Risk Management Policy

Version 2 February 2019

Table of Contents

1. Introduction

Purpose of this Policy

Managed Accounts Holdings Limited ABN 34 128 316 441 ('MGP') is a holding company of companies, and in particular a financial services business carried out by Investment Administration Services Pty Limited ABN 86 109 199 108 and which trades as 'managedaccounts.com.au'.

MGP and its controlled companies together are referred to as the Group in this Policy.

Investment Administration Services ('IAS') holds an Australian Financial Services Licence ('AFSL') No. 284316.

Regulatory expectations for risk management systems are aligning and are expected to continue to do so into the future. Increasingly, more uniform systems, methods and practices arise and align from the various policy and guidance from regulators in Australia and around the world.

As an AFS Licensee, IAS must have adequate risk management systems.[1] ASIC and APRA have indicated that a Licensee must have measures in place to ensure that it complies with its obligation on an on-going basis.[2] Also, ASIC has prescribed its expectation for standards of Risk Management for Responsible Entities [RE's] in its Regulatory Guide 259 of March 2017 which is now expected to become a significant benchmark for non-APRA regulated entities.

Further, the key requirements of APRA's Prudential Standard SPS 220 require that an APRA-regulated institution must:

- have a risk management framework that is appropriate to its size, business mix and complexity;
- maintain a Board-approved risk appetite;
- maintain a Board-approved risk management strategy that describes the key elements of the risk management framework to give effect to its approach to managing risk;
- have a Board-approved business plan that sets out its approach for the operational implementation of its strategic objectives;
- maintain adequate resources to manage, mitigate and monitor material risks, and ensure compliance with this Prudential Standard; and
- notify APRA when it becomes aware of a significant breach of, or material deviation from, the risk management framework, or that the risk management framework does not adequately address a material risk

[1] Section 912A(1)(h) of the Act, RG 259 March 2017

[2] ASIC RG 104.Section D

From this regulatory backdrop, this Policy aims to provide a framework and process for managing risk within the Group and to the highest appropriate regulatory standards that are applicable and appropriate to the extent of the Group's current business 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 IAS 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.

Application of this Policy

This Policy applies to all Group entities and its representatives (directors, employees and contractors etc).

Review and Amendment of Policy

The Risk Management Policy and the risk management framework which it describes will be reviewed on an annual basis. The scope of the annual review will include whether the implementation of risk management processes is in accordance with this Policy, current regulatory expectations and is consistent with logical risk management practices and expectations for MGP and its clients.

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.'[3]

[3] AS/NZS ISO 31000:2009

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 also 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 overall 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 have 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.'[4]

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.

ASIC Regulatory Guide 104 states that ASIC expects AFSL Licensees to 'have a structures process for identifying, managing and managing risk faced by the Licensee'.

RG104.62 ASIC expects the risk management systems will:

a) be based on a structured and systematic process that considers the Licensee's obligations under the Act;

b) identify and evaluate risks faced by the business, focussing on risks that adversely affect consumers and market integrity;

c) establish and maintain controls designed to manage or mitigate those risks; and

d) fully implement and monitor those controls to ensure they are effective.

The guidance provided by ASIC in RG104 for designing and testing measures to ensure a licensee complies with its obligations with respect to a risk management system is included in Appendix 1.

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.

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

3. Responsibilities

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 broadly classified as strategic, operational, financial, legal, contractual and technological. Additionally, many other sub-categories of risk exist including but not limited to regulatory risk, human resource including key person risk, market, business resumption, cyber and continuity risk etc.

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 MGP's disclosure obligations); and

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

To assist them, the Board has established:

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

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

Board Audit, Risk & Compliance Committee

The Board Audit, Risk & Compliance ('ARMCC') Committee 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. It operates in accordance with a Charter, which outlines its structure and responsibilities

The Executive Audit, Risk & Compliance Committee ("ERMCC") operates as a subset of the Executive Committee and supervises the administration of risk at a management and operational level and reports to the ARMCC above on its activities and oversight.

Risk & Compliance Management

The Head of Risk Management, Compliance and Legal is responsible for the co-ordination and continued improvement of the Risk and Compliance Framework in conjunction with management and the Board. The responsibility for the risk management governance arrangements within IAS are 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, ERMCC
Effective operation of internal control structures/ risk treatments	CEO, Executives
Review and monitoring of effectiveness of risk management	ARMCC CEO Head of Risk and Compliance
Delivery of specific reporting and monitoring and supervision of risk in core functions	Manager of the functional areas, CEO, Head of Risk and Compliance

4. Risk Management Framework

The Group has implemented a Risk Management Framework broadly 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. [5]

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 and observation of business activity at multiple levels;

b) communication and consultation to ensure management are involved in the development and maintenance of ongoing risk monitoring and supervision;

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

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

Control and Assurance Checklists are maintained for the Group either in spreadsheet form or electronically as the case requires, and which describe the risks facing the business activities within the Group and the key controls surrounding those risks.

The checklists are reviewed at least quarterly and their results are presented to the ERMCC and summarised for the ARMCC.

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;

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

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

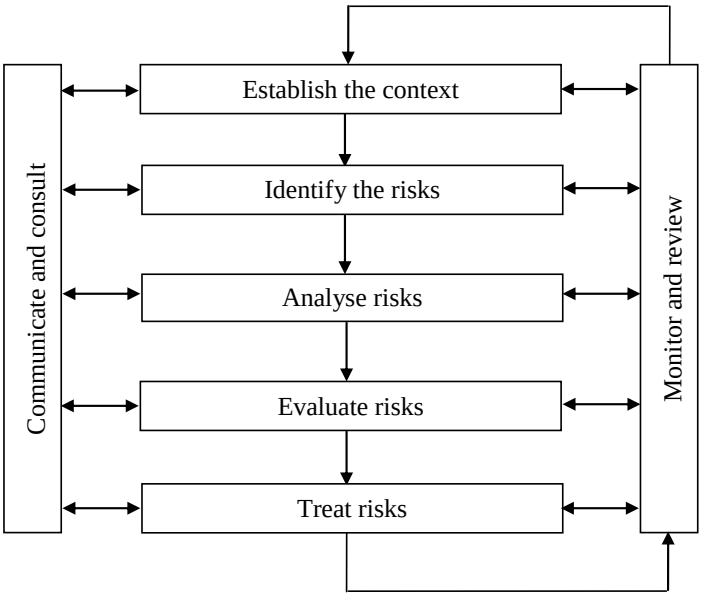
d) regular internal review, including an ERMCC structure; and

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

The Framework is intended to assist an organisation to integrate observance and control of risks into its overall management system.

5. The Risk Management Process

The risk management process can be broadly illustrated as follows:



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:

Establish the context

By establishing context, the organisation defines its objectives, outlines the internal and external parameters to be considered 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 i.e. 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 like 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 [Risk Tolerance]. Some criteria will be imposed by legal and regulatory requirements while some will reflect the organisation's values, objectives and resources.

Identify Risks

Risks at both the company and functional level are identified.

The primary mechanism for risk identification covers reviews of:

a) business processes,

b) regulatory environment,

c) technology and contractual arrangements,

d) company financials, and

e) operational risks.

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

Generic examples of risks for IAS' business are:

a) Political circumstances – including legislative changes relating to financial services,

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.

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.

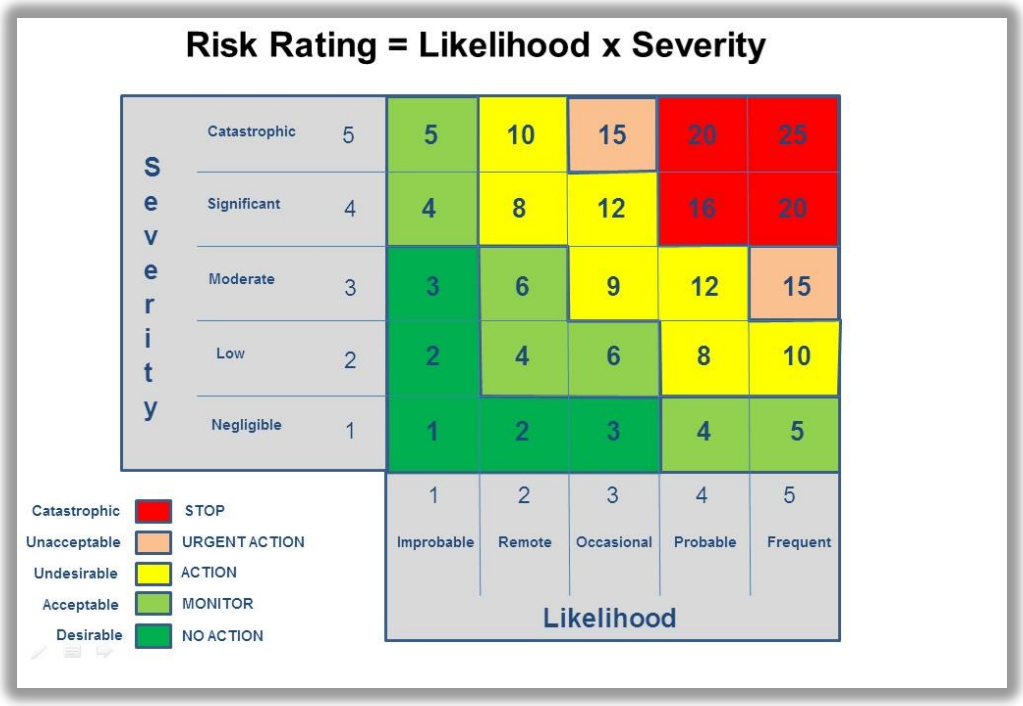
Qualitative measure of Consequence

Descriptor	Rating	Financial Value	Legal/ Reputation [Examples]
Negligible	1	Low financial loss – under $5k	Insignificant impact, no disruption to capability, no impact on reputation, no significant impact on clients
Low	2	Minor financial loss – $10k - $50k	Requires management attention - process resolution measures to be investigated and implemented
Moderate	3	Financial loss – $50k - $ 250k	Non-compliance with regulation, perhaps with sanction, fine/ enforcement, Adverse media or client attention
Significant	4	Financial loss – 250k - $1 m	Serious non-compliance with regulation, with fine/ enforcement Serious adverse public / client attention, Legal engagement from external parties, potential for adverse media
Catastrophic	5	Financial loss – over $1m	Regulator action, serious (or threatened) litigation (including class action, potential loss of license or ability to conduct business, large legal claim threatening viability of the company, adverse and ongoing media coverage

Qualitative measure of Likelihood

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

Risk Rating Matrix



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 [Risk Matrix] 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.

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.

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"[6]

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

The Risk Checklist contains details of key risk areas, an explanation of the associated risks, a risk assessment (detailing consequences and likelihood) and may highlight the controls that have been implemented.

The Risk Checklists are maintained by the Head of Risk and Compliance. The Checklists are distributed to functional areas for completion at a regular frequency and are reviewed by the

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

Head of Risk and Compliance and the results reported to the Executive Risk Committee and Board Audit Risk and Compliance Committee at the required frequency.

The Board reviews the Risk Checklists annually.

6. Risk Awareness and Training

The Board has primary 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.

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 Dimensions and Principles

The Group has created a structured Risk Management, Compliance and Legal infrastructure, vested with the authority and responsibility to identify measure, monitor, evaluate, and assist the management of risk across the group. This area's efforts to meet the goal of recognised leadership in risk management is designed in support of sound business practice and minimisation of the potential for error and loss by anticipating risks and reinforcing a solid control and operating framework for the organisation.

The Group's underpinning position on risk management is as follows:

"Risks most often are found where the commercial opportunities arise". On this premise, risk management focuses on ensuring our business is protected and can operate successfully and profitably with a minimum of necessary risk. On that basis, our group's first commitment to a risk-managed approach to business is to identify the "Dimensions of Risk" which our businesses are exposed to and then to elicit and adopt a series of "Risk Management Principles".

Risk and Assurance Checklists

Risk and assurance checklists may be maintained manually, via spreadsheet, or in semi or fully -automated electronic systems as decided by the business from time to time.

The risk and assurance categories chosen are intended to help the Group organise its risk identification and assessment activities on a grouped basis. Risk groups and sub-groups are considered when formulating risk checklists [risk matrices]. These will include all sources of risk affecting the area under consideration.

Assets

This collection of risks from various checklists and systems and when linked to the various other components of the Group's risk framework, shall address the Company's requirements to protect its intellectual, human and financial capital assets, maintain its reputation and allow it seek to achieve its stated strategy with a minimum of 'risk interference'.

People

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

Continuity

This collection of risks relates to IAS'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.

Financial

This collection of risks addresses IAS's exposure to loss if transactions are not processed in accordance with service levels and acceptable market 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 IAS'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 applicable to the Group. 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 and other competitive environment risks and can include changes in financial market conditions (domestic and international equity market movements, economic changes), regulation, competitors, etc.

External Investment Managers

This collection of risks relates to relationships and mandates with external investment managers for IAS's product, and the conduct of the external managers.

External Service Providers/Counterparties

This collection of risks relates to the provision of services by external parties to IAS.

Product

This collection of risks relate to demand for new products and services, offer documents, 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.

Operational

These various risks relate to the operational service and delivery environment of IAS including client registry, portfolio administration, reporting and adviser servicing.

MDA Compliance

These various risks relate to the specific MDA requirements under the Regulatory Guide and Class Order.

RISK PLOT- PRIORITY RISKS – Mth/Year