Australian Foundation Investment Company

Risk Management Policy & Framework

May 2026

Table of Contents:

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 ('DJW');
- Mirrabooka Investments Limited ('Mirrabooka'); and
- AMCIL Limited ('AMCIL').

AICS and the Board of AFIC 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.

The Board and Audit Committee of AFI 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 AFI 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 AFI Audit Committee does not consider it necessary for AFI 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. AFI and AICS also use other external parties to review various aspects of risk and risk management – e.g. 4Walls and InphySec/Fujitsu for cyber security.

AICS and AFI, by their nature, are not directly exposed to material economic, environmental and social sustainability risks, but the AFI 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 AFI and the measures established by them to manage and monitor the factors that could potentially prevent them from achieving business objectives.

Senior management and the Boards demonstrate commitment to risk management through clear mandates, alignment of objectives, and the provision of resources. Integration of risk considerations into planning and reporting processes ensures that risk management is part of strategic and operational decision-making. 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 AFI to enable it to meet its obligations and objectives.
- Increase the likelihood that AICS and AFI 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 AFI; and a strong risk culture is well-entrenched.
- 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).

In meeting these objectives, AICS and AFI align their framework with *ISO 31000:2018 Risk Management — Guidelines* and the *ASX Corporate Governance Principles* to ensure integration of risk management into governance and decision-making processes.

This document provides an overview of the framework within AICS and AFI 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 AICS and AFI are responsible for ensuring that risk management is integrated with corporate governance, strategy development and performance management. The Framework provides the foundation and arrangements to embed risk management into decision-making at all levels by defining accountability, resources, communication and reporting mechanisms.

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.

The Framework is reviewed in accordance with the continuous improvement principles mandated by AS/NZS ISO 31000:2018 and monitored against benchmarks set out in APRA CPS 230 (2025) where applicable.

In addition, the Executive Management Team ('EMT'), Investment Team and Portfolio Manager and the Investment Committee of AFI 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 AFI (and twice for AICS), and by the Investment Committee (for AFI) 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 AFI is based on the AS/NZS ISO 31000:2018 Risk Management – Guidelines which emphasises leadership and integration of risk management into governance, strategy and decision-making processes.

Continuous improvement is maintained through annual review of the Risk Management Framework and lessons learned from incidents and assurance activities.

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 AFI's strategies and the achievement of goals. AICS and AFI 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 AFI.

Review of policy

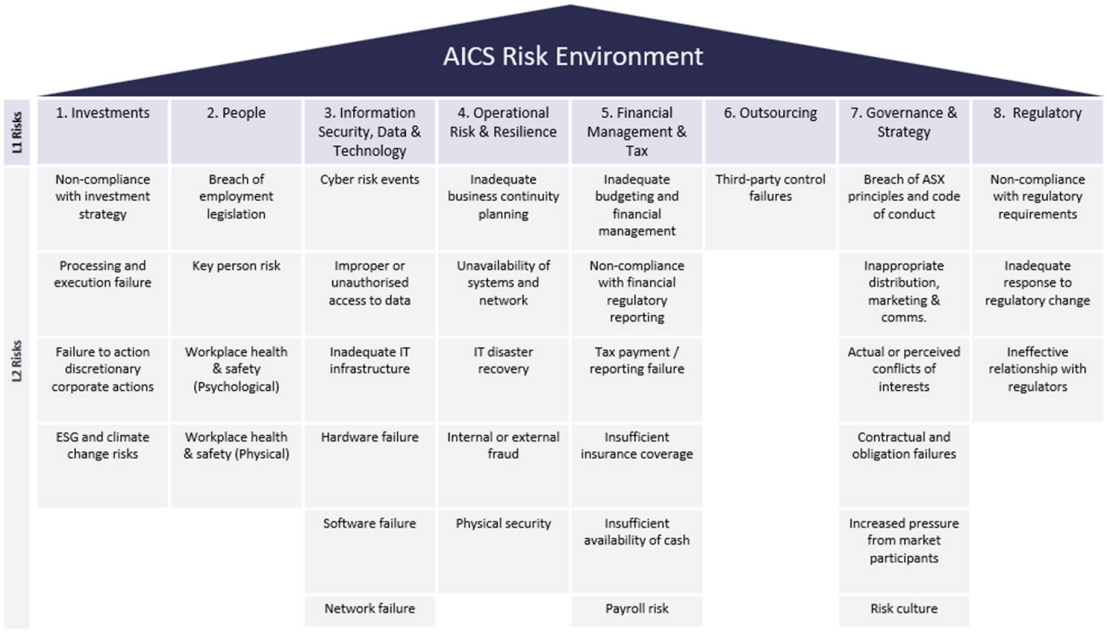
This policy will be reviewed internally on an on-going basis and by external experts on a periodic basis. Responsibility for ensuring that this review is performed rests with the CFO / Risk Officer. Any significant changes are provided to the Audit Committees of AICS and AFI for review and formal approval.

5. Material risks

AICS has adopted the Operational Risk data Exchange Association (ORX)'s Reference Taxonomy for Risk Identification and Categorisation. This is a standard used widely through the Financial Services Industry. AICS recognises the following Level 1 Risks (or risk categories) that are associated with its activity:

L1 Risk Category	Definition
1. Investment	A risk that investment decisions, or failures in the operational processes supporting those decisions, may lead to sub-optimal performance.
2. People	Lack of appropriate employment practices and attraction and retention policies leading to unwanted employee departures. This also includes the risk of a failure to maintain a healthy risk culture.
3. Information Security, Data & Technology	A risk of financial losses, disruption or damage to the reputation of AICS and AFI, 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.
4. Operational Risk & Resilience	A risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from internal and external events.
5. Financial management	The risk of financial loss to members resulting from internal or external factors or inadequate financial controls.
6. Outsourcing	A risk of direct or indirect loss due to service providers' failure to comply with service level agreements and standards.
7. Governance & Strategy	A risk of poor governance or decline in competitive advantage leading to a reduction in investor confidence and decline in market share and share price.
8. Regulatory	A risk of losses incurred by AFI as a result of failure (or perceived failure) to comply with relevant laws and regulations.

These Level 1 Risks are further categorised as Level 2 risks, as depicted in the diagram below:



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 AFI 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, which is generally not greater than a "medium" level of risk. This RAS is separately maintained within the 'Risk Profile and Risk Register' Summary Report.

The Risk Profile and Risk Register outlines the material Level 1 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 AFI'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 AFI'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 also consider emerging ESG and climate-related financial disclosures consistent with AASB S2 frameworks when setting risk appetite.

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 AFI'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 AFI 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 AFI aim to ensure continuous improvement of their risk management and governance framework and these are reported through to the Audit Committees.

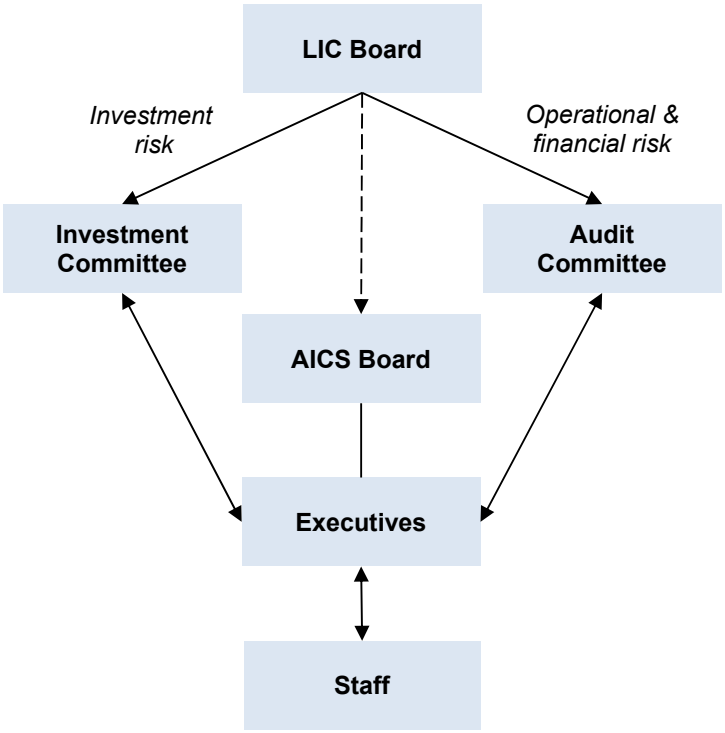
Those risks that are acceptable to the Board will be subject to regular review and reporting. Key high-level risks, together with materially relevant subordinate risks, will be subject to review by the Internal Auditor. The results of these reviews are presented to the Audit Committees and to the Boards, 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, AFI. 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 AFI:



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

Board of Directors	The Board of Directors of AFI holds the following responsibilities: ▪ To establish policies for the oversight and management of material business risks, and disclose a summary of these policies. ▪ 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). ▪ To determine the overarching risk appetite (also for AICS) ▪ 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. ▪ To review, at least annually, the policies and procedures on risk oversight and management as approved by the Audit Committee (also for AICS). ▪ To ensure that risk management is integrated with strategy setting, business planning and performance evaluation in line with AS/NZS ISO 31000:2018 Principle 2

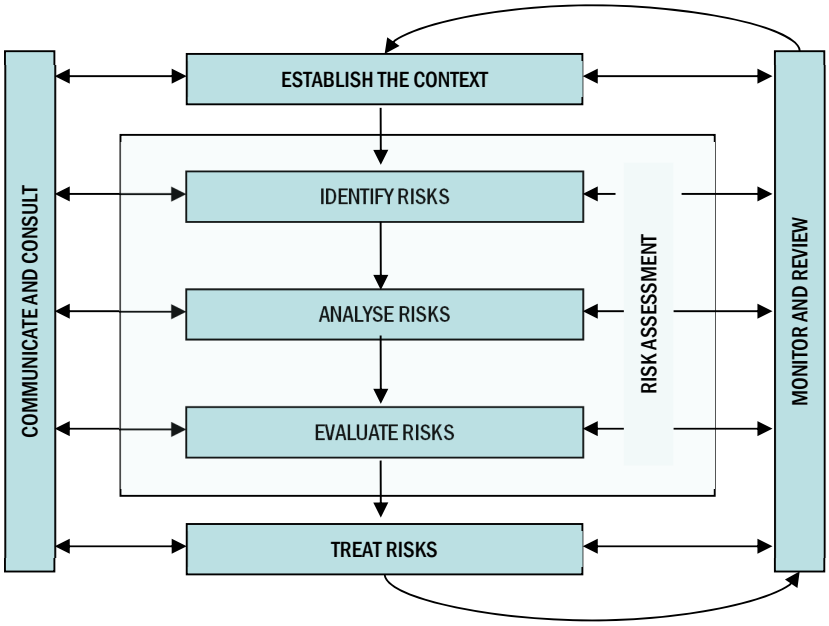
Audit Committee	The Audit Committee of each Company (AICS and AFI) has the following responsibilities: ► To review and approve the Risk Management Policy & Framework. ► To report to the Board on the process and responsibilities for managing risk. ► To confirm that appropriate risk management methodologies and practices have been implemented across the organisation through receiving relevant risk reporting from the EMT and internal audit, and external reports where considered appropriate: ► To report to the Board on the organisation's adherence to the Risk Management Policy & Framework and to report on material matters, findings and recommendations, pertaining to risk management and the internal compliance and control framework. ► 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. ► To review the policies and practices in meeting its compliance obligations with regards to laws, regulations, codes and company policies. 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 AFI has access to them as needed.
Investment Committee	The Investment Committee has the following responsibilities: ► Investment decisions including adding new investments, increasing or reducing existing investments and disposals and review and authorise transactions. ► Set, monitor and review authorisation limits for the Investment Team. ► Review recommendations for voting instructions. ► Review portfolios with regards to weightings and investment risk (including economic, environmental and social sustainability risks) and concentration risk. ► Monitor option coverage and the risks of having stock being called away or put stock. ► Review liquidity and contingencies. ► Review and monitor the implementation of the investment delegation of authority to assess ongoing effectiveness. ► Report to the Board any breaches of delegation. The CIO (Chief Investment Officer – currently the CEO) ensures that the investments are made in accordance with the delegated authorities.
Managing Director & Chief Financial Officer / Risk Officer	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 AFI's Risk Management Policy & Framework. This is achieved through the development of an appropriate infrastructure to identify, measure, manage and report risks. The Managing Director is ultimately accountable for managing material risks in accordance with the approved Risk Management Policy and risk appetite. The CFO/Risk Officer has the delegated authority (and responsibility) for the system of risk oversight and management and internal control. The CFO / Risk Officer performs the following risk management functions: ► Ensuring risk management processes are established and operating effectively. ► Maintaining a central risk register for recording risks identified and the mitigating strategies throughout AICS and the investment companies. ► 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. ► Summarising and prioritising risks for the Audit Committee. ► Monitoring the performance of outsourced service providers and assessing their risk management, particularly with regards to the provision of IT. ► Recommending education and training in risk practices and processes.

	► Ownership of the risk register and communication of required measures to all staff.
EMT	Responsibility for risk management rests with each member of the EMT who is to lead risk management processes within AICS. Key responsibilities include: ► Implementing the Risk Management Policy & Framework and processes. ► Considering key risks as part of the strategic and business planning processes. ► Reporting risk events in accordance with the reporting process included in the framework. ► Reporting to AFI and to the Board of AICS on the risk profiles and risk mitigation plans of AICS, as appropriate. ► Implementing measures to appropriately resolve risk issues as they are identified, within their respective lines and actions fully completed in a timely manner. ► Maintaining and promoting a culture of risk management and compliance. ► Raising awareness of the relevant risks to staff and ensuring compliance with AICS policy, procedures and controls. ► Ensuring risk management performance indicators align with corporate performance indicators. ► Ensuring that the necessary resources are allocated to risk management.
Employees	Employees are responsible for: ► 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. ► Performing duties without risk to other employees, AICS customers, AFI shareholders or the community in general or to their own health and safety. ► Complying with operational policies procedures and risk mitigation controls within daily tasks in AICS operations. ► Attending and completing required training ► Identifying and escalating any potential risks and issues in accordance with the Risk Management Policy & Framework. ► Providing risk management related information, as requested by their manager. ► 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. ► Perform ad-hoc testing of controls not covered as part of ASAE 3150 review as needed.
Company Secretary & Compliance	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 AFI Audit Committee. 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.
Internal Auditor	Internal audit performs reviews which are aligned to the key risks in AICS and AFI reporting to the Audit Committee and the Board on the: ► Periodic assessment and update of AICS Risk Register. ► 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. ► Reviews included in the annual internal audit plan as approved by the Audit Committee.
External Auditor	External auditor's responsibilities include: ► To express a review conclusion on the half-year financial report of AFI 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 AFI in accordance with Australian Auditing Standards.

	► To perform an external audit of AFSL compliance by AICS. ► To provide an extensive review and half-yearly sign-off of tax balances.
Tax Agent	The Tax Agent's responsibilities include: ► To review taxation information and prepare tax returns

8. Risk Management Methodology

The Risk Management Policy & Framework has been developed to take into account the guidelines outlined in AS / NZS ISO 31000: 2018 Risk Management – Guidelines and utilising guidance from its internal and external auditors.
This policy also cross-references the Australian Signals Directorate's *Essential Eight* (2023.1) for cyber maturity.
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 AFI. 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 Communication and Consultation

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.

8.2 Scope, Context and Criteria

The Scope, Context and Criteria define the internal and external parameters to be considered and set the criteria against which risk will be evaluated (including risk appetite, likelihood and consequence scales)

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 and criteria includes consideration of the following:

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

8.3 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 AFI'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 AFI 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 AFI 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.

8.4 Evaluate and Treat 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 Reasonable Worst-Case Consequence (RWCC) or worst-case scenario is anticipated. Each risk is assessed in terms of:

- The likelihood of an event occurring.
- The impact or consequences of the identified risk if it occurred – together, the 'inherent' risk.
- Existing controls and the success of those controls in mitigating risk.
- 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	▸ Is expected to occur in most circumstances, or ▸ Has more than 90% chance of occurring in the next 12 months
4	Likely	▸ Will probably occur in most circumstances, or ▸ Has 51% - 90% chance of occurring within the next 12 months.
3	Possible	▸ Might occur at some time, or ▸ Has 11% - 50% chance of occurring within the next 12 months
2	Unlikely	▸ May occur at some time, or ▸ Has 6 - 10% chance of occurring within the next 12 months.
1	Rare	▸ May occur only in exceptional circumstances, or ▸ Has less than 5% chance of occurring within the next 12 months.

Consequence:

The risks facing AICS and AFI 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 AFI Board (see Section 8.5). Consequence ratings are neither exclusive nor comprehensive (i.e. significant expense may be incurred without significant negative publicity):

The 5 consequence levels utilised are : Critical, Major, Moderate, Minor and Insignificant. They are each assessed across Reputation impact, Regulatory Impact, Business Impact, Financial Impact and Shareholder Impact.

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

Control Design

Control activities are procedures and tasks established and implemented as part of AICS and AFI's 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.

AICS/AFI control design includes a control, description, and (where appropriate) objective, owner, and effectiveness rating.

Controls can be preventative (stops a risk), detective (identifies when a risk has become an event) or directive (guidance on what should occur e.g. policies and training):

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.

Key Controls

The following definition has been adopted to support the classification of controls as key and non-key.

A key control is fundamental to reducing the likelihood and/or impact of a risk, and/or for meeting compliance with regulatory, legislative or contractual requirements. It plays a central role in preventing, detecting or managing issues before they materialise and cause significant, systemic or pervasive harm to AICS and its listed investment companies.

Key controls are typically characterised by the following:

- ***High impact if the control fails*** – Failure of a key control would significantly increase the risk of a material issue, error or regulatory breach.
- ***Limited reliance on other controls*** – If the key control does not operate as intended, other controls are unlikely to sufficiently prevent or detect the issue on a timely basis.

- ***Primary risk response*** – The key control represents the main method for managing the material risk within its defined risk appetite and tolerance.
- ***Critical to compliance*** – The key control is necessary to demonstrate compliance with regulatory, legislative or contractual requirements.

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 controls as outlined in the Risk Register, and consideration as to whether others need to be included, 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 responsible control owners and review of any relevant third-party reporting (e.g. internal audit reporting and ASAE 3150 controls audit). The date of such an effectiveness review is either the date of the last Audit Committee at which the Risk Register and this Framework are reviewed, or as documented elsewhere.

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	► 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).
2	Partially Effective	► 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 ► 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.
3	Ineffective	► 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 ► Controls are subject to major change, or ► Controls are in the process of being implemented and their effectiveness cannot be confirmed.

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:

Risk levels (e.g. "Medium") are also defined with reference to the Key Risk Indicators for individual risks as specified in the Risk Register.

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

8.5 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 AFI 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.

Option	Description
Avoid	Avoid and abstain from an activity when the accumulative opportunity for gain is outweighed by the accumulative opportunity for loss.
Mitigation Controls	Implementation of new controls or strengthening existing controls.
Transference	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).
Accept	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.

8.6 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

8.7 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:

Activity	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

8.8 Continuous Improvement

AICS and AFI are committed to continual improvement of the Risk Management Framework through regular independent assurance reviews, benchmarking and analysis of control deficiencies to ensure ongoing alignment to ISO 31000:2018.

The Framework and process are evaluated for effectiveness and performance at least annually. Findings from internal audit, incident analysis and external reviews inform corrective and preventive actions. Lessons learned are communicated to the Board and used to update risk criteria, methods and training.

8.9 Recording and Reporting

AICS and AFI maintain records required to meet their various obligations – including requirements related to taxation, Financial Services Licence, privacy, ASIC and ASX.

A breach register is maintained and reviewed where appropriate, as are key risk incidents, which are recorded and reported to the relevant Committee.

Risk management activities and outcomes must be documented and reported consistently to enable accountability and transparency. Reports should describe identified risks, analysis, decisions, actions, and performance metrics. AICS will retain risk records in accordance with its governance and records management policy.

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) Insufficient availability of cash (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 form the trading or investment portfolios and dividends receivable).

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

b) Investment risk

The Investment Committee reviews AFI'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 AFI are committed to a risk-aware culture that recognises human and cultural factors as integral to effective risk manag ement (AS/NZS ISO 31000:2018 Principle H).

Behavioural expectations include accountability for controls, open communication of risks, and proactive learning from incidents.

The Boards recognise that this requires that leadership demonstrates ethical and risk-informed decision-making.

They also seek to ensure compliance with the applicable regulatory requirements and internal policies and procedures. AICS' and AFI'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 has 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

Detailed risk indicators are maintained as part of the Risk Register and reviewed by the CFO/Risk Officer

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

ASD	Australian Signals Directorate
Breach	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.
Consequence	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.
Control	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.
CSN	Common Shareholder Number. Identifies the Company's holdings on the NZX.
Effectiveness	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.
Event	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
Issue	A control weakness – no negative event need have happened, but an event is usually in indicator of an issue.
Key Risk Indicators	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.
Lag indicators	Lagging indicators provide information on past events or issues.
Lead indicators	Leading indicators are forward looking and help detect future changes in probability of a risk materialising.
Likelihood	Chance that a particular risk will occur.
Opportunity	Uncertain beneficial event or condition that, if it occurs, will result in favourable outcomes
Residual Risk	Risk level remaining after agreed actions and controls have been implemented.
Risk	The chance of something happening that will have an impact upon objectives. It is measured in terms of consequence and likelihood.
Risk Appetite	The amount/level of risk AICS is willing to accept in delivering its strategic objectives.
Risk Management	Coordinated activities to direct and control the company with regard to risk.
Risk Management Framework	Set of components that provide the foundations and organisational arrangements for integrating, designing, impl ementing, evaluating and continually improving risk management throughout the organisation. (*ISO 31000:2018 Clause 5*)
Risk Management Policy	Statement of the overall intentions and direction of the company related to Risk Management.

Risk Management Process	Systematic application of policies and procedures to the activities of communicating and consulting, defining scope, context and criteria, assessing, treating, monitoring, reviewing, recording and reporting risk
Risk Treatment	Process to modify risk (avoid, transfer, control, mitigate or consciously accept).