |
| 2.1. RISK MANAGEMENT METHODOLOGY .....                       | 6         |
| 2.2. IDENTIFY KEY RISKS.....                                 | 6         |
| 2.3. STANDARD RISK CATEGORIES.....                           | 7         |
| 2.4. ANALYSE AND EVALUATE RISK .....                         | 7         |
| 2.5. RATING OR MEASUREMENT OF RISK.....                      | 7         |
| CONSEQUENCE.....   | 8         |
| 2.6. CONTROL AND RISK TREATMENT STRATEGIES.....              | 8         |
| 2.7. MONITORING AND RECORDING RISK .....                     | 8         |
| 2.8. RISK REPORTING .....                                    | 9         |
| <b>3. ADOPTION BY THE BOARD.....</b>                         | <b>10</b> |

# **1. OVERVIEW**

## **1.1. PURPOSE**

The policy provides authoritative guidance on the management of AIMS Funds Management group of companies' (AIMS) business risks and obligations with respect to operating a financial services business in Australia.

## **1.2. INTRODUCTION**

The Board is primarily responsible for establishing an appropriate risk management framework and policy. The Board has delegated responsibility to AIMS management for implementing the risk management policy and the supporting risk management processes to ensure effective risk management. This policy has been developed in accordance with:

- Relevant legislation, including ASIC risk management requirements applicable to AIMS's financial services.
- Leading industry standards, including the International Standard ISO 31000.

AIMS's commitment to this policy is reflected through the provision of adequate resources to implement the policy and appropriate training to ensure that all staff understand and have the competencies with respect to this implementation.

This policy is compulsory in its application. Business Unit Managers have the responsibility and authority to implement the policy and monitor its implementation in the everyday activities of their respective Business Units.

## **1.3. AMENDMENT AND APPROVAL**

This policy can only be amended with the approval of the Audit, Risk and Compliance Committee under the supervision of the Board.

## **1.4. DEFINITIONS**

In this Policy:

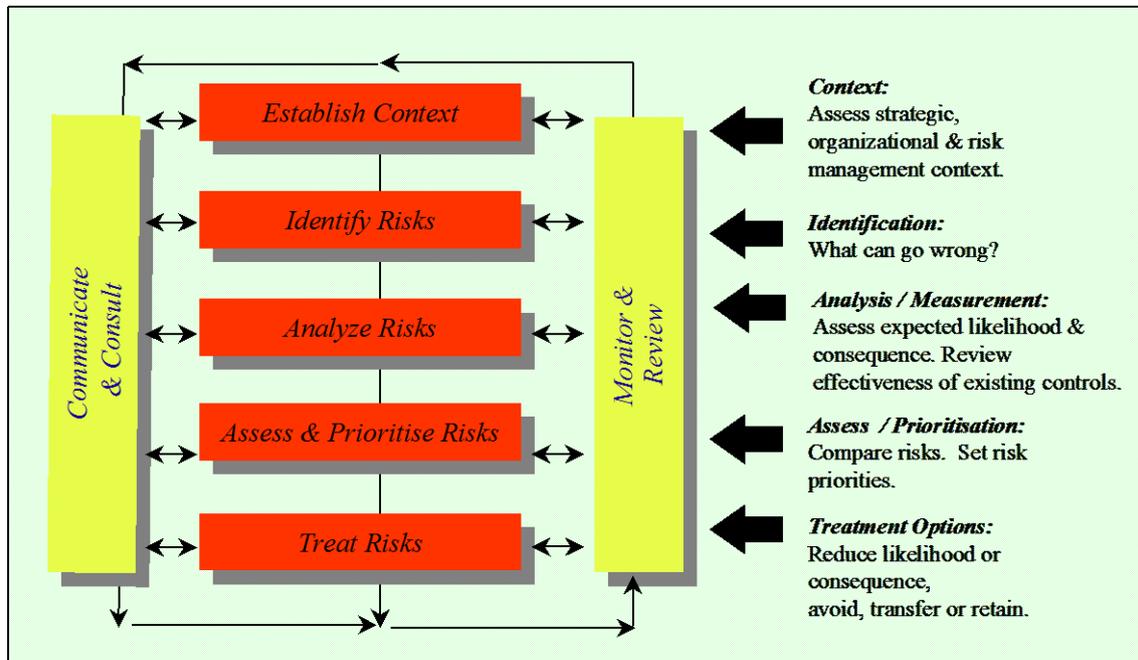
- (a) "AIMS" means the AIMS Funds Management group of companies, which consist of AIMS Fund Management Limited, AIMS Real Estate Funds Limited and AIMS Investment Managers Limited.
- (b) "Board" means the Board of Directors.
- (c) "Business Unit" means a business unit of AIMS, being those business units identified on the organisational chart of AIMS and approved by the Board from time to time.
- (d) "Compliance Officer" means the person who is from time to time appointed by the Board to the position of Compliance Officer.
- (e) "Director" means a director of AIMS.
- (f) "Documents" means all written records and includes electronic records and computer files.

- (g) "Policy" means this document.
- (h) "Risk" means a threat that an event or action will adversely affect AIMS's ability to maximise stakeholder value and to achieve its business objectives. Business risk arises as much from the possibility that opportunities will not be realised as it does from the possibility that threats will materialise or that errors will be made. Risk not only includes the possibility of economic or financial loss or gains but also business interruption, reputation and image concerns.
- (i) "Staff" means directors, officers, employees and contractors of AIMS.

## 2. AIMS RISK MANAGEMENT METHODOLOGY AND APPROACH

### 2.1. RISK MANAGEMENT METHODOLOGY

A diagrammatic overview of AIMS's risk management methodology and approach is presented in the chart below and fully described in this policy.



The key components of AIMS risk management methodology include:

- Identify the risks associated with AIMS's activities.
- Standardise risk categories.
- Analyse the likelihood and consequence of risks associated with AIMS's activities.
- Assess and prioritise the risks identified.
- Identify risk treatment options with the objective to minimise losses and maximise opportunities.
- Provide objective information to decision-makers.

### 2.2. IDENTIFY KEY RISKS

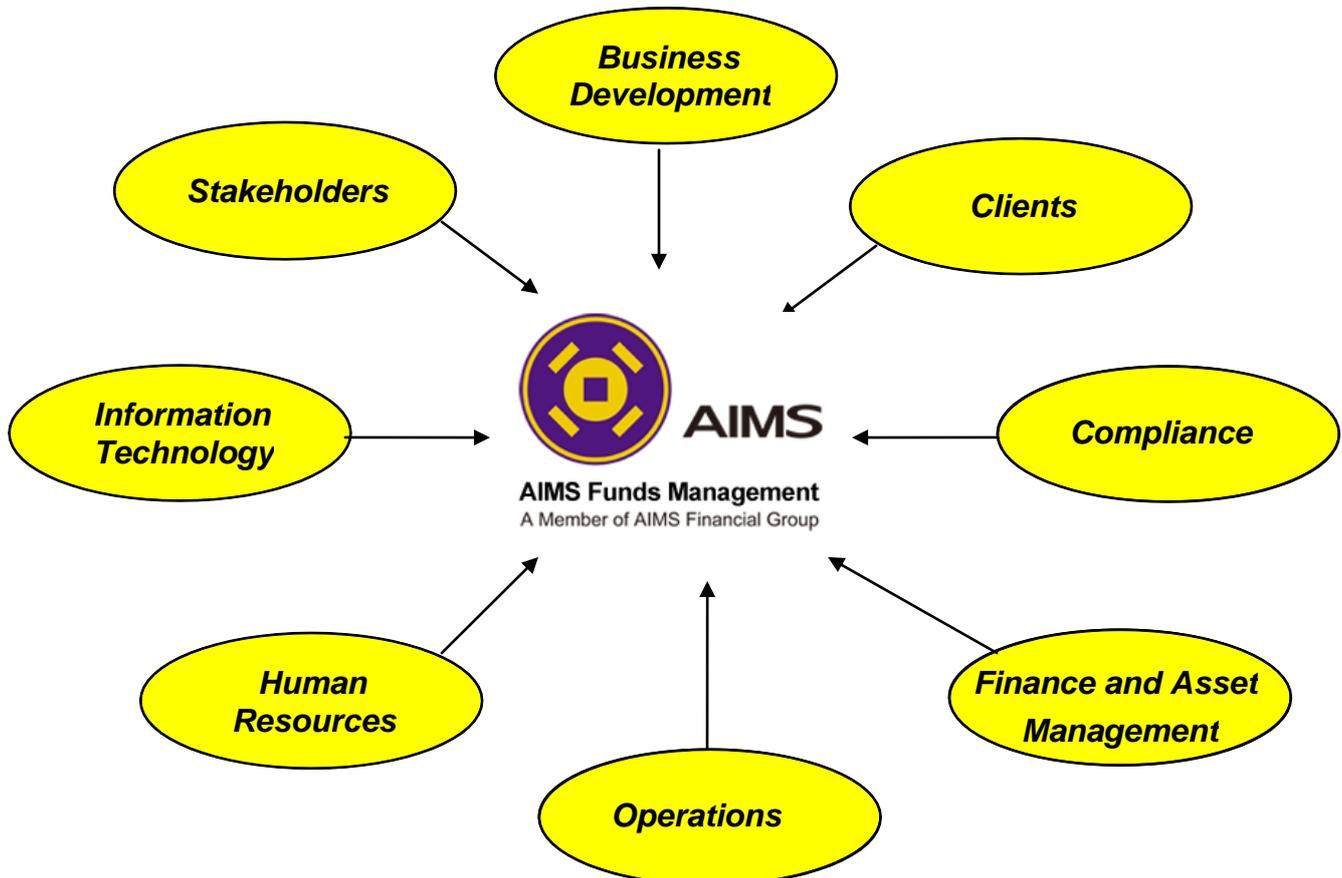
AIMS's approach to risk requires the consideration of all risks that threaten the achievement of business objectives, including compliance with statutory and ethical requirements associated with operating a financial services business in Australia. The objective is to identify all unacceptably high risks and develop processes and controls to manage or mitigate these risks.

Lower-level risks are also considered, but priority should be given to developing treatment plans for high and extreme risks.

This risk assessment and management process is cyclical and ongoing. Monitoring and reviews are performed at all stages of the process in addition to the periodic review of risks and controls.

### 2.3. STANDARD RISK CATEGORIES

The following diagram illustrates the generic AIMS risk categories that will be used for risk assessment and reporting purposes.



### 2.4. ANALYSE AND EVALUATE RISK

AIMS will evaluate the risk implications of all decisions in relation to both existing and proposed activities, systems and procedures. All risks identified will be assessed and documented, together with the processes that reduce those risks, including:

- Identification of the impact that each risk will have on AIMS's operations and activities.
- Assurance that it has the expertise, policies and systems in place to measure monitor and control the risk.
- Consideration of the impact on the financial condition of AIMS arising from the new risk.

### 2.5. RATING OR MEASUREMENT OF RISK

Upon identification, the risk will be assessed having regard to the likelihood, consequence and actions management propose to take to mitigate the risk.

Likelihood and consequence are defined below:

- The *Likelihood* that the business risk may occur.
- The *Consequence* the business risk would have on AIMS if the risk were to occur.

The risk rating definitions and criteria for measuring the likelihood and consequence of risks have been established in accordance with ISO 31000.

Based on the risk rating and definitions detailed above, the Business Unit and AIMS risk assessment will be summarised in the risk profile illustrated below:

The following table indicates the risk rating levels to be used.

Abbreviations:

H = High

S = Significant

M = Medium

L = Low.

## RISK CONSEQUENCE AND LIKELIHOOD MATRIX

| LIKELIHOOD     |   | CONSEQUENCE   |       |          |       |              |
|----------------|---|---------------|-------|----------|-------|--------------|
|                |   | Insignificant | Minor | Moderate | Major | Catastrophic |
|                |   | 1             | 2     | 3        | 4     | 5            |
| Almost certain | 5 | M             | S     | H        | H     | H            |
| Likely         | 4 | M             | M     | S        | H     | H            |
| Possible       | 3 | L             | M     | M        | S     | H            |
| Unlikely       | 2 | L             | L     | M        | M     | S            |
| Rare           | 1 | L             | L     | L        | M     | M            |

### 2.6. CONTROL AND RISK TREATMENT STRATEGIES

Controls are those processes which assist in limiting the risk associated with pursuing business objectives or which lessen the possibility of a compliance breach. Controls include policies, practices and procedures, management systems and structures that assist AIMS to operate efficiently, fairly and honestly and within regulatory parameters. GRC Manager (an internet based compliance and risk program) actively manages this process within the group.

The risks that AIMS encounter can be treated by one of four strategies. A risk can be accepted, reduced, avoided or transferred to a third party, such as an insurer. Senior management should develop and present the business unit risk and control assessment, and the AIMS Board will determine the level of risk tolerance against the respective AIMS risk categories.

### 2.7. MONITORING AND RECORDING RISK

The Legal and Compliance team is responsible for the coordination of risk management throughout the business. Business Unit Managers will be responsible for monitoring the risk profile of their Business Unit on an ongoing basis. As new risks are identified or existing risks expire or change their characteristics, the Business Unit Manager must advise the Legal and Compliance Officer who will update the Risk Register. The Legal and Compliance Officer will coordinate an annual review of all organisational risks together with the Business Unit Managers. The annual review will take place prior to the annual business planning process so that the business plan can have due regard to the risk profile of the business.

The information gathered from the annual business unit risk assessment will provide the basis for documenting the Risk Register. An example of the Risk Register is provided below:

| Risk No | Risk (Explanation) | Business Unit | Likelihood (Rating 1 – 5) | Consequence (Rating 1 – 5) | Risk Rating | Risk Category | Controls |
|---------|--------------------|---------------|---------------------------|----------------------------|-------------|---------------|----------|
|---------|--------------------|---------------|---------------------------|----------------------------|-------------|---------------|----------|

The Risk Register will record risks identified, inherent and residual risk ratings, internal controls established, and the action or strategy required to mitigate unacceptable risks. The Risk Register will be reviewed and updated at least annually through Business Unit risk assessment workshops. Each Business Unit Manager will be responsible for the ongoing maintenance of the Risk Register, which will also be accessible to the Legal and Compliance Officer.

In addition, AIMS is committed to a transparent monitoring and compliance program. Internal Audit will review the risk assessment and test the effectiveness of key controls as part of the audit reviews and report any exceptions to the Audit, Risk and Compliance Committee.

## 2.8. RISK REPORTING

Business Unit Managers will provide a six monthly certification that risks have been managed in line with this policy. The Legal and Compliance Officer will provide a consolidated report to the Audit, Risk and Compliance Committee on a six monthly basis, reflecting the current Business Unit risk profile and a summary of any major changes since the last report.

In addition, all new business proposals presented to the Audit, Risk and Compliance Committee will include an analysis of the associated risks. Business proposals submitted should include an analysis of:

- The risks associated with the proposal and the mitigating strategies that have been determined to manage the risks.
- The compliance requirements relevant to the proposal and how it is planned to meet those requirements.

In assessing the risks, the ratings referred to above should be applied and included in the new business proposal.

### **3. ADOPTION BY THE BOARD**

This Risk Management Policy was first adopted by the Board at a meeting of Directors on 29 April 2010.