



**Mirrabooka Investments Limited**  
**Risk Management Policy & Framework**

**June 2023**

**Table of Contents:**

**1. INTRODUCTION .....3**

**2. OBJECTIVES OF THE RISK MANAGEMENT POLICY AND FRAMEWORK .....4**

**3. RISK MANAGEMENT POLICY & FRAMEWORK.....5**

**4. RISK MANAGEMENT POLICY STATEMENT .....6**

**5. MATERIAL RISKS .....8**

**6. RISK APPETITE.....9**

**7. ROLES AND RESPONSIBILITIES.....10**

**8. RISK MANAGEMENT METHODOLOGY .....15**

**9. STRESS TESTING .....24**

**10. RISK CULTURE.....25**

**APPENDIX A. RISK INDICATORS .....26**

**APPENDIX B. KEY RISK MANAGEMENT DEFINITIONS .....29**

## 1. Introduction

Australian Investment Company Services Limited ('AICS') is wholly owned by the investment companies AFIC and Djerriwarrh with 75 per cent and 25 per cent stakes, respectively. Board representatives from Mirrabooka and AMCIL are also invited to attend AICS Board and Audit, Risk Management and Remuneration Committee ("ARRC") Meetings, and their input sought.

AICS provides administrative and managerial support for the following listed investment companies (collectively "the investment companies"):

- ▶ Australian Foundation Investment Company Limited ('AFIC');
- ▶ Djerriwarrh Investments Limited ('Djerriwarrh');
- ▶ Mirrabooka Investments Limited ('Mirrabooka'); and
- ▶ AMCIL Limited ('AMCIL').

AICS and the Board of Mirrabooka recognise that risk management is an essential element of good corporate governance. They have established an effective risk framework which is designed to optimise shareholder returns by:

- ▶ minimising the risk of loss due to operational failures or fraud; and
- ▶ highlighting the areas of investment risk to aid in decision making.

The Board has requested that the Risk Management Policy be accommodated in a written, published framework as a matter of appropriate corporate governance and in accordance with Principle 7 ("Recognising and Managing Risk") of the 4th Edition of the ASX's Corporate Governance Principles and Recommendations.

Prudential Standard CPS 220 requires an APRA-regulated institution (applicable to banks and insurers) to have systems for identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating material risks that may affect its ability to meet its obligations to depositors and/or policyholders. Whilst compliance with CPS 220 is not a direct requirement for AICS and Mirrabooka, this standard has been considered in the development of the risk management framework and applied in a fit for purpose context relative to the nature and size of these companies. Although Mirrabooka and AICS do not hold shareholder details on their systems, have shareholder accounts or keep security records (shares are held by the sponsoring broker or in NZ directly by the share registry via a CSN) cyber security remains a key focus for risk management in order to safeguard normal business operations.

The Board and Audit Committee of Mirrabooka have agreed that they will adopt the following Framework as relevant to each of the Companies. The Framework is reviewed annually by the AICS ARRC and the Mirrabooka Audit Committee.

AICS has an internal audit function, which is currently outsourced to EY. EY report to the AICS ARRC which is composed entirely of non-executive Directors. Their findings and reports, where appropriate, are shared with the Audit Committees of the investment companies

As AICS has been delegated the day-to-day responsibility for managing operational risk (including fraud), the Mirrabooka Audit Committee does not consider it necessary for Mirrabooka itself to have an internal audit function. The reports that AICS and EY provide, together with their review (at least annually) of the Risk Management Framework and Risk Register and their presence at AICS ARRC meetings plus the direct reports of the AICS executives to the Audit Committee provide sufficient evidence and information for them to have oversight of the risk management function, evaluate the effectiveness of the risk management and internal control processes and to monitor its continual improvement. Mirrabooka and AICS also use other external parties to review various aspects of risk and risk management – e.g. SecureWorks for cyber security.

AICS and Mirrabooka, by their nature, are not directly exposed to material economic, environmental and social sustainability risks (as defined in the ASX Corporate Governance Principles), but the Mirrabooka Investment Committee does consider these risks, amongst others, in reviewing the portfolio of current and potential investments, as noted in the Annual Report and on the Company's website.

## **2. Objectives of the Risk Management Policy and Framework**

This document sets out the Risk Management Policy and Framework of AICS and Mirrabooka and the measures established by them to manage and monitor the factors that could potentially prevent them from achieving business objectives.

A Risk Management Policy and Framework that is appropriate for the size and complexity of the organisation will form the basis for embedding enterprise risk management within the culture of the organisation. The objectives of this policy are to:

- ▶ Enable AICS to provide an efficient and reliable service to Mirrabooka to enable it to meet its obligations and objectives.
- ▶ Increase the likelihood that AICS and Mirrabooka will be successful in their business operations by mitigating potentially damaging events occurring (e.g. operational risk, including cyber risks) and maximising the results of positive events (e.g. financial position, investment strategies, etc.), through the implementation of risk management strategies.
- ▶ Comply with all relevant legislation and relevant guidelines (e.g. ASX Corporate Governance Principles and Recommendations).
- ▶ Provide decision makers with the means to identify risks and to determine whether the controls in place are adequate to mitigate those risks.
- ▶ Provide a mechanism to assess the levels of risk that can be accepted.
- ▶ Ensure that the application of risk management practices is understood by the employees of AICS and the Directors and officers of Mirrabooka; and a strong risk culture is well-entrenched. This has been reinforced during the current requirements and includes adaptations where necessary – for instance, email approval of payments and authorisation of invoices as opposed to physical authorisation.
- ▶ Reduce the consequence and/or likelihood of potentially damaging events by regular reviews of investments and investment strategies (by the Investment Committee) or by transferring the impact of potentially damaging events to third parties (e.g. by insurance and contractual arrangements).

This document provides an overview of the framework within AICS and Mirrabooka for the management of risks associated with activities undertaken to meet their objectives. The document also outlines the risk management approach taken to identify, assess, treat and monitor the risks facing the businesses.

### 3. Risk Management Policy & Framework

The Boards of Directors of each of AICS and Mirrabooka recognise that effective risk management is an integral part of good management practice. Risk management is integrated into the investment philosophy via wide portfolios of stocks that are kept under review and business plans and practices and a culture of compliance is actively promoted. The Boards of Directors have ultimate responsibility for ensuring the adequacy of risk management systems and ensuring that risks are identified and addressed in a timely and adequate manner.

AICS and its' senior management, as part of their day-to-day duties, have regard for the risks inherent in the businesses, and have established and maintain compliance and risk management policies and procedures, compliance monitoring programmes and a culture of compliance and risk management.

In addition, the Executive Management Team ('EMT'), Investment Team and Portfolio Manager and the Investment Committee of Mirrabooka have regard for the investment risks inherent in the businesses and the investment portfolios of the companies.

The Boards are assisted in their risk management activities by their Audit Committees which meet usually three times per year for Mirrabooka (and twice for AICS), and by the Investment Committee (for Mirrabooka) with regards to investment risk.

Co-ordination of the risk management activities is the responsibility of the "Risk Officer." The Risk Officer is the Chief Financial Officer.

The hierarchy of elements which comprise the Risk Management Policy & Framework is shown in the diagram below.



## 4. Risk Management Policy Statement

### *Purpose*

The aim of this policy is to provide clear guidelines on the management of risks to enable the achievement of strategic and operational objectives.

### *Scope*

This policy aims to cover all material risks that the entity faces. It is to be adhered to by all employees and Board members and, where relevant, contractors and consultants.

### *Approach*

The risk management methodology adopted by AICS and Mirrabooka is based on the AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines.

Key aspects of the methodology are:

1. Establish the context.
2. Identify risks.
3. Analyse the risks (including the Maximum Foreseeable Consequences of those risks).
4. Evaluate the risks (including rating the risks).
5. Treat the risks (including strategies to mitigate).
6. Monitor and Review.
7. Communicate and Consult.

### *Risk Management Culture*

Company policies and training are designed to ensure that staff behaviour that relates to their individual performance involve informed decisions based on a reasonable analysis of foreseeable risks, opportunities and their associated impacts on the implementation of AICS and Mirrabooka's strategies and the achievement of goals. AICS and Mirrabooka maintain an open culture that emphasises open and speedy communication that seeks to identify issues before they arise and to swiftly remedy any gaps that may arise.

### *Responsibilities*

The responsibility for implementing this policy rests with all employees, management and Board / Committee members; and where relevant, contractors and consultants to AICS and / or Mirrabooka.

*Review of policy*

This policy will be reviewed internally on an on-going basis and by external experts on a periodic basis. Responsibility for ensuring that this review is performed rests with the CFO / Risk Officer. Any significant changes are provided to the Audit Committees of AICS and Mirrabooka for review and formal approval.

## 5. Material risks

AICS recognises the following key risks (or risk categories) that are associated with its activity:

- a) **Financial Risk** – the risk of financial loss to members resulting from external or internal factors or inadequate financial controls. AICS and Mirrabooka further recognise the following sub-categories of financial risk:
  - i. **Liquidity risk** - a risk that cash funds may not be available for Mirrabooka to meet its preferred dividend options or invest in certain market conditions without having to sell assets from its investment portfolio.
  - ii. **Investment risk** – a risk that investment decisions may lead to sub-optimal performance.
- b) **Operational risks (non-financial risks)** - the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. AICS and Mirrabooka further recognise the following sub-categories of operational risk:
  - i. **Compliance risk** - a risk of losses incurred by Mirrabooka as a result of failure (or perceived failure) to comply with relevant laws, regulations and AICS' and/or Mirrabooka's policies. This includes compliance with taxation requirements. Taxation risk management is managed in accordance with the Tax Governance Policy of the Board and the Tax Governance Framework.
  - ii. **Governance risk** - a risk of poor governance reducing investor confidence.
  - iii. **Reputation risk** – a risk of loss resulting from damages to Mirrabooka's or AICS' reputation (including negative media and social media commentary).
  - iv. **Strategic risk** - The risk of a decline in competitive advantage, leading to a long-term decline in market share and share price. **Political risk** – The risk of unfavourable changes in the political and regulatory environment, including changes to Taxation Legislation, that may affect the ability of Mirrabooka and/or its shareholders to achieve their objectives.
  - v. **Environmental, Social & Governance risk** – the risk that investment decisions fail to adequately incorporate environmental, social and governance factors.
  - vi. **Outsourcing risk** – a risk of direct or indirect loss due to service providers' failure to comply with service level agreements and standards. Given that AICS and Mirrabooka place a substantial reliance on the third parties, outsourcing risk is recognised as a separate category.
  - vii. **Business continuity risk** – a failure to establish and implement an effective Business Continuity Plan and Disaster Recovery Plan.
  - viii. **Fraud risk** – a risk of losses due to shareholders' funds / assets misappropriated by staff or external parties.
  - ix. **People risk** – AICS recognise people risk as a key category of operational risk due to its relatively small number of employees, which makes it particularly susceptible to key person risk (e.g. lack of appropriate attraction and retention policies leading to unwanted departures). People risk also includes such risk sub-categories as a failure to maintain a healthy risk culture or appropriate HR policies and ensuring compliance with internal policies and procedures as a result of any change in personnel.
  - x. **Cyber risk** – a risk of financial losses, disruption or damage to the reputation of AICS and Mirrabooka, as a result of a failure or unauthorised or erroneous access or use of its information systems, that affect the confidentiality, availability, or integrity of information or information systems. This includes cyber-attacks such as distributed denial



of service (DDoS) attacks, ransomware, phishing, as well as loss of confidential data and other events. This includes any enhanced cyber risk that may eventuate with staff working from home.

Specific risks, associated controls established to mitigate the risks faced by AICS and Mirrabooka and accountabilities for managing respective risks are documented in the Risk Register. The Risk Register is maintained by the Chief Financial Officer and continually updated with an annual review to ensure that it remains current and relevant for AICS and Mirrabooka, and reflects accurate information on the risk profile and the effectiveness of their internal control environment.

## **6. Risk Appetite**

AICS has a Board approved Risk Appetite Statement (RAS) which sets out the degree of risk AICS is willing to accept in the pursuit of its strategic objectives. This RAS is separately maintained within the 'Risk Profile and Risk Register' Summary Report.

The Risk Profile and Risk Register outlines the material risk categories, risk appetite setting (risk tolerance), residual risk level, and executive and Board oversight. The register is reviewed annually by the Chief Financial Officer and presented to the Audit Committee.

The Board's approach is to ensure that AICS and Mirrabooka's activities are compatible with their defined risk management strategies and risk appetite. In determining their risk appetite (stated below), the Boards take into account the nature of their roles as a provider of financial services and for Mirrabooka's Board, the fact that as an investor in the equity markets, and the particular sectors in which it invests, the business will by definition carry a high level of equity risk.

The Boards will accept a conservative level of risk, directing that the risk exposure is to be reasonable at all times. Residual risks (after controls) assessed as Extreme or High will generally be considered to be outside AICS and Mirrabooka's risk appetite. Where residual extreme or high risks exist after controls, the Board will be required to formally approve these risks.

It is recognised that some risks are inherent to the AICS and Mirrabooka business (e.g. the market risk resulting from the investment in tradeable securities). The Boards' governance policies and risk management practices, supported by the experienced Executive Management team, provide a level of assurance that appropriate control measures are implemented for new and evolving risks as they are identified. AICS and Mirrabooka aim to ensure continuous improvement of their risk management and governance framework and these are reported through to the Audit Committees.

AICS and Mirrabooka utilise the ASD 'Essential Eight Maturity Model' in their approach to cyber resilience. AICS and Mirrabooka aim to be at Maturity Level Three (fully aligned with intent of mitigation strategy) with a minimum acceptable level of Maturity Level Two (mostly aligned with intent of mitigation strategy). In addition, AICS has its cyber security framework reviewed under the NIST (National Institute of Standards and Framework) cyber security framework and has had it reviewed by external cyber security experts. Its outsourced IT provider is a member of the Australian Joint Cyber Security Centre and the Australian Information Security Association.

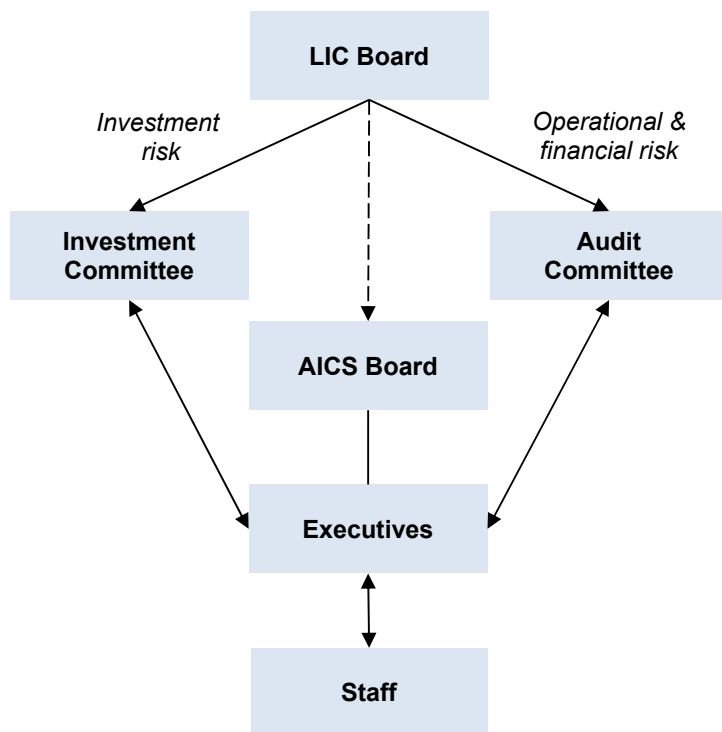
Those risks that are acceptable to the Board will be subject to regular review and reporting (including risk dashboard reporting outlining risk trends and emerging risks.) Key high-level risks, together with materially relevant subordinate risks, will be subject to review by the Internal Auditor. The results of these reviews are presented to the Audit Committees and to the Boards, where appropriate.

Potential indicators that can be used to monitor changes in the level of key risks inherent to AICS, are defined in Appendix A.

## **7. Roles and Responsibilities**

The Board of each company delegates to the Chief Executive Officer and EMT responsibility for implementing the operational risk management practices within AICS and, by definition, Mirrabooka. Investment risk lies largely within the oversight of the various Investment Committees on behalf of the Boards. The Risk Officer leads the ongoing implementation of, and compliance with, the Risk Management Policy & Framework. Over and above these accountabilities, everyone in the organisation has responsibility for managing risk.

A key objective of the Risk Management Policy & Framework is to embed a risk culture throughout the organisation. The following diagram outlines the Committee structure in place to oversee and manage risk across AICS and Mirrabooka:



The following table outlines the key responsibilities with regards to risk management at AICS and at Mirrabooka:

<b>Board of Directors</b>	<p>The Board of Directors of Mirrabooka holds the following responsibilities:</p> <ul style="list-style-type: none"> <li>▶ To ensure compliance with Principle 7 of the ASX Corporate Governance Principles and Recommendations:             <ul style="list-style-type: none"> <li>▪ To establish policies for the oversight and management of material business risks, and disclose a summary of these policies.</li> <li>▪ To require management to design and implement the risk management and internal control system to manage the company's material business risks and report to it on whether those risks are being managed effectively (also for AICS).</li> <li>▪ To determine the overarching risk appetite (also for AICS)</li> <li>▪ To require the CEO and CFO to assure the Board that the financial statements are founded on a sound system of risk management and internal control and that the system is operating effectively in all material respects in relation to financial reporting risks.</li> <li>▪ To review, at least annually, the policies and procedures on risk oversight and management as approved by the Audit Committee (also for AICS).</li> </ul> </li> </ul>
---------------------------	---

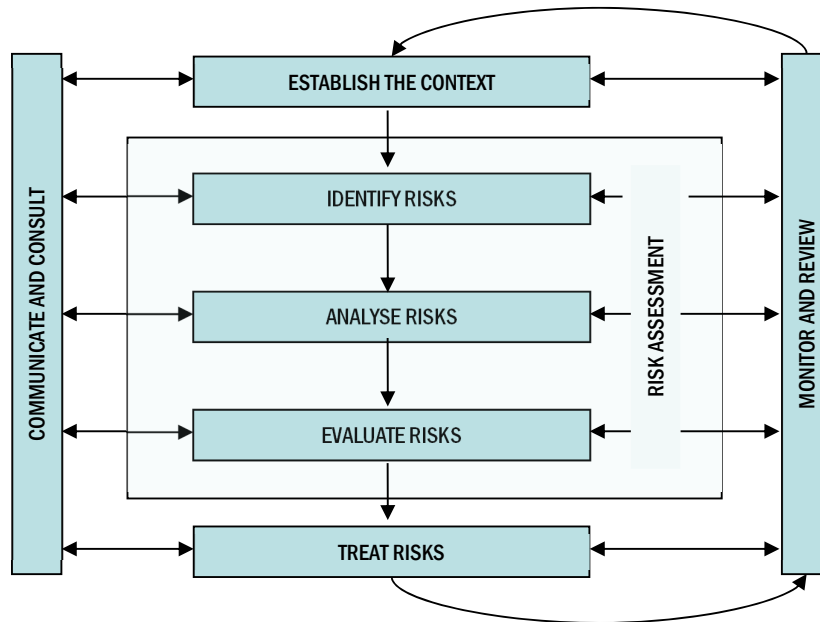
<p><b>Audit Committee</b></p>	<p>The Audit Committee of each Company (AICS and Mirrabooka) has the following responsibilities:</p> <ul style="list-style-type: none"> <li>▶ To review and approve the Risk Management Policy &amp; Framework.</li> <li>▶ To report to the Board on the process and responsibilities for managing risk.</li> <li>▶ To confirm that appropriate risk management methodologies and practices have been implemented across the organisation through: <ul style="list-style-type: none"> <li>▪ Receiving risk reporting (via assurance mapping, risk dashboards and other reports) from the EMT to provide assurance that all key risks have been appropriately identified and managed including any emerging risks.</li> <li>▪ Receiving internal audit reporting about the adequacy of risk and controls through the Internal Audit function (via AICS for Mirrabooka).</li> <li>▪ Receiving external reports on aspects of risk management as it or the EMT deem necessary.</li> </ul> </li> <li>▶ To report to the Board on the organisation's adherence to the Risk Management Policy &amp; Framework and to report on material matters, findings and recommendations, pertaining to risk management and the internal compliance and control framework.</li> <li>▶ To make recommendations to the Board in relation to its responsibilities to determine the risk appetite and review, at least annually, the policies and procedures on risk oversight and management and internal control.</li> <li>▶ To review the policies and practices in meeting its compliance obligations with regards to laws, regulations, codes and company policies.</li> </ul> <p>The EMT and auditors (both internal and external) provide regular reporting to the Audit Committee and Risk Management is a standing agenda item at each Audit Committee. Normally for the internal auditors this is via AICS although the Audit Committee of Mirrabooka has access to them as needed.</p>
<p><b>Investment Committee</b></p>	<p>The Investment Committee has the following responsibilities:</p> <ul style="list-style-type: none"> <li>▶ Investment decisions including adding new investments, increasing or reducing existing investments and disposals and review and authorise transactions.</li> <li>▶ Set, monitor and review authorisation limits for the Investment Team.</li> <li>▶ Review recommendations for voting instructions.</li> <li>▶ Review portfolios with regards to weightings and investment risk (including economic, environmental and social sustainability risks) and concentration risk.</li> <li>▶ Monitor option coverage and the risks of having stock being called away or put stock.</li> <li>▶ Review liquidity and contingencies.</li> <li>▶ Review and monitor the implementation of the investment delegation of authority to assess ongoing effectiveness.</li> <li>▶ Report to the Board any breaches of delegation.</li> </ul> <p>The CIO ensures that the investments are made in accordance with the delegated authorities.</p>
<p><b>Managing Director &amp; Chief Financial Officer / Risk Officer</b></p>	<p>The Managing Director and the CFO are responsible for ensuring that risks are identified and controls established to mitigate those risks. The CFO is responsible for assisting with establishing, overseeing, reviewing and maintaining Mirrabooka's Risk Management Policy &amp; Framework. This is achieved through the development of an appropriate infrastructure to identify, measure, manage and report risks.</p> <p>The Managing Director is ultimately accountable for managing material risks in accordance with the approved Risk Management Policy and risk appetite.</p> <p>The CFO/Risk Officer has the delegated authority (and responsibility) for the system of risk oversight and management and internal control.</p> <p>The CFO / Risk Officer performs the following risk management functions:</p> <ul style="list-style-type: none"> <li>▶ Ensuring risk management processes are established and operating effectively.</li> <li>▶ Maintaining a central risk register for recording risks identified and the mitigating strategies throughout AICS and the investment companies.</li> <li>▶ Assessing the design and operating effectiveness of key controls and mitigating strategies, including monitoring the results of external assessments such as the ASAE 3150 controls report.</li> </ul>

	<ul style="list-style-type: none"> <li>▶ Summarising and prioritising risks for the Audit Committee.</li> <li>▶ Monitoring the performance of outsourced service providers and assessing their risk management, particularly with regards to the provision of IT.</li> <li>▶ Recommending education and training in risk practices and processes.</li> <li>▶ Ownership of the risk register and communication of required measures to all staff.</li> </ul>
<b>EMT</b>	<p>Responsibility for risk management rests with each member of the EMT who is to lead risk management processes within AICS. Key responsibilities include:</p> <ul style="list-style-type: none"> <li>▶ Implementing the Risk Management Policy &amp; Framework and processes.</li> <li>▶ Considering key risks as part of the strategic and business planning processes.</li> <li>▶ Reporting risk events in accordance with the reporting process included in the framework.</li> <li>▶ Reporting to Mirrabooka and to the Board of AICS on the risk profiles and risk mitigation plans of AICS, as appropriate.</li> <li>▶ Implementing measures to appropriately resolve risk issues as they are identified, within their respective lines and actions fully completed in a timely manner.</li> <li>▶ Maintaining and promoting a culture of risk management and compliance.</li> <li>▶ Raising awareness of the relevant risks to staff and ensuring compliance with AICS policy, procedures and controls.</li> <li>▶ Ensuring risk management performance indicators align with corporate performance indicators.</li> <li>▶ Ensuring that the necessary resources are allocated to risk management.</li> </ul>
<b>Employees</b>	<p>Employees are responsible for:</p> <ul style="list-style-type: none"> <li>▶ Reporting any risk events (i.e. injury, hazard, financial loss (including fraud), service interruption, cyber incidents (other than disregarded emails)* etc.) as soon as it is detected or reported to the relevant member of the EMT.</li> <li>▶ Performing duties without risk to other employees, AICS customers, Mirrabooka shareholders or the community in general or to their own health and safety.</li> <li>▶ Complying with operational policies procedures and risk mitigation controls within daily tasks in AICS operations.</li> <li>▶ Identifying and escalating any potential risks and issues in accordance with the Risk Management Policy &amp; Framework.</li> <li>▶ Providing risk management related information, as requested by their manager.</li> <li>▶ The Investment Team have additional responsibilities for assessing the investment risk (including economic, environmental and social sustainability risks) of the investments held by the Investment Companies.</li> <li>▶ Perform ad-hoc testing of controls not covered as part of ASAE 3150 review as needed.</li> </ul> <p>* These are 'spam' and 'phishing' emails received by staff which are deleted without being acted upon.</p>
<b>Company Secretary &amp; Compliance</b>	<p>The Company Secretary has been appointed as Compliance Officer of AICS and is responsible for ensuring that effective compliance arrangements are in place for AICS to comply with AFSL and other compliance requirements. The Compliance Manager reports to the AICS Audit Committee on AFSL compliance quarterly, with that report forwarded to the Mirrabooka Audit Committee.</p> <p>In addition, the Company Secretary is responsible to the Board of AICS for reviewing, implementing and maintaining compliance with relevant Occupational Health and Safety, Privacy and Data Breach obligations and the Fair Work Act and other employment legislation.</p>
<b>Internal Auditor</b>	<p>Internal audit performs reviews which are aligned to the key risks in AICS and Mirrabooka reporting to the Audit Committee and the Board on the:</p> <ul style="list-style-type: none"> <li>▶ Periodic assessment and update of AICS Risk Register.</li> </ul>

	<ul style="list-style-type: none"> <li>▶ Audit of the design and operating effectiveness of the Internal Controls in accordance with ASAE 3150 Assurance Engagements on Controls or other relevant Standard(s) as agreed by the Audit Committee.</li> <li>▶ Reviews included in the annual internal audit plan as approved by the Audit Committee.</li> </ul>
<b>External Auditor</b>	<p>External auditor's responsibilities include:</p> <ul style="list-style-type: none"> <li>▶ To express a review conclusion on the half-year financial report of Mirrabooka by conducting an external review (half-year) and an audit opinion on the annual financial report by conducting an external audit (year-end) of the accounts of AICS and Mirrabooka in accordance with Australian Auditing Standards.</li> <li>▶ To perform an external audit of AFSL compliance by AICS.</li> <li>▶ To provide an extensive review and half-yearly sign-off of tax balances.</li> </ul>
<b>Tax Agent</b>	<p>The Tax Agent's responsibilities include:</p> <ul style="list-style-type: none"> <li>▶ To review taxation information and prepare tax returns</li> </ul>

## 8. Risk Management Methodology

The Risk Management Policy & Framework has been developed to take into account the principles and guidelines outlined in AS / NZS ISO 31000: 2009 Risk Management – Principles and Guidelines and utilising guidance from its internal and external auditors. This approach involves establishing the context in which it operates, identifying the risks, analysing those risks, evaluating the risks, treating the risks where appropriate and monitoring, reviewing and reporting risks and the overall performance of the framework. Part of the Risk Analysis process includes an assessment, including independent testing, of the controls that are in place to address those risks. The results of these tests are reported to the Audit Committees of AICS and Mirrabooka. This process is underpinned through regular communication and consultation with key business stakeholders. The following diagram represents an overview of this approach to risk management process:



### 8.1 Establish the Context

By establishing the context, AICS defines the internal, external and risk management context in which the risk management process will take place.

Risk management involves an appropriate balance between realising opportunities while attempting to minimise risks or losses.

The Boards and the Audit and Investment Committees have considered their material risks and mitigating procedures and controls within the Boards' risk appetite.

Specifically, establishing the context includes consideration of the following:

- ▶ The strategic direction of AICS and Mirrabooka;
- ▶ The social, cultural, political, legal, regulatory, taxation, technological, financial, technical, economic, natural and competitive environment;
- ▶ Any key drivers or trends having an impact on objectives;
- ▶ Capabilities including resources, knowledge, information systems and technologies;
- ▶ The form and extent of any contractual arrangements;

- ▶ Both AICS and Mirrabooka's culture and values; and
- ▶ The relevant stakeholders who will be involved in the management of the risks, both internal and external.

## 8.2 Identify Risks

### Definition of risk:

*This framework defines a risk as the chance of something happening that will have an impact upon the achievement of AICS' and Mirrabooka's business objectives. This broad definition of risk encapsulates threats or hazards (the risk of loss or the occurrence of negative events), uncertainty (the risk of variance between anticipated and outcomes and the actual results) and lost opportunity (the risk of positive events not occurring).*

AICS and Mirrabooka can both be viewed as mature, established businesses with well-recognised objectives and a well-understood investment risk profile. It is critical, however, that this does not translate into allowing the control environment to deteriorate over time or not identifying new risks on a timely basis. Accordingly, the following procedures are in place to identify risks:

- ▶ Maintenance of risk registers. The Risk Register has been developed by management and subject to consultation and review by external consultants. It is reviewed and updated on a regular basis by the Chief Financial Officer and the Company Secretary and formally by the Audit Committee on an annual basis. It is periodically reviewed by external experts.
- ▶ The audit committee of Mirrabooka has adopted the AICS risk register and will review on a periodic basis to validate its appropriateness.
- ▶ Developing a high awareness of the importance of risk management within the companies, including identifying training needs where necessary.
- ▶ Continuing oversight of investments and review of risk profiles by Investment Committee.
- ▶ Consultation with internal and external stakeholders and consultants.
- ▶ Aligning the annual Internal Audit plan with the risk register, with audit plan and reports reviewed by the audit committee and recommendations actioned by management.
- ▶ Monitoring of current market conditions and current / or potential events to identify key risks emerging from the external environment.

### Risks are identified taking into consideration:

- ▶ Legal and regulatory trends and pronouncements, including accounting and other applicable standards, including ASD's "essential Eight Maturity Model" for cyber risks.
- ▶ Industry and economic risk history and emerging trends.
- ▶ Organisational risk history.
- ▶ Organisational structure and size.



### 8.3 Analyse Risks

All new and existing risks identified are recorded in the risk register. As part of the development of the risk register all of the risks are analysed and evaluated. For each risk, the Maximum Foreseeable Consequences (MFC) or worst-case scenario is anticipated. Each risk is assessed in terms of:

- ▶ Existing controls and the success of those controls in mitigating risk.
- ▶ The likelihood of an event occurring.
- ▶ The impact or consequences of the identified risk if it occurred.
- ▶ The residual risk rating.

#### Likelihood:

Some events happen once in a lifetime. Others can happen almost every day. Analysing risks requires an assessment of their frequency of occurrence. This following table provides broad descriptions used to support likelihood ratings.

Likelihood Rating	Descriptor	Qualitative description
5	Almost Certain	<ul style="list-style-type: none"> <li>▶ Is expected to occur in most circumstances, or</li> <li>▶ Has more than 90% chance of occurring in the next 12 months</li> </ul>
4	Likely	<ul style="list-style-type: none"> <li>▶ Will probably occur in most circumstances, or</li> <li>▶ Has 51% - 75% chance of occurring within the next 12 months.</li> </ul>
3	Possible	<ul style="list-style-type: none"> <li>▶ Might occur at some time, or</li> <li>▶ Has 11% - 50% chance of occurring within the next 12 months</li> </ul>
2	Unlikely	<ul style="list-style-type: none"> <li>▶ May occur at some time, or</li> <li>▶ Has less than 6 - 10% chance of occurring within the next 12 months.</li> </ul>
1	Rare	<ul style="list-style-type: none"> <li>▶ May occur only in exceptional circumstances, or</li> <li>▶ Has less than 5% chance of occurring within the next 12 months.</li> </ul>

#### Consequence:

The risks facing AICS and Mirrabooka have financial, operational and reputational consequences.

Each consequence can be rated, in terms of its severity, from insignificant to catastrophic. Risks arising from market-wide price movements are not included, as these are considered investment risks (rather than operational risks) and accepted as such by the Mirrabooka Board (see Section 8.5). Consequence ratings, which are neither exclusive nor comprehensive (i.e. significant expense may be incurred without significant negative publicity) are explained in detail below:

Rating						
		<i>Reputation Impact</i>	<i>Regulatory Impact</i>	<i>Business Impact</i>	<i>Financial Impact</i>	<i>Shareholder Impact</i>
<b>Critical</b>	<b>5</b>	<ul style="list-style-type: none"> <li>▶ Substantial long term/ irreparable damage to brand and degradation of investor perception of value i.e. trust, affecting whole business.</li> <li>▶ Significant negative publicity, i.e. from TV, newspaper or social media.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Cessation of business or loss of financial services licence or loss of LIC status due to regulatory non-compliance.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Strategic / operational objectives unable to be achieved (all users affected).</li> </ul>	<ul style="list-style-type: none"> <li>▶ Significant write-down of investments (e.g., in the amount of more than 20% of the market value of Mirrabooka's investment portfolio).</li> <li>▶ Very significant / catastrophic expense or loss incurred (e.g. more than 30% of Mirrabooka's annual Net Profit After Tax).</li> </ul>	<ul style="list-style-type: none"> <li>▶ Severe shareholder impact, likely to result in loss of significant number of shareholders or very significant shareholder groups</li> </ul>
<b>Major</b>	<b>4</b>	<ul style="list-style-type: none"> <li>▶ Significant damage to brand and degradation of investor perception of value i.e. trust, affecting whole business.</li> <li>▶ Minor negative publicity, i.e. from state newspaper / radio or social media.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Fines, penalties and restrictions on business due to regulatory non-compliance.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Significant impact on strategic / operational objectives.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Major write down of investments (e.g. more than 10% but less than 20% of the market value of Mirrabooka's investment portfolio).</li> <li>▶ Significant expense / loss incurred (e.g. more than 10% but less than 30% of Mirrabooka's annual Net Profit After Tax).</li> </ul>	<ul style="list-style-type: none"> <li>▶ High shareholder impact, likely to result in loss of a large number of shareholders or significant shareholder groups</li> </ul>
<b>Moderate</b>	<b>3</b>	<ul style="list-style-type: none"> <li>▶ Moderate damage to brand and degradation of investor perception of value.</li> <li>▶ Local negative publicity, i.e. from newspaper / radio or social media.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Low level fines (issuance of directive) due to regulatory non-compliance.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Medium impact on strategic / operational objectives.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Moderate write-down of investments (e.g. less than 10% of Mirrabooka's total annual revenue or profit).</li> <li>▶ Moderate expense / loss incurred (e.g. more than 2.5% but less than 10% of Mirrabooka's annual Net Profit After Tax).</li> </ul>	<ul style="list-style-type: none"> <li>▶ Shareholder dissatisfaction, likely to result in some shareholder impact</li> </ul>
<b>Minor</b>	<b>2</b>	<ul style="list-style-type: none"> <li>▶ Minimal damage to brand and degradation of investor perception of value.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Censure due to regulatory non-compliance.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Minimal impact on strategic / operational objectives.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Minor expense / loss incurred (e.g. more than 0.1% but less than 2.5% of Mirrabooka's annual Net Profit After Tax).</li> </ul>	<ul style="list-style-type: none"> <li>▶ Minor dissatisfied shareholders</li> <li>▶ Low shareholder impact</li> </ul>
<b>Insignificant</b>	<b>1</b>	<ul style="list-style-type: none"> <li>▶ Little or no brand damage or degradation of investor perception of value.</li> </ul>	<ul style="list-style-type: none"> <li>▶ No regulatory impact.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Consequences are dealt with by routine operations.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Insignificant expense / loss incurred (e.g. less than 0.1% of Mirrabooka's annual Net Profit After Tax).</li> </ul>	<ul style="list-style-type: none"> <li>▶ Minimal isolated shareholder dissatisfaction</li> <li>▶ No adverse impact on shareholders</li> </ul>

Following the assessment of risks likelihood and consequence, AICS and Mirrabooka identify and evaluate the effectiveness of controls and mitigating actions to determine the residual risk level.

#### **8.4 Control Design**

Control activities are procedures and tasks established and implemented as part of business units' regular activities to help ensure specific risks are adequately mitigated. The design of the control should meet a defined objective to address each risk. A control mix of different controls with individual objectives may be required for significant risks.

A good control design will include a control name, description, objective, owner, type (preventive/ detective/directive), method (manual, automated, or semi-automated), and effectiveness rating.

Controls can be preventive, detective or directive:

- Preventative controls stops a risk occurring so reducing the likelihood
- Detective controls identify when a risk has become an event (incident or breach) so that it can be remediated quickly and reduce the impact.
- Directive controls provide guidance on what should occur. Directive (soft) controls include policies and procedures, and training. These are not sufficient on their own to address risks and must be accompanied by at least a preventative or detective control.

Controls can be manual, automated or a combination of the two (i.e., semi-automated):

- **Manual controls** are performed solely by humans.
- **Automated controls** are embedded within a system and require no human intervention to perform a control.
- **Semi-automated controls** are controls that are housed within a system but require human actions for them to operate, i.e. a review and approval of a transaction by a human in a system: without the approval the system will not permit the transaction to be posted.

#### **8.5 Control Effectiveness**

For risks to be managed within tolerance, controls have to be well-designed and operating effectively. Where controls exist but are not operated and monitored, then adequate control does not exist. In order for mitigating practices/controls to be effective they also must be communicated, actioned and monitored. When assessing the effectiveness of controls, the table below is utilised.

The effectiveness of key controls is reassessed and updated on a regular (at least annual) basis by the Chief Financial Officer through understanding of the business, policies, procedures, practices and processes in addition to discussion with key responsible control owners and review of any relevant third-party reporting (e.g. internal audit reporting and ASAE 3150 controls audit).

Where more than one control exists to mitigate a particular risk, overall control effectiveness rating, based on which a residual risk rating is assessed, is determined by:

- a) consideration of the relevant impact of each control on mitigating a respective risk, and
- b) proportion of effective versus ineffective controls.

Rating		Description
1	Effective	<ul style="list-style-type: none"> <li>▶ Controls are adequately designed, fully implemented and operating effectively to manage the risks and achieve the objectives in an efficient manner (e.g. controls are documented, consistently performed and applied, communicated, maintained, and regularly tested).</li> </ul>
2	Partially Effective	<ul style="list-style-type: none"> <li>▶ Controls are adequately designed, implemented and operating somewhat effectively to manage the risks and achieve the objectives. Some efficiency opportunities have been identified but not yet actioned, or</li> <li>▶ Controls are adequately designed, but not fully implemented and operating partially effectively (e.g. controls are only partially documented or communicated, performed intermittently, gaps in application, infrequently tested or maintained). Improvement opportunities have been identified but not yet actioned.</li> </ul>
3	Ineffective	<ul style="list-style-type: none"> <li>▶ Controls are not adequately designed, implemented and operating effectively (e.g. controls are not documented, not performed or ad-hoc application, partially communicated, not tested or maintained), or</li> <li>▶ Controls are subject to major change, or</li> <li>▶ Controls are in the process of being implemented and their effectiveness cannot be confirmed.</li> </ul>

### 8.6 Evaluate Residual Risks

The purpose of risk evaluation is to make decisions, based on the outcomes of risk analysis, about which risks need treatment and treatment priorities. Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered.

#### Risk Rating Table:

Residual risk is the level of risk that remains after consideration of all existing mitigants / controls.

The Matrix below depicts the residual risk ratings applied to each of the risks identified:

Likelihood	Maximum Foreseeable Consequence (after controls)				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Low	Medium	High	Extreme	Extreme
Likely	Low	Medium	Medium	High	Extreme
Possible	Low	Low	Medium	Medium	High
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Low	Medium	High

The required action to address the residual risks is then applied according to the following table, unless the Audit Committee determines that the residual risk rating for that particular risk is acceptable:

Colour	Response
E	Extreme risk: immediate action required
H	High risk: Senior Management attention needed
M	Medium risk: management responsibility must be specified
L	Low risk: manage by routine procedures

## 8.7 Risk Treatment

Risk treatment involves identifying the range of options for treating risks, assessing these options and the preparation and implementation of treatment plans. Risk treatment plans should be developed to bring about a residual risk level that is in line with the organisation's risk tolerance. Where an organisation's residual risk is above the risk tolerance, an analysis should be undertaken on the risk treatment options (possibly including cost/benefit analysis) and an action plan should be developed that is owned by individuals and has completion timeframes.

Treatment plans should detail:

- ▶ The reason for the selection of the treatment option including any expected benefits to be gained;
- ▶ The person responsible for the approval and implementation of the treatment plan;
- ▶ Proposed actions to achieve the treatment plan;
- ▶ Key resource requirements to deliver the treatment plan;
- ▶ Timing of implementation
- ▶ Documentation to evidence requirements for implementation of treatment plans; and
- ▶ Assurance actions required to validate treatment plans' implementation

AICS and the Board of Mirrabooka have determined that currently a material risk would be unacceptable and would require immediate action if any residual risk rating was Extreme or High or if the controls were ineffective. Excluded from this is the risk of investing in equity instruments as a class – internal controls and procedures can reduce specific investment risk but as a Listed Investment Company that invests in a portfolio of equities the Board accepts that there remains a high risk that over the medium to long term there will be periods of capital loss, realised or unrealised, as noted in the market movements during the coronavirus pandemic.

Risk tolerances can be established on an organisation-wide basis or specific to an individual risk to an organisation's risk profile. An organisation's tolerance to individual risk can be difficult to formalise as the ongoing change in an organisation's context requires organisations to be dynamic and respond to risk events as deemed necessary by its officers.

Risk tolerance levels can be influenced by adjusting some key aspects of the Risk Management Policy & Framework (i.e., definitions within the consequence and likelihood ratings).

### *Risk Treatment Options:*

When deciding upon an appropriate risk treatment plan, the organisation may consider a range of options to treat the risk. The option chosen will vary whether the risk will bring about positive or negative consequences. Traditionally, risk management

principles have been utilised to manage risks that may have a negative impact upon objectives. Below is a table that further describes the various risk treatment options.

<b>Option</b>	<b>Description</b>
<i>Avoid</i>	Avoid and abstain from an activity when the accumulative opportunity for gain is outweighed by the accumulative opportunity for loss.
<i>Mitigation Controls</i>	Implementation of new controls or strengthening existing controls.
<i>Transference</i>	Sharing the potential gain or loss with a third party to reduce the exposure to the risk or set of risks associated with particular activities (for example by insurance or derivatives).
<i>Accept</i>	After establishing appropriate controls, the company needs to accept the residual risk within the decision / activity and monitor those controls in place.

*Assessing Risk Treatment Options:*

A number of treatment options can be considered and applied either individually or in combination. Selecting the most appropriate option(s) involves balancing the costs of implementing each treatment against the benefits derived from it. In general, the cost of managing risks needs to be commensurate with the benefits obtained. When making such cost versus benefit judgements, the context should be taken into account. It is important to consider all direct and indirect costs and benefits whether tangible or intangible, and measured in financial or other terms.

**8.8 Risk Management Tools**

AICS manages key risks through the utilisation of the following risk management tools:

1. Day-to-day management of activities
2. Risk assessments (including project risk assessments)
3. Risk register
4. Monitoring of KRIs
5. Risk reporting
6. EMT review and communication
7. Staff communication, feedback, training and education
8. Audit Committee Oversight
9. Internal audits

## 8.9 Monitor and Review

Monitoring and review is part of the Risk Management process for the purposes of:

- ▶ Analysing and learning lessons from events, changes and trends.
- ▶ Identifying emerging risks.
- ▶ Identifying key risk indicators and monitoring trends in the external and internal context which can require revision of risk ratings, treatments and priorities.
- ▶ Ensuring that the risk treatment measures are effective in both design and operation.
- ▶ Ensuring that sufficient progress is being made in addressing the material risk mitigation and control issues.

The CFO / Risk Officer is responsible for the operation of a monitoring program throughout the year, designed to ensure that the risk profile remains relevant and current. This review will also seek to assess whether the controls in place are adequate with regards to the nature of the risks and are operating in an effective manner.

To ensure that the Risk Management Policy & Framework remains up to date, the Boards, through the Audit Committees and EMT review the framework annually and on a regular basis through the Compliance Monitoring Assessments. The risks are also reviewed when circumstances relevant to the business change, to ensure that the measures remain relevant and effective, reflecting business developments and any major changes in legislation, the business risk profile, the environment and technology.

The ongoing monitoring of any further actions and the existence and effectiveness of internal and financial controls is performed by Internal & External Audit, Audit Committee and by management assessments of the control environment.

KRIs are metrics that assist with monitoring changes or potential changes in key risk exposure. The business works with management to identify, monitor and report on KRIs on a periodic basis. For example, monthly/quarterly.

The following summarises the key risk monitoring and review activities to be undertaken by AICS, the investment companies or external parties:

Report name	Activity	Period covered	Frequency	Responsibility
	Review and approve the Risk Management Policy & Framework.		Annually	Audit Committee
	Review of risk profile and risk registers.		Ongoing	CFO/Internal Audit
	Reviews of compliance by external audits.		Annually	Audit Committee/ CFO

## 8.10 Issue management

- Issues exist where controls to manage risk do not exist or are not designed well enough or operating effectively. Issues identification is the purpose of risk management activities and is an indicator of a risk aware organisation if issues are identified before a risk event or incident/breach occurs. Issues are therefore control weaknesses and, as such, the controls identified as such need to be enhanced. Issue management governs the recording of identified control weaknesses, and the tracking of action plans to remediate.
- Where issues exist or events (see below) have occurred that indicate a control weakness, the risk exposures in the risk register should be updated until the control(s) have been remediated.

- The documentation of an issue should include an issue name, description of the issue, who identified the issue, date of issue identification, associated risk and control, root cause, gross financial impact (if any), rating (high/medium/low), repeated issue identifier, due date for closure, issue owner, actions to resolve the issue, and due date for issue resolution. The issue management process should monitor if issues are closed within due dates, and include an assurance process for implemented actions. Issues should be tracked using an issue register and should be periodically reported to senior management.

### **8.11 Event Management**

When a risk materialises, it is an event. When there is a financial or non-financial loss associated, it is a loss. Recording events in an on-going register is valuable for the following reasons:

1. It provides information to assist in the making of business risk decisions;
2. It acts as a corporate memory;
3. It demonstrates an existing risk exposure and facilitates management of that exposure; and
4. It provides context for risk scoring.

The documentation of a risk event should include a description of the event, its cause, gross financial outcome amounts, date of the loss, rating (high/medium/low)\, repeated events identifier, due date for closure, event owners, recoveries and action taken. Risk events should be tagged to issues and managed as part of the issue management process. Relevant risk events occurring at outsourced service providers (that impact AICS and Mirrabooka) would also be captured within the events register and analysis would be performed examining how these impact on the relevant AICS and/or Mirrabooka's risk profile.

### **8.12 Communicate and Consult**

Effective communication and consultation are important to ensure that those responsible for implementing risk management, and those with a vested interest understand the basis upon which decisions are made and provide input to the identification and evaluation of risks. Management at AICS have communicated and consulted with stakeholders (in particular, the investment companies) at each stage of the risk management process. As their views can have a significant impact on the decisions made, it is important that the stakeholders' perception is identified, recorded and taken into account in the decision-making process. In particular, stakeholders' views of what is an acceptable risk (risk criteria) or the desired target risk can change over time.

## **9. Stress testing**

AICS utilises stress-testing to evaluate the potential impact of adverse but plausible changes in external factors on its portfolio and assists the Executive Leadership Team in decision-making.

Stress testing outcomes are regularly reviewed by the Executive Leadership Team

AICS conducts stress-testing in relation to the following risks:

#### *a) Liquidity risk*

To assess potential impact of unfavourable market changes on its portfolio, AICS performs an assessment of the potential impact of a movement in stock prices on the value of the call/put exposures. This also includes upcoming payments (such as purchases,



taxation payments and dividends payable) and amounts receivable (such as sales from the trading or investment portfolios and dividends receivable).

The results of the scenario analysis are reported through the liquidity report to the Investment Committee.

*b) Investment risk*

Mirrabooka

The Investment Committee reviews Mirrabooka's holdings with reference to market weightings in the portfolio, both at a stock value and at a delta-weighted value.

The appropriateness of scenarios is reviewed by AICS at least annually.

## **10. Risk culture**

AICS and Mirrabooka are committed to instilling and maintaining a healthy risk culture, that promotes and demonstrates risk accountability, high standards of ethical conduct and recognises the long-term interests of their shareholders as their core values.

They also seek to ensure compliance with the applicable regulatory requirements and internal policies and procedures. AICS' and Mirrabooka's corporate principles of conduct outline the company's values and behaviours expected from directors and employees.

Given the size of the organisation, AICS monitors its risk culture through internal communications and interactions with staff. An informal view on risk culture is also requested from both Internal and External Audit at Audit Committee meetings periodically. On an as-needs basis, a more formal assessment of risk culture will be considered (e.g. risk culture survey).

AICS have developed and implemented a whistle-blower protection framework and policy, to ensure that individuals are able to, in a secure way, express their concerns about unlawful behaviour or breaches of policies and procedures.

### **Risk training**

AICS provides annual risk training to staff members with the aim of enhancing risk knowledge and awareness. Risk training may include risk management framework, event management processes, risk culture, as well as current and emerging risks.

In addition, AICS periodically engages third party providers including its internal auditor, EY, to deliver training programs on specialised subjects (e.g. cyber security).

## Appendix A. Risk indicators

Risk Category	Material Risk	Potential risk indicators
<i>Investment risk</i>		
1.1	Investment Decisions may lead to sub-optimal performance	<i>Lagging indicators:</i> ▶ Sustained under-performance against index or other relevant measures
1.2	Non-compliance with investment strategy, objectives and mandates.	<i>Lagging indicators:</i> ▶ Trades conducted without due authorisation
<i>Compliance risk</i>		
2.1	Continuous disclosure, statutory reporting and other ASX Listing and Legal requirements (including OH&S and the Fair Work Act) may not be complied with leading to regulatory intervention	<i>Lagging indicators:</i> ▶ Regular or material breaches of ASX or Legal (including ASIC) reporting requirements <i>Leading indicators:</i> ▶ Audit recommendations not closed for over 6 months
2.2	Company may lose Financial Services Licence with attendant restriction on activities and reputational damage	<i>Leading indicators:</i> ▶ FSL breach notifications received or non-compliance with FSL audits
2.3	Inaccurate or non-compliant marketing material or communication to stakeholders resulting in non-compliance with the Competition and Consumer Act	<i>Lagging indicators:</i> ▶ Adverse regulatory findings or complaints in relation to the communications and marketing materials
2.4	Income / CGT / Other taxation calculations and payments may be inaccurate or delayed. Tax reporting may be inaccurate and not in accordance with ATO legislation	<i>Lagging indicators:</i> ▶ Regular or material errors identified in tax calculation and reporting by internal or external auditors ▶ Adverse findings by ATO Reviews/Audits <i>Leading indicators:</i> ▶ Outcomes of reviews of methodologies and calculations by external advisers
2.5	Financial reporting may not be accurate and not in accordance with accounting standards	<i>Lagging indicators:</i> ▶ Identified disparities between Company's financial reports and Auditor's recommendations <i>Leading indicators:</i> ▶ Consultations with auditors regarding changes to accounting standards. ▶ Review and approval of pro-forma financial statements prior to year-end by external auditors ▶ Review of treatment of material transactions by external advisers
<i>Governance risk</i>		
3.1	Board may not meet relevant standards e.g. ASX Principles of Corporate Governance	<i>Lagging indicators:</i> ▶ Non-compliance with ASX Principles of Corporate Governance not satisfactorily explained or ignored
3.2	AICS may not meet required governance standards.	<i>Leading indicators:</i> ▶ Ceases to be a majority of non-executive, external directors ▶ Audit recommendations not closed within a suitable period.
3.3	Outside interests may result in conflicts of interest	<i>Lagging indicators:</i> ▶ Conflicts of interest identified but not resolved <i>Leading indicators:</i> ▶ Annual certifications by staff uncompleted ▶

<b>Risk Category</b>	<b>Material Risk</b>	<b>Potential risk indicators</b>
<i>Reputation risk</i>		
4.1	AICS/Mirrabooka come under sustained attack through negative commentary through various media channels (including social media).	<i>Lagging indicators:</i> ▶ Sustained negative coverage of Mirrabooka in the media
<i>Strategic risk</i>		
5.1	Increased competition from other LICs / investment vehicles (e.g. ETFs) / Products leading to loss of business / market share and fall of share price	<i>Lagging indicators:</i> ▶ Large reduction in numbers of shareholders  <i>Leading indicators:</i> ▶ Sustained trading at a large discount to NTA
<i>Political risk</i>		
6.1	The risk of unfavourable changes in the political and regulatory environment, including changes to Taxation Legislation, that may affect the ability of Mirrabooka and/or its shareholders to achieve their objectives.	<i>Other considerations:</i> ▶ Changes in actual or proposed legislation ▶ Changes in economic environment
<i>Operational risks</i>		
<i>7.1 Outsourcing</i>		
7.1.1	Service providers do not comply with service level agreements and standards.	<i>Lagging indicators:</i> ▶ Tickets not closed during agreed periods or SLA thresholds continuously un-met
<i>7.2 Business continuity risk</i>		
7.2.1	Disaster event resulting in loss of Business Continuity (systems / premises / people)	<i>Leading indicators:</i> ▶ Business Continuity Plan not tested ▶ Information systems/ data inaccessible based on the disaster recovery plan performed or not recovered within the recovery time objectives
<i>7.3 Fraud risk</i>		
7.3.1	Shareholders' funds / assets may be misappropriated by staff or external parties	<i>Lagging indicators:</i> ▶ Identified incidents of internal or external fraud
7.3.2	Unauthorised trading resulting financial or reputational loss.	<i>Lagging indicators:</i> ▶ Financial losses incurred as a result of unauthorised trading
<i>7.4 People risk</i>		
7.4.1	Inadequate resources and employee capability (skills) / key employees may leave with irreplaceable corporate knowledge (key person risk)	<i>Lagging indicators:</i> ▶ Number of resignations of key personnel  <i>Leading indicators:</i> ▶ Succession plans undeveloped
7.4.2	Failure, to maintain a healthy risk culture and commitment to high standards of ethical conduct	<i>Lagging indicators:</i> ▶ Non-compliance with the Corporate principles of conduct
7.4.3	Failure to ensure compliance with the regulatory requirements and internal policies and procedures.	<i>Leading indicators:</i> ▶ Material or regular non-compliance with regulatory requirements and/or internal policies and procedures identified through either external review or internal oversight
<i>7.5 Cyber risk</i>		
7.5.1	A failure, unauthorised or erroneous access or use of AICS' or Mirrabooka's information systems (that affect the confidentiality,	<i>Lagging indicators:</i> ▶ Identified breaches of cyber security  <i>Leading indicators:</i> ▶ Outstanding recommendations from IT Security reviews

<b>Risk Category</b>	<b>Material Risk</b>	<b>Potential risk indicators</b>
	availability, or integrity of information or its information systems including websites hacked and rendered inoperable, or loss of confidential data	<ul style="list-style-type: none"> <li>▶ Updates/security patches not implemented.</li> </ul>
<i>7.6 Other operational risks</i>		
7.6.1	Trades may not be settled in a timely manner resulting in financial / reputational loss. Credit risk as a result of timing differences between payment / receipt of stock / cash	<i>Lagging indicators:</i> <ul style="list-style-type: none"> <li>▶ Regular and systematic failure of trades to settle</li> </ul>
7.6.2	Company may lose LIC status due to investments not being made in accordance with LIC tax legislation	<i>Lagging indicators:</i> <ul style="list-style-type: none"> <li>▶ LIC status not reviewed in accordance with legislation</li> <li>▶ ATO reviews/audits determine that all gains are on revenue account</li> </ul>
7.6.3	Loss of Goldman Sachs as Sponsoring Broker / Options Clearing Broker	<i>Other considerations:</i> <ul style="list-style-type: none"> <li>▶ Notification received of withdrawal of service</li> </ul>
7.6.4	Erroneous investment processing including inaccurate deal capture, confirmation and settlement	<i>Lagging indicators:</i> <ul style="list-style-type: none"> <li>▶ Regular or systematic failure to process transactions identified through internal or external review</li> </ul>
7.6.5	Failure to action discretionary corporate actions	<i>Lagging indicators:</i> <ul style="list-style-type: none"> <li>▶ Regular or systematic failure to action discretionary items identified through internal or external review</li> </ul>
7.6.6	AICS may fail to provide adequate services to Mirrabooka in accordance with contracted requirements	<i>Lagging indicators:</i> <ul style="list-style-type: none"> <li>▶ Mirrabooka Audit Committee identifies material or unaddressed non-compliance with services agreement</li> </ul>
7.6.7	Insufficient insurance cover leads to financial loss	<i>Lagging indicators:</i> <ul style="list-style-type: none"> <li>▶ Claims made where losses incurred were greater than the amount of insurance payment received</li> </ul> <i>Leading indicators:</i> <ul style="list-style-type: none"> <li>▶ Appropriate insurance cover not maintained</li> </ul>
7.6.8	IT systems may be inadequate or outmoded.	<i>Leading indicators:</i> <ul style="list-style-type: none"> <li>▶ IT systems or software no longer supported by vendors with no contingency plans in place.</li> <li>▶ Number of Sev 1 failures of IT systems</li> </ul>
7.6.9	Loss of IT service provider	<i>Lagging indicators:</i> <ul style="list-style-type: none"> <li>▶ IT systems unavailable or support unresponsive</li> </ul> <i>Leading indicators:</i> <ul style="list-style-type: none"> <li>▶ Alternative contingency plans not defined for key service providers;</li> </ul>
7.6.10	Availability of Funding / Increased interest costs on debt exposures due to interest rate rises	<i>Leading indicators:</i> <ul style="list-style-type: none"> <li>▶ Reluctance of banks to extend debt facilities</li> </ul>
7.6.11	AFIC, with its controlling interest may apply undue pressure on AICS to provide preferential treatment to the detriment of the minority shareholder and other LIC's which use their services.	<i>Leading indicators:</i> <ul style="list-style-type: none"> <li>▶ DJW, MIR or AMH Audit Committee identifies material or unaddressed non-compliance with services agreement</li> </ul>

Note - The outcomes of the audit work performed by EY in accordance with ASAE 3150 Assurance Engagements on Controls also inform the assessment of risks.

## Appendix B. Key Risk Management Definitions

<b>ASD</b>	Australian Security Directorate
<b>Breach</b>	Where an incident has, or may have a regulatory impact, then timelines apply in managing the incident so that the incident can be reported to regulators (if required) in accordance with the law.
<b>Consequence</b>	Impact or outcome of a risk if it occurs e.g., loss, injury, disadvantage. Usually measured as the worst plausible case for losses or the best possible case for opportunities.
<b>Control</b>	A measure that is modifying risk. Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organises, and directs the performance of sufficient controls to provide reasonable assurance that objectives and goals will be achieved. Controls can be preventative, detective or directive.
<b>CSN</b>	Common Shareholder Number. Identifies the Company's holdings on the NZX.
<b>Effectiveness</b>	Effectiveness of Risk Management, control, and governance processes is present if processes are operating in a manner that provides reasonable assurance that the organisation's objectives and goals will be achieved.
<b>Event</b>	An occurrence (often due to control failures) that could result in either a financial, reputational, customer, system or regulatory/legal impact, or is a near miss
<b>Issue</b>	A control weakness – no negative event need have happened, but an event is usually in indicator of an issue.
<b>Key Risk Indicators</b>	A metric for a particular risk which shows a potential change in likelihood or impact of that risk occurring. AICS aim to have a combination of lagging and leading indicators.
<b>Lag Indicators</b>	Lagging indicators provide information on past events or issues.
<b>Lead Indicators</b>	Leading indicators are forward looking and help detect future changes in probability of a risk materialising.
<b>Likelihood</b>	Chance that a particular risk will occur.
<b>Opportunity</b>	Uncertain beneficial event or condition that, if it occurs, will result in favourable outcomes
<b>Residual Risk</b>	Risk level remaining after agreed actions and controls have been implemented.
<b>Risk</b>	The chance of something happening that will have an impact upon objectives. It is measured in terms of consequence and likelihood.
<b>Risk Appetite</b>	The amount of risk AICS is willing to accept in delivering its strategic objectives.
<b>Risk Management</b>	Coordinated activities to direct and control the company with regard to risk.

<b>Risk Management Framework</b>	Set of components that provide the foundations and corporate arrangements for designing, implementing, monitoring, reviewing and continually improving Risk Management throughout the company.
<b>Risk Management Policy</b>	Statement of the overall intentions and direction of the company related to Risk Management.
<b>Risk Management Process</b>	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk.
<b>Risk Treatment</b>	Process to modify risk (avoid, transfer, control, mitigate or consciously accept).
<b>Risk Appetite</b>	The level of risk that AICS is willing to accept in the pursuit of objectives