

Risk Management Policy

Document Owner:

General Manager Operations

Contributors:

General Manager Finance and Risk
General Manager Corporate Strategy
Head of Portfolio Risk & Compliance
Head of Enterprise Risk
General Counsel
Head of Tax

Document History

Version	Date	Changes/Modifications	Approved By	Status
1.0	1 July 2011			Final
2	10 Sep 2012	Annual Review.	Board	Final
2A	13 Feb 2014	Responsibilities updated, addition of Internal Audit charter and Model review process	CEO	Final
3	July 2014	Biennial policy update	Board	Final
3A	28 Oct 2014	Updates to Schedules 3B and 3C	CEO	Final
4	17 Jun 2015	Updates to Schedule 2 (Risk Appetite Statement) due to 2015 Investments Constraints Review. Also, some minor tidy-ups.	Board	Final
4A	7 Aug 2015	Update to Schedule 7 (Operational Risk - Fraud Risk Framework) to include bribery and corruption; Revision to Schedule 8 (Operational Risk - Taxation Risk Management Framework). Tidy-up to remove reference to Risk Records.	CEO	Final
5	15 Sep 2015	Updated to Schedule 7 to reflect recommendations from the audits of Bribery and Corruption and Fraud risk practices.	Board	Final
6	21 Jun 2016	Biennial policy update	Board	Final
7	20 Sep 2016	Updated Schedule 2 (Risk Appetite Statement) and Schedule 4 (Risk Assessment Framework)	Board	Final
7A	8 Dec 2016	Update to Schedule 12: Legislative and Regulatory Risk – Legislative Compliance Framework	CEO	Final
8	21 Feb 2017	Amended to make the RAS consistent with the PCIMS Policy; Updates to Schedule 1 (Responsibilities); Update Policy Diagram	Board / CEO	Final

9	14 Mar 2017	Change to the Internal Audit Charter - Clause 5	Board	Final
10	13 Apr 2017	Change to Schedule 2 (Risk Appetite Statement) and Schedule 4 (Risk Assessment Framework)	Board	Final
10A	24 May 2017	Change to Schedule 3A (Proper Instructions Framework) required for securities lending.	CEO	Final
10B	13 Jun 2017	Change to Schedule 5 (Internal Audit Charter) – Internal Audit Evaluation.	Board	Final
11	6 Aug 2019	General refresh/review by policy owner and schedule owners	Board	Final
11A	25 Spt 2019	Update to Schedule 3A (Proper Instructions Framework)	CEO	Final
12	11 Dec 2019	Update to Schedule 5 (Internal Audit Charter)	Board	Final
13	26 Feb 2020	Updates to Background, Schedule 1, Schedule 9, and Schedule 13 to reflect changes in the Internal Learning Opportunities Process	Board	Final
13A	11 Mar 2020	Updates Schedule 1 (Responsibilities), Schedule 3A (Proper Instructions Framework), and Schedule 10B (Information Security Framework)	CEO	Final
13B	13 Mar 2020	Updates to Schedule 1, Schedule 9, and Schedule 13 to reflect changes in the Internal Learning Opportunities Process	CEO	Final
14	26 Nov 2020	Updates to Schedule 2 (Appendix 1 - Risk Appetite for Investments)	Board	Final

Contents

1	Background	4
2	Objective	4
3	Definitions	4
4	Scope	4
5	Delegations and Authorities	5
6	Risk Appetite Statement	6
7	Risk Management Framework	6
8	Reporting	8
9	Control Section.....	9
Schedule 1:	Responsibilities.....	10
Schedule 2:	Risk Appetite Statement.....	12
Schedule 3:	Risk Management Framework	19
Schedule 4:	Risk Assessment Framework	30
Schedule 5	Internal Audit Charter	33
Schedule 6:	Risk to Strategy	37
Schedule 7:	Operational Risk - Fraud, Bribery and Corruption Risk Framework.....	39
Schedule 8:	Operational Risk - Tax Risk Management Framework	43
Schedule 9:	Operational Risk - Internal Learning Opportunities Process	45
Schedule 10A:	Operational Risk - Business Continuity Management	47
Schedule 10B:	Information Security Framework.....	48
Schedule 11:	Operational Risk - Model Oversight Process	50
Schedule 12:	Legislative and Regulatory Risk - Legislative Compliance Framework.....	52
Schedule 13:	Reporting Framework	60

1 Background

- 1.1 Risk is an integral part of doing business. We are committed to a business strategy that supports the proactive identification, assessment, measurement, management and reporting of risk, and uses risk information to enhance decision-making and develop appropriate management strategies.
- 1.2 Risk cannot be eliminated, but it must be clearly understood to ensure that the risks taken are appropriate for the returns anticipated.
- 1.3 Risk is any internal or external factor which poses a potential threat or opportunity to our ability to fulfil our purpose. Risk is characterised by uncertainty and is measured in terms of the impact of an event and the likelihood of its occurrence.
- 1.4 We have a decentralised approach to risk management, and operate on a 'multiple lines of defence' basis. This ensures that responsibility and accountability for risk management is at each business unit level, where risk is seen as part of the overall business process and a robust framework of identification, evaluation, monitoring and control exists. The Enterprise Risk team facilitate this approach.
- 1.5 When developing this policy we were cognisant of the Risk Management principles and guidelines promulgated by the Australian/New Zealand Standard (AS/NZS ISO 31000:2009).

2 Objective

- 2.1 To implement effective controls and frameworks to ensure risks are managed effectively and in compliance with our governance and legislative requirements.

3 Definitions

- 3.1 To aid with interpretation of this policy we have a Glossary of Terms, which defines all technical terms used in our policy documents. In this policy the first instance of any such defined term is highlighted in bold. References to other documents are italicised.

4 Scope

- 4.1 Five major risks are outlined below. The first three risks are within scope of this policy:

<i>Risk</i>	<i>Definition</i>	<i>Scope of this policy</i>
1. Risk to Strategy	The risk that we make inappropriate strategic choices or are unable to successfully implement selected strategies.	<u>In scope</u> . Risk management processes are integrated into Strategic Planning (Schedule 6).
2. Operational risk	The risk of loss from inadequate or failed internal processes, people and systems or from external factors.	<u>In scope</u> . Fraud, tax, learning and opportunities, business continuity, information security, and model oversight frameworks (Schedules 3, 7, 8, 9, 10, and 11 respectively).
3. Legislative and regulatory risk	The risk of loss due to non-compliance with laws, rules and regulations and prescribed industry practice.	<u>In scope</u> . The legislative compliance framework (Schedule 12).
4. Investment risk	The standard deviation of expected returns.	<u>In scope</u> . Risk appetite statement (Schedule 2).

		<p><u>Out of scope</u>. Investment controls and frameworks to operate within the risk appetite statement. These are addressed through:</p> <ul style="list-style-type: none"> • <i>Statement of Investment Policies, Standards and Procedures</i> • <i>Investment Risk Allocation Policy</i> • <i>Externally Managed Investments Policy</i> • <i>Direct Investments Policy</i> • <i>Strategic Tilting Policy</i> • <i>Portfolio Completion & Internally Managed Securities Policy</i> • <i>Derivatives Policy</i> • <i>Investment Valuation Policy</i>
5. Reputation risk	Risk of loss of reputation or credibility sufficient to have a commercial or other practical impact due to internal or external factors.	<p><u>Out of scope</u>¹. Addressed through:</p> <ul style="list-style-type: none"> • <i>Communications Policy</i> • Responsible investments standards included in the <i>Statement of Investment Policies, Standards and Procedures</i> • <i>Direct Investment Policy</i> in respect of New Zealand direct investments <p>¹ although reputation risk is not directly covered by this policy, controls in this policy do by their nature seek to minimize the threat of reputation risk.</p>

- 4.2 While this policy sets Investment and Reputational risks as out of scope, these risks are addressed from an enterprise-wide level within the Enterprise Risk Report and Risk Register frameworks that assist the Board's understanding of the risks that we face.

5 Delegations and Authorities

- 5.1 The *Delegations Policy* governs the delegations and authorities that apply in all policy documents. In the event of any discrepancy between this policy and the *Delegations Policy* the *Delegations Policy* will prevail.
- 5.2 The Board has reserved certain matters either to itself, a committee of the Board or the Chief Executive. All other matters are delegated to the Chief Executive who may sub-delegate them to Guardians' staff. All delegates and sub-delegates must exercise their authorities in compliance with the general conditions of delegation and sub-delegation set out in Schedule 2 of the *Delegations Policy*.
- 5.3 There are certain responsibilities inherent under this policy. Those responsibilities, and the person responsible for them, are outlined in Schedule 1.

6 Risk Appetite Statement

Our risk appetite statement sets out the Board's approach to risk management and return. The risk appetite reflects how much risk we are willing to take in the pursuit of our strategic objectives.

The constraints then provide a guide from the Board through:

- Risk Appetite: the overall amount of risk we are willing to take in pursuit of our strategic objectives;
- Risk Limits: the limits we establish to ensure our risk profile stays within the levels set in the risk appetite statement.

6.1 We will maintain and adhere to a Risk Appetite Statement.

6.2 The Risk Appetite Statement must be approved by the Board.

6.3 An outline of the Risk Appetite Statement must be maintained in Schedule 2.

7 Risk Management Framework

The objective of our Risk Management framework is to ensure we operate within our agreed risk limits. We do this by the:

- effective and efficient continuity of operations;
- safeguarding of our assets;
- preservation and enhancement of our reputation;
- reliability of internal and external reporting;
- compliance with applicable laws and regulations.

Creating and maintaining a culture consistent with our risk management framework is an important element of operational risk management, as are our selection and recruitment processes.

7.1 We will maintain and adhere to a risk management framework that ensures:

- the risk management process is evident whenever key decisions are made;
- risks are identified and evaluated;
- effective responses and control activities are developed for these risks; and
- appropriate monitoring and timely re-evaluation of risks.

7.2 An outline of the risk management framework as it exists in current practice must be maintained in Schedule 3.

7.3 An outline of the framework for assessing the likelihood and consequence of each identified risk as it exists in current practice must be maintained in Schedule 4.

7.4 An outline of the Board Audit Committee's Internal Audit charter as it exists in current practice must be maintained in Schedule 5.

Strategic Risk

7.5 We will maintain and adhere to a strategic planning and implementation framework that supports achievement of strategic goals and objectives and minimises the adverse impact of undesirable incidents or unexpected adverse changes in the external business environment.

7.6 An outline of the strategic planning and implementation framework as it exists in current practice must be maintained in Schedule 6.

Operational Risk

- 7.7 We will manage operational risk through business procedures focussed on identifying risks and implementing effective controls as well as conducting internal audit reviews and obtaining attestations.
- 7.8 We will maintain and adhere to a robust key person risk framework which ensures:
- We identify both temporary and permanent cover required for key roles in the event of loss of staff;
 - For roles requiring immediate cover we maintain a list of internal resource and/or external consultants that could be used as cover in the event of loss of staff; and
 - We review key person risk and mitigation measures at least annually and report to the Employee Policy and Remuneration Committee.
- 7.9 We will maintain and adhere to a robust fraud management framework in order to minimise the potential for fraud and unethical or corrupt behaviour, and to ensure any instances are identified and properly managed.
- 7.10 An outline of the fraud management framework as it exists in current practice must be maintained in Schedule 7.
- 7.11 We will maintain and adhere to a tax risk management framework which ensures:
- Financial reporting for tax is prepared accurately and the correct amount of tax is paid in all jurisdictions in compliance with tax law and tax practice;
 - Tax planning is consistent with any legislative or Ministerial directive;
 - All unusual and material tax issues are signed off by professional tax advisors and if appropriate, and possible, by tax authorities; and
 - Tax leakage from the Fund is effectively managed without undue risk (including financial and reputation risk) to the Guardians.
- 7.12 An outline of the tax risk management framework as it exists in current practice must be maintained in Schedule 8.
- 7.13 To enable continuous improvement of risk management practices, we will operate an open, honest, no-blame culture and ensure Learning & Opportunities reports are submitted, analysed and actions resolved on a timely basis.
- 7.14 An outline of the Learning & Opportunities Process as it exists in current practice must be maintained in Schedule 9.
- 7.15 We will maintain a cost effective Business Continuity Management (BCM) framework to:
- Protect the welfare and safety of staff at all times;
 - Provide timely availability of key resources to operate critical business processes;
 - Protect our resources; and
 - Protect our reputation.

- 7.16 An outline of the BCM framework as it exists in current practice must be maintained in Schedule 10A.
- 7.17 The objective of the Policy relating to information security is to maintain an effective information security framework that secures systems and information through three key initiatives, Security, Vigilance and Resilience:
- Security – Provide systems and controls that secure systems and information to appropriate standards.
 - Vigilance – Monitoring and protecting information and systems, whether provided by third parties or developed internally, to ensure systems and information are secure.
 - Resilience – Provide an incident response solution that seeks to enable the Guardians to restart operations within the recovery time objective should an incident compromise its systems.
- 7.18 The Guardians has established a framework for information security governance, management, operations and assurance. This framework is summarised in Schedule 10B of this policy.
- 7.19 The Guardians will identify, assess, and mitigate information security risks according to the Guardians risk management process.
- 7.20 The Guardians will consider the recommendations of the NZ Information Security Manual (NZISM) and the Protective Security Requirements (PSR) when designing and assessing security processes and controls. However, the Guardians is not mandated to comply with or to report its conformance with NZISM or PSR.
- 7.21 Any changes to the NZISM or PSR will be reviewed by Guardians management, and the NZISM/PSR mapping table in Schedule 10B will be updated, if necessary, within 90 days of the change. Management will determine whether any Guardians standards need to be added or revised based on the new NZISM or PSR guidance.

Legislative and Regulatory Risk

- 7.22 We will maintain and adhere to a Legislative Compliance framework that ensures compliance with all our legal obligations is embedded into the way we do business.
- 7.23 An outline of that framework, as it exists in current practice must be maintained in Schedule 12.

8 Reporting

- 8.1 We must report to the Board on the following matters:
- Performance against relevant risk limits (as per the risk appetite statement)
 - Internal audit plan and audit reports
 - Strategic plan and implementation
 - Fraud incidents and investigation reports
 - Tax position
 - Learning Opportunities
 - Cyber security dashboard
 - Enterprise risks

8.2 An outline of the reporting framework, as it exists in current practice must be maintained in Schedule 13.

8.3 We will report proposed material changes to the following schedules to the Board for their approval:

- Schedule 2: Risk Appetite Statement
- Schedule 3: Risk Management Framework
- Schedule 4: Risk Assessment Framework
- Schedule 5: Internal Audit Charter (to the Audit Committee)
- Schedule 13: Reporting Framework

8.4 We must report to the Board, for their information, material changes to the following schedules of this policy:

- Schedule 1: Responsibilities
- Schedule 3A: Proper Instructions Framework
- Schedule 3B: Standard Settlement Instructions and Payment Control Framework
- Schedule 3C – Foreign Currency Bank Account and Money Market Accounts Operating Framework
- Schedule 6: Risk to Strategy
- Schedule 7: Fraud Risk Framework
- Schedule 8: Tax Risk Management Framework
- Schedule 9: Learning Opportunities Process
- Schedule 10A: Business Continuity Management
- Schedule 10B: Information Security Framework
- Schedule 11: Model Oversight Framework
- Schedule 12: Legislative Compliance Framework

9 Control Section

Approved this June 2016, and amended 6 August 2019 and 26 February 2020

GM Operations _____

Chief Executive Officer _____

Board Chairman _____

Schedule 1: Responsibilities

GM Operations will:	<ul style="list-style-type: none"> ensure this policy is kept current and relevant to the activities being undertaken (including schedules 1, 10, 13) ensure this policy is reviewed every five years jointly (with the GM Finance and Risk) recommend PI Persons to the Chief Executive jointly (with the GM Finance and Risk) review all approved PI Persons annually review the Business Impact Analysis and update the BCP within 90 days of any major operational or system changes or at least on a two yearly basis. review and sign off the annual IT security assurance plan
Head of Strategic Development will:	<ul style="list-style-type: none"> ensure schedule 6 (strategic risk) is kept current and relevant to the activities being undertaken report the draft Strategic Plan annually to the Leadership Team and Board report progress with implementing the Strategic Plan biannually to the Leadership Team and Board
GM of Finance and Risk will:	<ul style="list-style-type: none"> ensure schedules 7 (fraud risk framework) and 8 (tax risk management framework), are kept current and relevant to the activities being undertaken jointly (with the GM Operations) recommend PI Persons to the Chief Executive jointly (with the GM Operations) review all approved PI Persons annually ensure that the form of compliance certification is reviewed at least annually report compliance certification six monthly, alternating between the Board and the Audit Committee ensure fraud training is conducted at least every two years
Head of Finance will:	<ul style="list-style-type: none"> review the Proper Instructions Framework annually
Head of Internal Audit will:	<ul style="list-style-type: none"> ensure schedule 5 (internal audit charter), is kept current and relevant to the activities being undertaken prepare an audit plan and report annually to the Audit Committee report audit findings to the subsequent Audit Committee meetings report fraud incidents immediately to the Chief Executive investigate and report fraud investigations to the Chief Executive and subsequent Audit Committee meeting
Fraud Control Officer will:	<ul style="list-style-type: none"> review Fraud, Bribery & Corruption Risk Assessment every two years
Head of Risk will:	<ul style="list-style-type: none"> report performance against relevant risk limits (as per Risk Appetite Statement) to each Board meeting ensure schedules 2, 3, 4, and 9 are kept current and relevant to the activities being undertaken report biannually to the Risk Committee, Leadership Team and the Board on Enterprise Risks review and sign off the annual IT security assurance plan report on material Learning Opportunities to the Chief Executive and subsequent Audit Committee meeting report on Learning Opportunities at each Audit Committee meeting report material policy breaches notified through the Learning Opportunities reporting process immediately to the RC and Board report all policy breaches notified through the Learning Opportunities reporting process to the subsequent Audit Committee meeting
Head of Tax will:	<ul style="list-style-type: none"> report on our tax position quarterly to the Audit Committee

Head of IT will:	<ul style="list-style-type: none"> manage the BCM programme to ensure capability is tested at least annually and plan remains current obtain assurances from key service partners that they have the requisite BCM capabilities in place review changes to the NZISM and PSR and, where appropriate, update the Information Security Framework within 90 days of notice report on cyber security preparedness and threats quarterly to the Risk Committee, Leadership Team and Board undertake responsibilities of the Chief Information Security Officer (CISO) as outlined in the NZISM prepare the annual information security strategy
IT Security Manager will:	<ul style="list-style-type: none"> undertake responsibilities of the Information Technology Security Manager (ITSM) as outlined in the NZISM prepare a monthly review of security metrics and the results of assurance activities
General Counsel will:	<ul style="list-style-type: none"> maintain a register of legislative compliance risks identify and respond to relevant changes or proposed changes to our legal obligations ensure the legislative compliance framework is reviewed at least every five years ensure schedule 12 (legislative compliance) is kept current maintain a record of policy owners report material changes to the schedules of this policy as part of the annual SIPSP review to the Risk Committee and Board meetings and under the no surprises protocol review and log all proposed policy changes
GM of Human Resources will:	<ul style="list-style-type: none"> maintain records of relevant compliance training review key person risk at least annually report assessment of key person risk annually to the ERPC
Chair of the RC will:	<ul style="list-style-type: none"> ensure Operational Risk Assessment (ORA) actions are closed ensure schedule 11 (model oversight framework) is kept current and relevant to the activities being undertaken
All GMs will:	<ul style="list-style-type: none"> confirm that key models within their area of responsibility are operating as intended.
All Managers will:	<ul style="list-style-type: none"> ensure all staff are trained and regularly updated regarding their responsibilities in suspected cases of fraud, including any legal or regulatory issues that may result
All staff will:	<ul style="list-style-type: none"> comply with all Guardians policies report any observed policy breaches or potential procedure and control issues in line with the Learning & Opportunities schedule or Code of Conduct assess and take prompt action to manage risks associated with their function

Responsibilities approved by Chief Executive on 21 June 2016, 6 August 2019, 17 December 2019, 11 March 2020, and 13 March 2020

Schedule 2: Risk Appetite Statement

1 The Guardians' Purpose

- 1.1 New Zealand Superannuation (or universal retirement income) is funded from general government revenue; that is, in large part from the taxes paid by New Zealanders. As the population ages in the decades ahead, it is anticipated that superannuation payments will occupy a substantially greater share of government revenue. The New Zealand Superannuation Fund (**Fund**) has been created to partially address this challenge.
- 1.2 The key objective under the governing Act is for the Guardians of the Fund (**Guardians**) to invest the Fund on a prudent, commercial basis, in a manner consistent with:
- Best-practice portfolio management; and
 - Maximising return without undue risk to the Fund as a whole; and
 - Avoiding prejudice to New Zealand's reputation as a responsible member of the world community.

2 Role of the Board of the Guardians

- 2.1 The Guardians is governed by a board (**Board**) which executes its responsibilities independently of the Crown.
- 2.2 The Board has developed a Risk Appetite Statement that:
- aligns with the key objective of the Guardians; and
 - provides guidance for developing the strategic objectives of the Guardians as set by the Board from time to time.

3 Role of Management of the Guardians

- 3.1 The Risk Appetite Statement guides management (**Management**) in:
- operating the Guardians;
 - managing and administering the Fund in accordance with the requirements of the Act; and
 - delivering on the strategic objectives of the Guardians as set by the Board.
- 3.2 The Fund is a collection of assets, which is consolidated into the Crown balance sheet. The Guardians manages and administers the Fund.

4 The Fund's fundamental risk

- 4.1 The fundamental risk that the Guardians face is that it fails to meet its institutional purpose, which is to meet its mandate under the Act.
- 4.2 If Government contributions are suspended or deferred then the Board believes that this will have a negative impact on the Guardians' ability to meet its purpose.
- 4.3 The sole activity of the Guardians is to invest the Fund. This includes allocating contributions by the Crown to various investment opportunities and collecting financial returns from those investments. These opportunities offer financial returns because the invested capital is ultimately directed towards economic enterprise: businesses that create the goods and services society needs.
- 4.4 However, enterprise can be more or less successful than anticipated, or even fail entirely. As a result, there is real economic risk, positive and negative, associated with the returns that an enterprise can offer for the use of an investor's capital. Investment risks and financial returns come hand in hand.

5 The Risk Appetite Statement and Risk Limits

- 5.1 The Board defines its risk appetite (**Risk Appetite**) as the amount of risk that the Board is willing or comfortable for Management to take in order to achieve the business goals of the Guardians. These are the risks the Board can tolerate.
- 5.2 The Board defines risk limits (**Risk Limits**) as a set of limits which the Board expects Management to operate within at all times; these limits reflect risks the Board cannot tolerate.
- 5.3 The Board expects Management to take steps to manage risks within the Board's Risk Appetite. The Board also expects that the Risk Limits will not be breached. If risks are taken beyond those Risk Limits and the Fund suffers severe losses as a result, then the Guardians may lose the confidence of its key stakeholders and, potentially, its license to operate the Fund.
- 5.4 The Guardians' seek exposure to the appropriate types of investment risk in order to deliver the financial returns necessary to meet its institutional purpose.

Risk	Definition	Appetite and Limits
Investment Risk	Investment Risk covers: <ul style="list-style-type: none"> • Periodic relative and absolute return parameters; • Fund absolute risk, active risk and the parameters of both; • Concentration limits; • Strategic tilting exposure; • Rebalancing absolute and relative risks; • Liquidity; and • Counterparty exposure. 	The Board has set out its Risk Appetite and Risk Limits for Investment Risk in Appendix 1

- 5.5 Business Risks cover the non-investment risk categories for which the Board has stated a Risk Appetite.
- 5.6 The Board has calibrated its Risk Appetite and Risk Limit for a number of its **Business Risks** (defined below) to align with a Moderate and Extreme risk level, as defined in our Risk Assessment Framework, as set out in Schedule 4.
- 5.7 As the Guardians executes its investment activities, it faces a wide variety of **Business Risks**. Therefore, once the Guardians has satisfactorily set a desired investment risk profile for the Fund as a whole, then it aims to manage its exposure to the associated Business Risks. It recognises that not all Business Risks have equal bearing on the Guardians' licence to operate. It also recognises that there is a cost-benefit analysis to apply in developing controls to appropriately manage Business Risks.
- 5.8 For example, the Board has an aspiration that the Guardians internally will have no serious harm injuries or deaths and, accordingly, the Board expects that it will apply strong controls to minimise risks in relation to health, safety and environmental risks. For the same reason, the Board actively monitors the health, safety and environmental governance compliance of certain investee companies as specifically reported to the Board.

Risk	Definition	Appetite and Limits
Business Risk	Business Risk covers: <ul style="list-style-type: none"> • Unintended profit or loss • Processes • Health and Safety • Business Continuity • Cyber • Staff • Conduct • Regulatory 	The Board has set out its Risk Appetite and Risk Limits for Business Risk in Appendix 3

6 Assessing Risks against Risk Appetite

- 6.1 The Board's Risk Appetite is applicable across the activities of the Guardians. This Risk Appetite is reflected in its Statement of Investment Policies, Standards and Procedures.
- 6.2 The Board expects Management to manage, measure and monitor the actual risk profile of the Guardians and Fund against its Risk Appetite and its Risk Limits.
- 6.3 The Board also actively monitors the health, safety and environmental governance compliance of certain investee companies as specifically reported to the Board.
- 6.4 Management will identify key risk indicators (and perform stress testing and scenario testing where appropriate) to assist the Board to assess the Fund and Guardians' exposure to the key risks that it has identified.
- 6.5 Clear accountability, monitoring and reporting to the Board provides good governance to effectively manage the key risks within the Risk Appetite Statement established by the Board. Management has primary responsibility for providing this governance.
- 6.6 The Board requires Management to effectively communicate this Risk Appetite Statement to all staff at the Guardians and external stakeholders.
- 6.7 In order to ensure the Guardians and the Fund are operating within the Risk Appetite Statement, the Guardians has developed a Risk Assessment Framework (**Framework**). The Framework is intended to ensure that risks are effectively identified, understood and treated by Management with appropriate accountability. Refer Schedule 4.

7 Review

- 7.1 The Board will review this Risk Appetite Statement and Limits at least every five years.

Appendix 1: Risk Appetite for Investments

The Investment Risk Appetite of the Fund is:

Metric	Investment Risk Limits	Measurement	Risk Limit	Reporting	Approved
Fund Level Risk					
Fund active risk	We expect the active risk of the Fund to be around 4% on average over the long term, and no more than 8% at any point in time.	As measured by the annualised standard deviation of the difference in the expected return of the actual portfolio from that of the reference portfolio	8%	Active risk is measured and monitored daily by Ops and reported monthly at each LT and at each Board meeting.	By Board April 2014
Fund one year downside risk	We have a 5% chance that the reference portfolio return over 1 year will be $\leq -18.4\%$. We have a 1% chance that the reference portfolio return over 1 year will be $\leq -30.4\%$.	As measured by the return of the reference portfolio		Performance reported at each LT and Board meeting.	By Board April 2020
Fund three year downside risk	We have a 5% chance that the reference portfolio return over 3 years will be $\leq -9.3\%$. We have a 1% chance that the reference portfolio return over 3 years will be $\leq -16.5\%$.	As measured by the return of the reference portfolio		Performance reported at each LT and Board meeting.	By Board April 2020

Metric	Investment Risk Limits	Measurement	Risk Limit	Reporting	Approved
Concentration					
Opportunity	We expect that the commitment to any investment opportunity will be no more than 10% of the NAV of the Fund, except where exceptions have been approved by the Board.	As measured by the NAV of the commitments and the actual portfolio, with exceptions listed in Schedule 7 of the <i>Investment Risk Allocation Policy</i>	10% of NAV for each opportunity	Reported weekly by FTG. Reported monthly to LT and in Board Dashboard.	By Board November 2020
Single sector within a country	We expect that the commitment to any single sector within a country will be no more than 3% of the capital of the Fund. Applies to value-add opportunities, with the exception of sovereign debt derivatives referenced to an index, Tilting, and Factors.	As measured by the NAV of the sector within a country and the actual portfolio.	3% of NAV	Reported weekly by FTG. Reported monthly to LT and in Board Dashboard.	By Board November 2020
Single manager	We expect that any manager will have investments of no more than 25% of the NAV of the Fund	As measured by the NAV of the mandates with a manager and that of the actual Fund portfolio	25% of NAV	Reported weekly by FTG. Reported monthly to LT and in Board Dashboard.	By Board June November 2020
Single private markets manager	We expect that any private market manager will have commitments of no more than 5% of the NAV of the Fund	As measured by the NAV of the mandates with a manager and that of the actual Fund portfolio	5% of NAV	Reported weekly by FTG. Reported monthly to LT and in Board Dashboard.	By Board November 2020

Metric	Investment Risk Limits	Measurement	Risk Limit	Reporting	Approved
Strategy-Specific					
Single Mandate Active Risk	We expect that active risk of any single mandate will be no more than 0.5% at the fund level.	As measured by the active risk of a mandate at the fund level	0.5% active risk at fund level	Reported monthly to LT and in Board Dashboard	By Board June 2015
Single Asset	We expect that the commitment to any single asset within a value-add opportunity, with the exception of sovereign debt or derivatives referenced to an index, will be no more than 2% of the capital of the Fund	As measured by the NAV of the asset, where a single asset can be either a listed security, or an asset we own directly, including both equity and debt ownership	≤ 2% of NAV	Reported weekly to FTG. Reported monthly to LT and in Board Dashboard.	By Board November 2020

Metric	Investment Risk Limits	Measurement	Risk Limit	Reporting	Approved
Portfolio Completion					
Rebalancing absolute risk	We expect the absolute risk of the Fund to be no different to that of the rebalancing target on average over the long term, and within a range of +/- 0.3% of the absolute risk of the rebalancing target at any point in time	As measured by the difference in the annualised standard deviation of expected return of the actual portfolio and that of the rebalancing target	0.3%	Reported daily by the Rebalancing Tool	By Board June 2015
Rebalancing relative risk limit	We expect the relative risk that results from rebalancing drift to be no more than 0.5% at any point in time	As measured by the annualized standard deviation of the difference in returns between the actual portfolio and the rebalancing target	0.5%	Reported daily by the Rebalancing Tool	By Board June 2015
Liquidity – Short Term Management	The Fund must hold enough Highly Liquid Assets to satisfy at least one MLR	As measured by the notional of each class of derivatives * an Asset Multiplier	1 MLR	Reported weekly by FTG Reported monthly to LT and in Board Dashboard	By Board November 2020
Liquidity Replenishment Level	We expect that in normal market conditions the Fund will maintain liquidity that is expected to sustain the Fund's activities through a severe downturn in market prices, and for there to be sufficient liquidity to sustain activities through a downturn of half of that magnitude at any point in time.	As measured by units called EMVs which correspond to approximately the worst three-day downward movement in pricing of listed markets. A severe downturn in this context is defined as 4 EMV in each of the major markets. The percentage movements that define an EMV are set out in Schedule 7 of the <i>Investment Risk Allocation Policy</i> .	2 EMV	Measured and monitored by FTG. Reported monthly to IC and Board. Board notified if below 3 EMV.	By Board June 2012
Counterparty failure	We expect that if there is a counterparty failure and where there are contagion effects the maximum loss to a single counterparty will be limited to 2% of the capital of the Fund. (5% for Australian/NZ banks).	As measured by the NAV of the actual Fund portfolio	2% of NAV (5% for Australian/NZ banks)	Counterparty risk limits measured and monitored daily. Reported weekly to FTG. Reported at each LT, Board and Audit meeting.	By Board June 2009 via approval of the Direct Management Policy

Appendix 2: Risk Appetite and Risk Limits for Business Risks

Business Risks	Risk Appetite	Risk Limit
Unintended profit or loss impacts	No more than a \$10m impact once in every 10 years	\$30m impact once in every 10 years
Processes	Failure of project up to \$10m no more than once in every 10 years	Failure of project up to \$30m once in every 10 years

For the following Business Risks, the Board has the following Risk Appetite:

Business Risks	Risk Appetite
Health & Safety	No fatalities or serious harm
Business continuity	No permanent loss of key data
Cyber	No permanent loss of key data; no financial extortion; no breach of payment controls
Staff	No loss of personnel that would result in an investment strategy or activity having to stop
Conduct	No incidents of misconduct
Regulatory	No breaches of law, contract or regulation resulting in fundamental failure to achieve purpose

Approved by Board on July 2014 and amended on 17 June 2015, 21 June 2016, 20 September 2016, and 21 February 2017

Schedule 3: Risk Management Framework

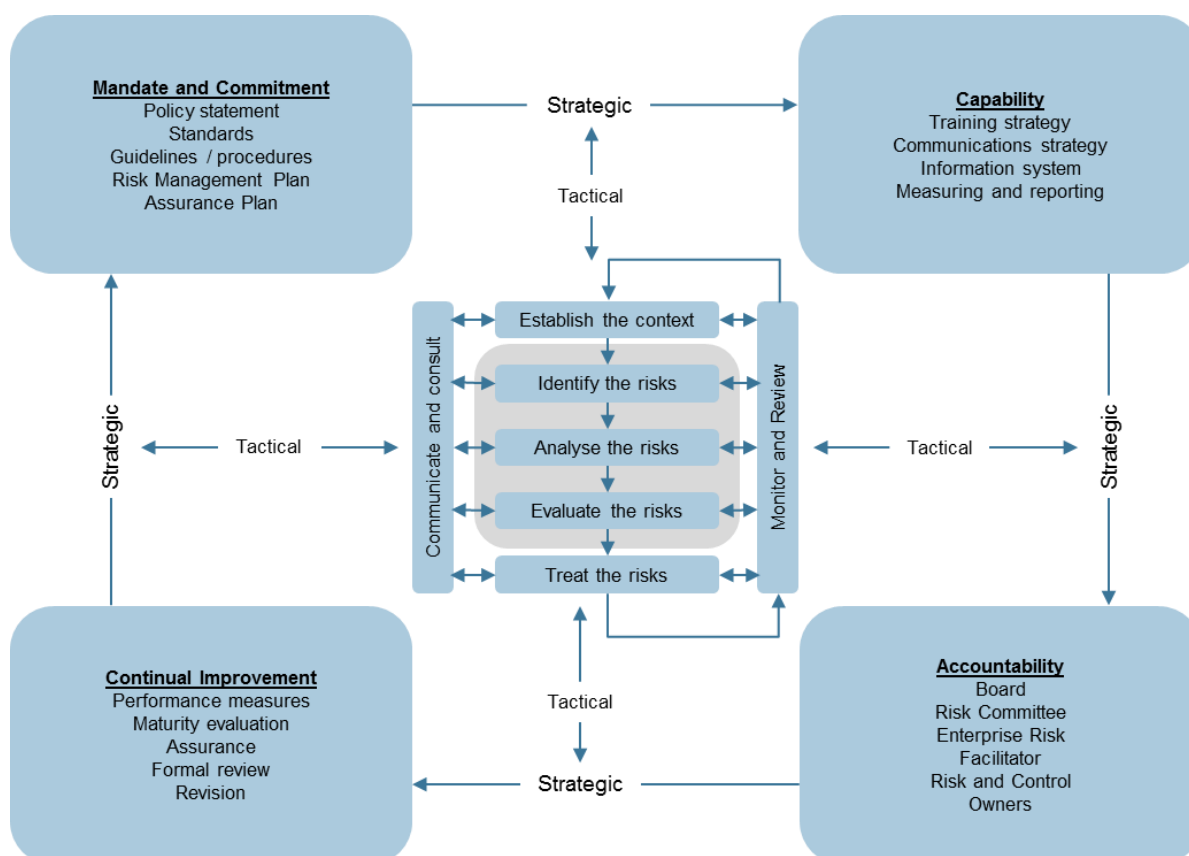
3.1 Our approach to risk management is based on the following core elements:

- The Board establishes the risk appetite; this is captured in the risk appetite statement.
- The risk appetite is reflected in policies that are all approved by the Board.
- Management ensure the policies are implemented and maintained for identification, monitoring, measurement and management of all relevant risks.
- Internal audit and internal risk functions provide assurance to the Board and Audit Committee of performance against internal controls and risk management systems.

3.2 The purpose of effective risk management is to drive value in the business by reducing uncertainty and improving the likelihood of successful outcomes for decision making, projects and enterprise activities.

3.3 Using AS/NZS 31000:2009 as a guide, our risk management framework spans activities establishing organisational intent (including policy development), capability development (including training and analysis), accountability (including responsibilities and oversight) and continual improvement (including effectiveness evaluation). At its core is the process for identifying and addressing risks in the business. This framework is described in Figure One.

Figure One: Risk Management Process



© Broadleaf Capital International Pty Ltd

- 3.4 At the core of our risk management framework is the process of risk identification, risk analysis, risk control effectiveness and risk treatment / residual risk analysis. We link this process with the development of our policies and risk governance structures to ensure we monitor, review, communicate and consult on our risks. This process is described in the four stages below:

Stage 1 Risk identification

- 3.5 Identification of uncertain events or conditions that could affect the achievement of our objectives and outputs, based on the high-level Strategic Plan, lower-level business plans, each business unit's key processes/activities and consideration of external/environmental factors.

Stage 2 Risk Analysis

- 3.6 The likelihood of these events is subjectively rated with consequences evaluated in terms of their impact on our stated objectives. Risk Analysis is undertaken through the Enterprise Risk Report, Business Unit Risk Registers, New Investment Initiatives (Operational Risk Assessments) and Project Risk Assessment.

Stage 3 Control effectiveness rating

- 3.7 This stage is to analyse the effectiveness of existing controls in managing risks. Controls may include policies, procedures, standards, processes and codes of practice.
- 3.8 Control effectiveness is assessed formally at least annually, complemented by findings from external and internal audits, reported incidents and any other relevant facts.

Stage 4 Residual Risk Analysis

- 3.9 Residual Risk Analysis involves assessing the level of risk remaining for each identified risk after consideration of inherent risk and total control.
- 3.10 For each residual risk we assess the risk to determine what is the best risk management strategy to adopt:
- accept the risk and make a conscious decision to not take any action, or
 - accept the risk but take some actions to lessen or minimize its likelihood or impact, or
 - transfer the risk (in whole or in part) to another individual or organization (e.g. through insurance), or
 - eliminate the risk by ceasing to perform the activity causing it.
- 3.11 Our assessment of the appropriate risk management strategy is captured in the Enterprise Risk Report and Business Unit Risk Registers which then feeds into the business unit plans and business initiatives.

Risk Management Governance

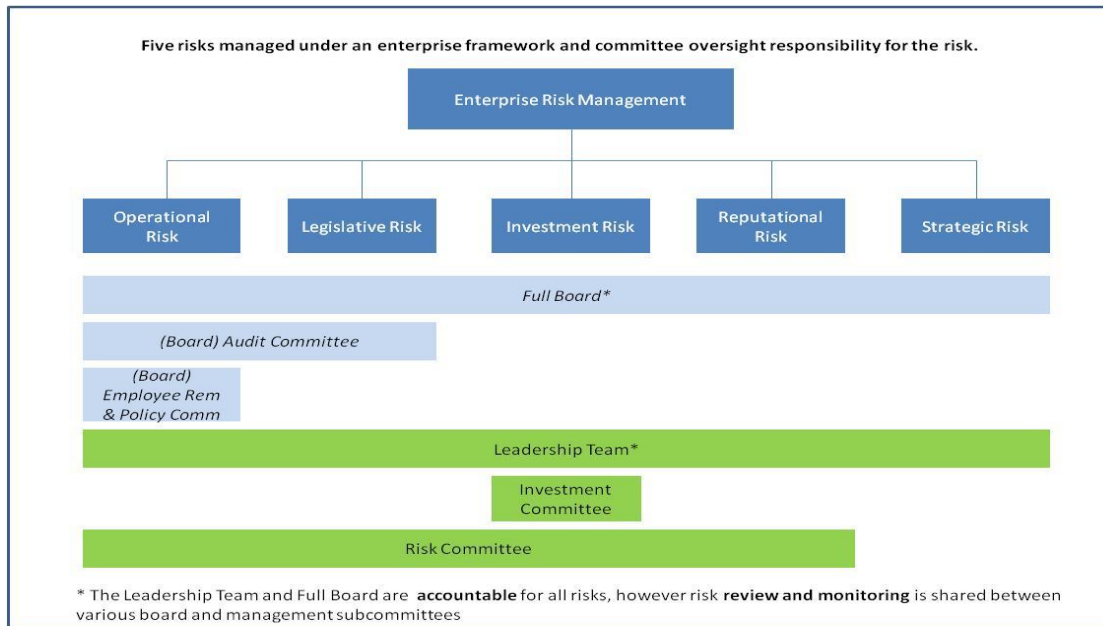
- 3.12 To promote transparency and clear accountability, the process we use for managing the acceptance of non-investment risk is set out below:

- a) The severity of the residual risk will determine who has the power to accept the risk. Those authorised to accept risks are set out in the Delegations Policy
 - b) For consistency our existing risk assessment framework is used for rating risks (refer Schedule 4).
 - c) The relevant General Manager ensures all accepted risks are updated into the business unit's risk register. Transaction or project specific risks are recorded in either the operational risk assessment (ORA) for the transaction, the Project Plan for a major project initiative (e.g. IT project) or other relevant documentation (e.g. Document Execution Form) supporting the transaction.
 - d) Where an accepted risk is rated high or above, in addition to recording the item in the business unit's risk register, the risk owner ensures the risk is updated into the Enterprise Risk Report for review by the Risk Committee and, subsequently, the Board.
 - e) Documentation is retained by the relevant General Manager to clearly evidence the acceptance of the risk by the approver and the reasons for the acceptance.
 - f) The authority to accept risks is role specific and cannot be delegated by a General Manager or Head of Business Unit to any other person.
 - g) Accepted risks are periodically reviewed in accordance with the timeframe specified in the Risk Committee business unit risk register review calendar. Accepted risks must be reviewed at least annually.
 - h) As part of the annual risk review cycle, enterprise risk reports are updated to capture 'High' and other relevant risks that have been accepted by a business unit.
- 3.13 The Leadership Team and Board are accountable for all risks: however, oversight responsibility for reviewing and monitoring the enterprise risk report, business unit risk registers and Operational Risk Assessments rests with the Risk Committee.
- 3.14 The Risk Committee is composed of relevant subject matter experts from within the appropriate functional areas of the organisation and when assessing risks it aims to identify risks that individual business units might not identify (by reason of not seeing the whole-of-organisation perspective) and to ensure risks are treated consistently across Business Units.

Training

- 3.15 Training is provided to staff in a range of delivery methods to ensure that risk awareness is enhanced across the business. Improved risk awareness leads to more effective controls and identification of emerging risks.

Figure Two: Risk Governance

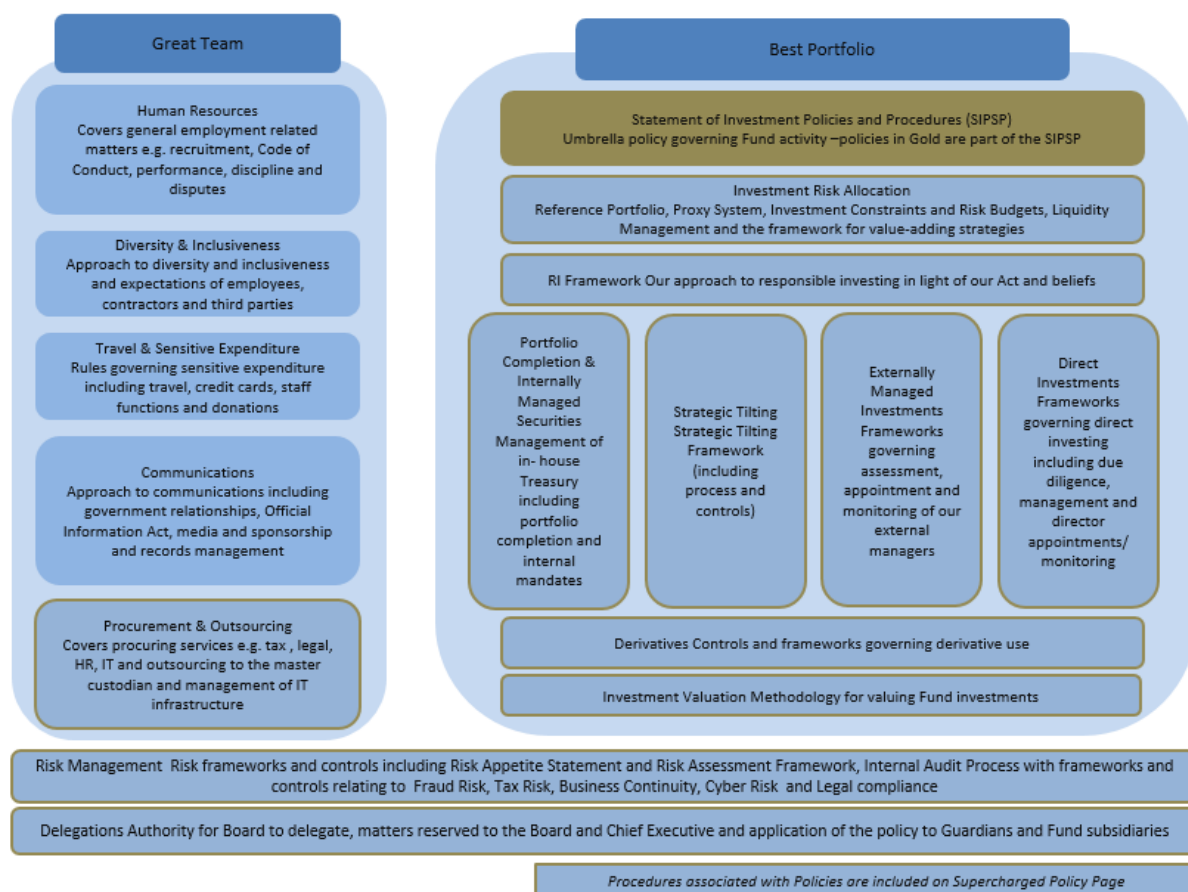


- 3.16 The Risk Committee evaluates the risks referred to it in terms of degree of risk (likelihood / impact) as well as effectiveness of existing controls or treatments, and the need for implementation of additional controls. It recommends appropriate courses of action directly to the relevant units, who are then responsible for incorporating the required risk mitigating activities into their business plans. The Risk Committee monitors implementation of its recommendations.
- 3.17 If new controls and treatments cannot be accommodated within existing resources they are referred to the Leadership Team for prioritisation.

Policy Framework

- 3.18 Development, implementation and maintenance of policies are key to our control environment and compliance programme. These are a key set of documents that:
- set out clearly the Board's expectations for management and the standards management will adhere to in meeting those expectations;
 - highlight and ensure compliance with our legal obligations.
- 3.19 Policy statements are approved by the Board and may only be altered by the Board. Management is responsible for developing and adhering to standards to meet the requirements of those statements. The Board has full visibility of, and in some cases control over, those standards.

Figure Three: Current Policies



Responsibility for Policies

- 3.20 Each policy has an ‘owner’. Owners are responsible for initiating and co-ordinating changes to their policy as required to ensure it remains up to date in light of changes to our business or legal obligations. Authority to approve changes is clearly shown in each policy. All major changes are reviewed by the General Counsel. Changes to policy statements or material changes to schedules are then reported to the Board for either information or approval as required by the policy.
- 3.21 Policies are reviewed by the policy owner in accordance with the policy review timetable set by the Board. As part of this review the policy owner certifies to the Risk Committee that their policy remains up to date and complete. A policy owner may rely on certifications by subject matter experts and other staff as to the accuracy and completeness of the content.
- 3.22 General Counsel is responsible for maintaining a record of policy owners.

Monitoring and Assessment of Policy Compliance

- 3.23 All staff have the following objectives in their role descriptions:

- Comply with the Code of Conduct including the Securities Markets Procedure, the Delegations Policy and all other policies applicable to them.
- Report any observed policy breaches or potential procedure and control issues in line with the Learning & Opportunities Process (Schedule 9).
- Assess and take prompt action to manage risks associated with their function.

- 3.24 All staff certify to their manager compliance with the policies applicable to them on a periodic basis. The form of certification is developed and reviewed annually by the General Counsel in consultation with the Leadership Team. Compliance certifications include cross references to the relevant Policies.
- 3.25 The Chief Executive Officer certifies to the Audit Committee compliance by the organisation with the policies on a six monthly basis.
- 3.26 In addition to certification, we will have testing methodologies to provide assurance that we have been compliant in those areas where this is possible and apply those tests at an appropriate frequency based on an assessment of the risk.

Availability of Policies

- 3.27 All policies are available to all staff on our intranet and to the Board and the public on our internet site. Whenever a new policy is published or an existing policy is materially updated, all staff are advised by the intranet.

Training

- 3.28 We require every manager to ensure that their staff receive adequate initial and refresher training on the compliance obligations specific to their areas of responsibility. Policy reviews also consider whether refresher training is necessary.
- 3.29 Training may include presentations to new employees, refresher seminars or on the job coaching. The General Manager Human Resources keeps records of completion of relevant compliance training.

Key Controls

- 3.30 The following documents contain key controls in our management of risk that are not covered elsewhere in this policy or in other policies:
- Proper Instruction Framework: attached as appendix 3A.
 - Standard Settlement Instructions and Payment Control Framework attached as appendix 3B.
 - Foreign Currency Bank Account Operating Framework attached as appendix 3C.
- 3.31 The Risk Committee will undertake an annual review of the Proper Instruction framework.

Approved by Board on 21 June 2016 and amended 6 August 2019

Schedule 3A – Proper Instructions Framework

Proper instructions (PI's) are the means by which directions are provided with respect to the Fund from the Guardians to the Custodian, an external manager or an Approved Counterparty for a Direct Transaction.

PI's can cover almost any requirement including: the transfer of cash; the booking of accounting entries; the establishment of an investment mandate; or the addition or removal of users from a system.

Required levels of approval differ depending on the outcome of an instruction.

The tables below summarises the approvals required under the PI framework, by instruction type. 'PI approval requirements' refers to what category of Authorised Signatory is required to approve the transaction (i.e. Part A or Part B Authorised Signatory).

PI Approval Requirements – Non Cash Instructions

Transaction (typical examples, not a definitive list)	PI Approval Requirements
Tax accruals Unit pricing changes / private market revaluations Manager instructions IMAs – new or amended Account opening / amendment / closing Compliance Monitoring Updates (e.g. new Responsible Investment exclusion list) Client Provided Pricing Instructions to Northern Trust Internal transfer of securities or positions (excl. cash) between accounts Recall of security (e.g. for voting) from Securities Lending Manager Non-cash Tri-party agent instructions Non cash collateral (initial margin futures, OTC collateral, repo collateral) Derivative instructions, not involving cash movements OTC Derivatives Clearing Instructions to Northern Trust (includes fee accruals, interest accruals and other non-cash bookings)	1 x Authorised Signatory (either 'Part A' or 'Part B')
Addition or removal of an Authorised Signatory Addition or Removal of any Authorised System User, including "GCM Input/Approver", "GCM Senior Approver", GCM profile Input/Approver or "TOE Input/Approver" Any other one off non-cash transfers to an external party (including 'free-of-cash transfers') Authorising the custodian to provide information to a 3rd party Melbourne Vault Securities – addition or removal of docs	2 x 'Part A - Authorised Signatories'
Addition or change of any SSI to the SSI library or addition or change of any GCM profile	2 x 'Part A - Authorised Signatories' (one signatory must be one of: 'General Manager Finance & Risk' or 'Head of Finance')
Trades using VCON or a Swap Execution Facility (SEF)	Any 1 Authorised Dealer
OTC trade confirmations	Legal Business Unit approval for the template, and then signed by any 1 Authorised Signatory (either 'Part A' or 'Part B')

PI Approval Requirements – Cash Instructions (both manual and automated – i.e. SWIFT, flat file instruction etc.)

Transaction (typical examples; not a definitive list)	PI Approval Requirements
Internal cash transfers or cash receipts	1 x Authorised Signatory (either 'Part A' or 'Part B') or any 1 Authorised Dealer
Internal mandates – equities, fixed income, RCDs, Repos, etc.	1 x Authorised Signatory (either 'Part A' or 'Part B') or any 1 Authorised Dealer
Internal mandates – FX, 3 rd party deposits, call interest, repo cash collateral, OTC cash collateral, futures cash margin, collateral interest, repo collateral interest, OTC derivatives, CDSs, OTC Margin (Initial Margin & Variation Margin), Securities Lending cash collateral moves etc.	2 x Authorised Signatories (either 'Part A' or 'Part B') or any 1 x Authorised Signatory (either 'Part A' or 'Part B') plus any 1 Authorised Dealer
Supplier payments, tax payments, investment funding (accompanied by a non-cash PI) etc. via GCM	1 x Authorised Signatory (either 'Part A' or 'Part B') for payments under \$1m otherwise 2 x Authorised Signatories (either 'Part A' or 'Part B') - (2 nd approver must be a designated senior approver)
Investment funding via TOE	2 x Authorised Signatories (either 'Part A' or 'Part B')
Any other one-off clean cash movements out of the Fund (e.g. fixed asset purchases, monthly custodian fees)	2 x 'Part A - Authorised Signatories'
Tri-Party Agent Instructions	2 x Authorised Signatories (either 'Part A' or 'Part B') or any 1 x Authorised Signatory (either 'Part A' or 'Part B') plus any 1 Authorised Dealer

Approved by the CEO on 21 June 2016, and updated 24 May 2017, 27 August 2019, 25 September 2019, and 11 March 2020.

Schedule 3B – Standard Settlement Instructions and Payment Control Framework

	Process Steps:	Performed by:	Mandatory?
Group 1: Investment related payments by the Fund to counterparties	Obtain schedule of SSIs directly from counterparty, signed by 2 of their authorised signatories (PDF format). Any SSI changes due to a third party payment request need to be confirmed by a written documentation that has been authenticated by the actual contractual beneficiary. This documentation will include at a minimum, the SSI details of the third party.	SSI Admins	Yes
	Obtain a copy of the counterparty's Authorised Signatories list directly from the counterparty (PDF format)	SSI Admins	Yes
	Check signatures on SSI schedule to the Authorised Signatories list, ensuring signatory's authority is valid	SSI Admins	Yes
	Verify back to an independent function at the counterparty that the SSI schedule is correct	SSI Admins	Yes but the minimum criteria cannot be specified but instead need to be tailored by the SSI Admins in each case, and may require commercial judgment to be exercised
	Advise confirmed SSIs to the custodian via PI, or: Enter SSI's within the Bloomberg SSI library.	Operations SSI Admins	Yes - refer to PI framework Yes - refer to PI framework
Group 2: Investment related payments by the Fund to other than counterparties, e.g. private market fund calls, one-off investment transactions as part of our direct investment strategy, etc.	Obtain payee bank details from payee	Operations or Finance	Yes
	Verify back to an independent function at the counterparty that the payee details are correct	Risk	Yes
	Enter SSIs into Northern Trust Global Cash Movement System, or if a one off payment, advise Northern Trust via a PI	Risk Finance	Yes - refer to PI framework
Group 3: Creditor related payments by the Fund and the Guardians, e.g. manager fees, custodian fees, other general expenses, and fixed assets, etc.	Obtain advice from creditor to confirm payee account details	Finance	Yes
	Confirm that the supplier is a legitimate business as per the NZ supplier and Overseas Supplier set up checklist.	Administration (Guardians) / Risk (Fund)	Yes
	Verify the bank details as per the NZ supplier and Overseas Supplier	Administration (Guardians) /	Yes

	set up checklist.	Risk (Fund)	
	Payee details loaded into internal library for Guardians' creditor payments	Administration	Yes
	PI process covers Fund fixed asset purchases	Refer PI framework	Yes - refer to PI framework
	Payee details loaded into GCM for Fund creditor payments	Risk and Compliance	Yes - refer to PI framework

Approved by the CEO on 28 October 2014 and 27 August 2019

Schedule 3C – Foreign Currency Bank Account and Money Market Accounts Operating Framework

Function:	Control:
Opening and Closing Foreign Currency Bank Accounts or altering Bank Account Signatories.	Existing Delegations Policy
Control of payees from Foreign Currency bank Accounts.	Existing SSI Framework
Verifying SSI's on the setup of Money market accounts.	Existing SSI Framework
Systems administration – establishes who may operate the Foreign Currency Bank accounts.	Any system changes must be approved by 2 Authorised Bank Account Signatories before being implemented. IT and Risk and Compliance are responsible for setting up users of the system (including the type of access)
Money Market Administration – communications to the counterparty on the control process and who may enter into money market transactions on GNZS's behalf.	The "Authorised Dealers, Authorised Signatories and the Control process" Notification (the Notification) must be sent to the counterparty. This is to be signed by 2 Authorised Signatories.
Transfer of funds to/from bank/custodian	Require the review of any 2 Authorised Bank Account Signatories <u>or</u> any 2 PI Persons as nominated by the GM Operations and GM Finance and Risk and approved by the CEO
All other Foreign Currency account transactions.	Require the approval of 2 Authorised Bank Account Signatories
Authority to open / close a Money Market account.	Primary authority to open / close a Money Market account rests with the General Manager Portfolio Completion. Prior to approval, the considerations on opening a Money Market account is to be formally discussed at the weekly Funding and treasury Group meeting.

Approved by the CEO on 28 October 2014

Schedule 4: Risk Assessment Framework

Potential Risk Impact

- 4.1 The Guardians has adopted a procedure for identifying and rating risks which reflects the recommendations of Australia/New Zealand ISO 31000 on Risk Management. Once a likelihood rating has been applied to a risk, the Guardians assigns an impact rating if that risk were to occur. The following table provides a calibration for how a risk is assigned an impact rating.
- 4.2 Each potential risk is rated for likelihood of occurrence and severity of impact. The purpose is to seek “directional accuracy” and use the process to rank and prioritise risks for further additional treatment rather than define it as an absolute measure or expected outcome.
- 4.3 If risk realisation could result in multiple impacts (e.g. a “Minor” Investment impact but “Major” Business impact) the higher impact rating should be selected.
- 4.4 The Guardians see reputation risk primarily as a consequence stemming from the realisation of Fund or Business risks. For this reason, a description of serious reputation consequences is provided below the table. When specific risks to the Guardians’ reputation emerge, then management plans are activated.

Business Risks		
	Unintended profit or loss impacts	Processes
Severe	\$20m - \$30m	Failure of project of between \$20m - \$30m. More than 10 instances of fundamental process failure leading to complete breakdown of operations
Major	\$10m - \$20m	Failure ¹ of project of between \$10m and \$20m Qualified audit report Custodian Normal operational errors >400 errors Custodian Major errors >24 pa Organisational errors reported to the Audit Committee > 24 pa
Moderate	\$5m – \$10m	Failure of project of \$5m - 10m Any OAG ESCO audit grade “Poor” Restatement of financial accounts or Fund performance Custodian Normal operational errors >300 errors Custodian Major errors >12 pa Organisational errors reported to the Audit Committee > 12 pa
Minor	\$1m - \$5m	Failure of Project of \$1m - 5m
Insignificant	-	-

¹ Failure of a project means any of the following: (1) No project benefits will be realised; no project success measures will be met; and/or the project will be stopped.

The Board has designated the potential impact of each of the following business risks to be unacceptable regardless of likelihood:

Health & Safety	Business Continuity	Cyber	Staff	Conduct	Regulatory
Fatalities or serious harm	Permanent loss of Key Data	Permanent loss of Key Data; financial extortion; breach of payment controls	Loss of personnel that would result in an investment strategy or activity having to stop	Incidents of misconduct	Breaches of law, contract or regulation resulting in fundamental failure to achieve purpose

Risks for Investee Companies

The Guardians actively monitors the health, safety and environmental governance compliance of certain investee companies as specifically reported to the Board

The following table is a calibration of the Guardians' view of the impact rating for health and safety risks for those companies which are monitored:

Severe	One death
Major	A maiming or incapacitation
Moderate	Serious harm injuries
Minor	A sentinel event such as a near miss that could have resulted in a serious harm injury
Insignificant	Near misses of a minor nature

Combined with a likelihood rating this impact rating provides the Guardians with a risk rating which informs the Guardians' response to such investee company risks

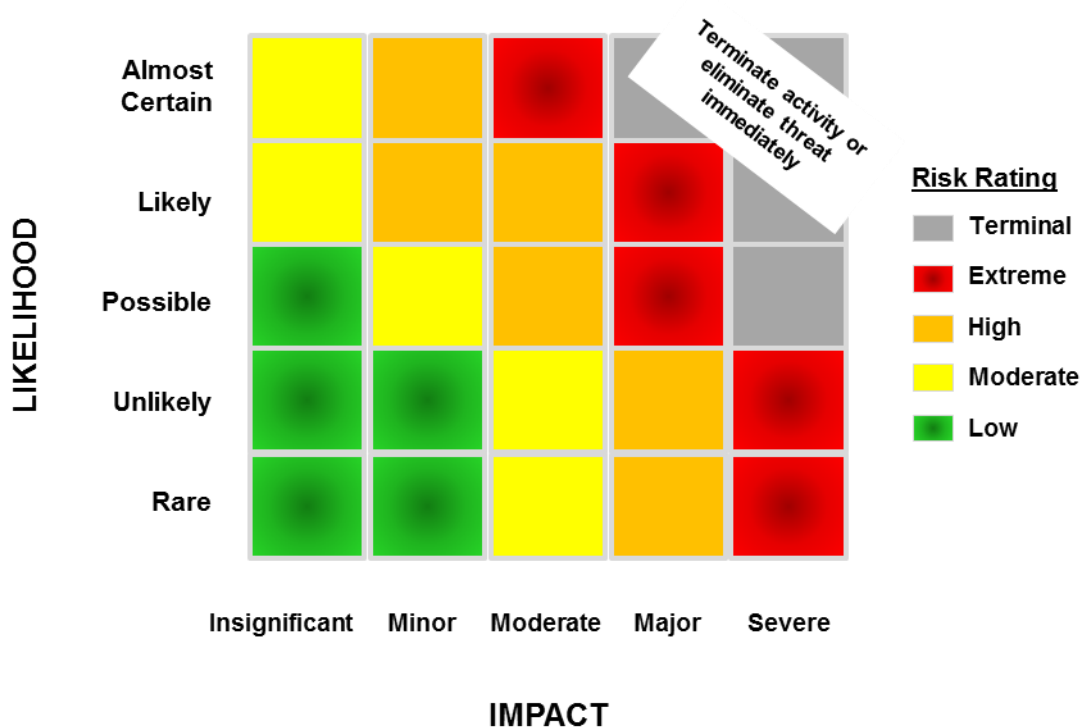
Reputation

Reputation is likely to be seriously affected if any of the following events take place:

- Independent review:
 - questions competence and integrity
 - attempts to significantly influence investment decisions
- Censure (e.g. State Services Commission, OAG, or Auditors)

In such case, management has an action plan to activate in order to assess the potential impact to reputation and take appropriate steps

LIKELIHOOD	Description
Almost Certain	The event is expected to occur in most circumstances (95% chance of occurring in next 12 months or in 19 out of every 20 years)
Likely	The event will probably occur at some time (50% chance in next 12 months or in 10 out of every 20 years)
Possible	The event may occur at some time (25% chance in the next 12 months or in 5 out of every 20 years)
Unlikely	The event is unlikely to occur (10% chance in the next 12 months or in only 2 out of every 20 years)
Rare	The event will occur only in exceptional circumstances (4% chance or only once every 25 years)



Approved by the Board on 21 February 2017

Schedule 5 Internal Audit Charter

1. Introduction

This charter identifies the purpose, authority, independence and responsibilities of the Internal Audit function. The Guardians of New Zealand Superannuation operate a co-sourced model for the provision of internal audit. For the purposes of the Internal Audit Charter, Internal Audit refers to internal audit activities undertaken by the Guardians' Internal Auditor or by external providers engaged by the Guardians' Internal Auditor.

2. Purpose

The purpose of the Internal Audit function is to provide independent and objective assurance designed to add value to the Guardians of New Zealand Superannuation (the Guardians) by assisting the Guardians to achieve its business objectives through a systematic and disciplined approach to evaluating and improving the effectiveness of governance, risk management and internal control.

The IA function will act via the Audit Committee as the Board's agent to:

- Provide the Audit Committee with independent assurance on the adequacy of the policies, processes and controls in place which underpin the successful conduct of the Guardians' business
- Assist the Guardians to develop and maintain systems of control which contribute to the successful achievement of its business objectives and strategies
- Assist managers to effectively discharge their responsibilities by providing good practice guidance and practical recommendations on particular activities
- Assist external audit by reporting findings from the internal audit programme so they may independently assess the degree of reliance they are able to place on the control environment when providing an opinion on the financial statements
- Liaise with external auditors and other risk and assurance providers as applicable
- Review operations to assure control systems are effective while identifying opportunities for improvement.

The Internal Audit function is not responsible for ensuring effective controls are in place.

3. Authority

Internal Audit has unrestricted access to all systems, functions, records, property and personnel of all Guardians' departments and to the external auditors and to other third parties as they determine necessary. Guardians' staff are to provide every assistance to Internal Audit.

4. Independence

In order to maintain its independence, the Internal Audit function shall have direct access to the Audit Committee. The Internal Audit function shall have neither authority over, nor responsibility for, the activities being audited. It has no executive or managerial powers, functions or duties except those relating to the management of the internal audit office.

To ensure independence, Internal Audit is directly responsible to the Audit Committee, working with the Chief Executive Officer and the GM Finance and Risk. The reporting lines for key activities are shown below.

	Responsibility
Receiving communications from the Head of Internal Audit on the results of the internal audit activities or other matters that the Head of Internal Audit determines are necessary, including private meetings with the Head of Internal Audit without management present, as well as annual confirmation of the organisational independence of the internal audit function.	Audit Committee
Approving all decisions regarding the performance evaluation, appointment, or removal of the Head of Internal Audit	Audit Committee Chair/CEO jointly
Approving the annual compensation and salary adjustment of the Head of Internal Audit	Audit Committee Chair/CEO jointly
Making appropriate inquiries of management and the Head of Internal Audit to determine whether there is audit scope or budgetary limitations that impede the ability of the internal audit activity to execute its responsibilities.	Audit Committee
Discretionary Authorities & Expenditure	CEO
Human resource administration	CEO
Internal communications and information flows	GM Fin & Risk
Administration of the internal audit activity's policies and procedures	GM Fin & Risk

To maintain objectivity, Internal Audit is not involved in day-to-day control procedures - each business unit is responsible for its own internal control and efficiency.

5. Responsibilities

The Internal Audit function is accountable for the quality of assurances and advice it gives and for the effective, efficient, and economic design and implementation of its audit plan including the development of the Internal Audit function.

The Audit Committee has responsibility for:

- Approving the annual internal audit plan
- Reviewing the Internal Audit function's performance against the audit plan and Internal Audit Charter.

The Internal Audit function has responsibility for:

- Developing a risk based annual audit plan for review and discussion with management and the Audit Committee, and approval by the Audit Committee
- Determining engagement scope
- Designing and performing relevant audit and testing plans to deliver audit engagements
- Managing the Internal Audit function's performance and reporting on these to the Audit Committee
- Monitoring all internal compliance and review annual work programmes within the Guardians and coordinate as required to ensure effectiveness of coverage
- Co-ordinating resources for special reviews as requested by the Audit Committee
- Timely reporting to the Chief Executive Officer and Audit Committee on each audit assignment on all significant findings and issues.
- Recommending, as necessary, changes to the annual audit plan during the year
- Enhancing the achievement of business objectives, especially the accuracy, adequacy, integrity, quality and effectiveness of business control systems (operational and finance)
- Helping identify areas of risk which could adversely impact on the success of the Guardian's business
- Keeping the Audit Committee apprised of business risks, audit activities and resulting actions, including quarterly reporting
- Operating in accordance with the Standards for Professional Practice of Internal Auditing issued by the Institute of Internal Audit or equivalent professional standards. Internal Audit shall abide by the Institute of Internal Auditors Code of Ethics
- Undertaking regular "self reviews" of work practices within the Internal Audit function
- Maintaining regular contact with the external auditors to ensure an effective use of resources and to avoid possible duplication of effort
- Coordinating any work required for the Audit Committee, including providing audit reports for its meetings.

Risk of fraud

While, the primary responsibility for the prevention and detection of fraud and error rests with management. Internal Audit assists in the prevention and detection of fraud by considering fraud risk and the factors that are associated with it during the course of audit assignments.

6. Scope of work

Internal Audit's scope of work will include but is not limited to review, advice and/or assurance over:

- Design, development, implementation and operation of risk management and governance processes, corporate operational policies and controls, processes, systems and procedures
- Performance and efficiency of operations and activities
- Accountabilities and delegations
- Reliability, adequacy and utilisation of financial management information
- Whether resources are used effectively, efficiently and economically
- Adequacy of protection afforded to assets
- Systems to ensure compliance with Guardians' policies, procedures and relevant legislation
- Internal controls.

7. Internal Audit Evaluation

The Head of Internal Audit will initiate a review of the performance of Internal Audit on a biennial basis. The review will generally be conducted on a self-assessment basis with appropriate input sought from the Audit Committee, Chief Executive, External Auditors and appropriate management. The review will be performed independently on a periodic basis (at least 5 yearly unless otherwise determined by the Chair of the Audit Committee).

Approved 14 March 2017, and amended 20 November 2019

Schedule 6: Risk to Strategy

- 6.1 Risk to strategy is the risk that we make strategic choices that do not attain the opportunities we seek or that threats are realised due to unsuccessful implementation of selected strategies. Managing this risk is primarily achieved through our Strategic Planning and Implementation processes, including the Target Operating Model.

Strategic Framework

- 6.2 Our strategy is designed to meet our obligations under the New Zealand Superannuation and Retirement Income Act 2001. The key elements of our strategic framework are shown below. The entire strategic framework is captured in our Strategic Plan. A copy of the current strategic plan is available on our intranet.

Figure Four: Strategic Framework



Planning Cycle

- 6.3 Our Planning Cycle is based on engagement of the Team, the Board and selected external parties.
- 6.4 The aim is for the strategic plan and budget to be approved annually at the March or April Board meetings. Financial forecasts are also submitted to Treasury around this time.
- 6.5 The action plans focus on translating the approved strategy into operational terms, aligning the organisation and making its implementation part of everyone's role. This is led by Management and involves developing more detailed business unit plans and measures that are transferred into individual performance management plans and the risk framework as appropriate. We review key risks associated with plan implementation

through risk analysis (as above) and against existing controls as part of this process.

6.6 Ongoing monitoring is focused on making strategy a continual process by ensuring ongoing progress, lessons and risks are monitored and acted on as appropriate. Management monitor all change included in the strategic plan and the Board monitor an agreed subset via the dashboard.

6.7 The annual cycle is shown below.

Figure Five: Annual Planning Cycle



Approved by Chief Executive on 12 June 2012

Schedule 7: Operational Risk - Fraud, Bribery and Corruption Risk Framework

7.1 **Fraud** is the deliberate practice of deception in order to receive unfair, unjustified or unlawful gain and, for the purposes of the policy, includes forms of dishonesty. Within this definition, examples of fraud may include, but are not limited to:

- unauthorised possession or use, or misappropriation of funds or other assets
- impropriety in the handling or reporting of money or financial transactions
- forgery or alteration of any document or computer file/record belonging to the Guardians or Fund
- forgery or alteration of a cheque, bank draft or any other financial instrument
- bribery, corruption or coercion
- destruction, removal or inappropriate use/disclosure of records, data, materials, intellectual property or assets for gain

Bribery is when

- a financial or other advantage is offered, given or promised to another person whether direct or indirect with the intention to induce or reward them or another person to perform their responsibilities or duties improperly or
- a financial or other advantage is requested, agreed to be received or accepted by another person whether direct or indirect with the intention of inducing or rewarding them or another person to perform their responsibilities or duties inappropriately.

Corruption is the misuse of a position of power or trust involving dishonest activity in which a director, employee or contractor acts contrary to the interests of the Guardian's and abuses their position of trust in order to achieve some personal gain or advantage for themselves or for another person or entity.

7.2 The GM Finance and Risk is the designated Fraud Control Officer. The role and responsibilities for fraud, bribery and corruption risk management are:

- a. Fraud Control planning – Fraud Control Officer
- b. Organisation fraud risk assessment – Leadership Team
- c. Fraud risk prevention and detection – all staff
- d. Fraud/suspected fraud response – initial points of contact must include CEO, GM Finance and Risk, Head of Internal Audit and General Counsel

7.3 There are a number of ways to identify the possibility of fraud, bribery and unethical or corrupt behaviour. Some of these include, but are not limited to:

- A robust recruitment and selection process, which ensures we employ people who adhere to strong ethical and professional standards, and are of good standing;
- A requirement for some employees to take two weeks (10 working days) consecutive leave per annum due to the nature of their roles;
- A requirement for some employees to take one week snap leave per annum, due to the nature of their roles;
- Effective application and enforcement of policies, procedures, and controls;
- Clear and applied delegation of authorities. Reviews include tests to ensure limits are being adhered to;
- Internal control systems, which ensure transactions and activities susceptible to fraud are reviewed regularly;
- Regular discussions with internal and external assurance providers, and remediation of any control weaknesses identified;

- Conducting forensic examination of personal computers in suspected cases of fraud or unethical behaviour;
- Setting stringent criteria for choosing service providers to ensure they are not appointed for personal gains; and
- Effective budget setting and financial management.

Gifts and Hospitality

- 7.4 All gifts and hospitality must comply with the guidance outlined in the Guardians Employee Code of Conduct. (part of the Human Resources Policy).

Facilitation payment

- 7.5 Facilitation payments are usually another name for a bribe.
- 7.6 We do not make, and will not accept, facilitation payments of any kind.
- 7.7 Facilitation payments are typically small, unofficial payments made to secure or expedite a routine government action by a government official. They are not commonly paid in New Zealand, but are common in some other jurisdictions in which we may operate.
- 7.8 If you are asked to make a payment on our behalf, you should always be mindful of what the payment is for and whether the amount requested is proportionate to the goods or services provided. You should always ask for a receipt which details the reason for the payment. If you have any suspicions, concerns or queries regarding a payment, you should raise these with the General Manager Finance and Risk.
- 7.9 Your safety is our primary concern and whilst New Zealand law prohibits facilitation payments, you are not required to place your life or liberty at risk. We understand that there may be circumstances in which you have no alternative but to make a facilitation payment in order to protect against loss of life, limb or liberty. Any such incidents should be reported to the General Manager Finance and Risk at the first available opportunity.

Sponsorships and Donations

- 7.10 Payments for sponsorships can only be made in accordance with the criteria outlined in our Communications Policy.
- 7.11 We do not make donations or contributions to political parties whether directly or indirectly. We can make donations to other bodies under certain circumstances, as set out in our Travel and Sensitive Expenditure Policy.

Investments, Investment Partners and Suppliers

- 7.12 The Fund's reputation and standing could be damaged by the acts of people working within our suppliers, investments and investment partners (together referred to as third parties). When engaging a third party, we must ensure that guidance relating to fraud, bribery and corruption outlined in the Externally Managed Investment Policy and Procurement and Outsourcing Policy is adhered to.

Whistle Blowing

- 7.13 We operate a Whistle Blowing procedure in accordance with the requirements of the Protected Disclosures Act 2000 to protect employees who expose serious wrongdoing against retaliatory action. Refer to the Employee Code of Conduct (part of the Human Resources Policy) for more information.

Reporting and Prosecution

- 7.14 If employees suspect an illegal or unethical act such as bribery, corruption, or fraud has occurred they should immediately inform their manager and/or their General Manager, the Head of Internal Audit or any other Leadership Team member they feel comfortable discussing with. Please note also the Whistle Blowing procedure referred to above, including the confidential external whistle-blowing service available. In some instances, it may be appropriate to make the disclosure directly to the Chief Executive Officer and/or to a member of the Board, for instance the Chairman of the Board or the Audit Committee.
- 7.15 If employees are unsure whether an act would be considered fraud, bribery or corruption they should seek guidance from their manager, General Manager or the CEO.
- 7.16 While employees must report incidents of fraud, bribery or corruption, they must not undertake their own investigations, unless assigned to do so by the officer in charge of investigations.
- 7.17 A Fraud Response plan is in place which outlines the process NZSF will follow when responding to a potential fraud event. The Fraud Response Plan also outlines who is expected to do what in the event that a suspected fraud is reported.
- 7.18 The Head of Internal Audit is the appointed officer responsible for co-ordinating the collation of all information and that sufficient information is recorded to enable further investigation(s). A third party may be engaged to ensure evidence is collected in an appropriate manner to meet legal requirements in the event of a prosecution. Any incidents of fraud are immediately reported to the Chief Executive Officer and a report of all relevant findings presented to the Chief Executive Officer and the Audit Committee.
- 7.19 A comprehensive investigation and analysis process is followed to ensure all fraud incidents, whether internal or external, are fully and carefully documented and managed in a consistent manner. A clear incident reporting process is followed to determine the way in which the fraud was perpetrated and to ensure action is taken to minimise the possibility of a repeat incident. All employees must cooperate with any investigation into suspected fraud, bribery or corruption.
- 7.20 A full report of the circumstances surrounding the suspected fraud or fraudulent behaviour is prepared at the conclusion of an investigation. This report includes lessons learned and recommendations to prevent a recurrence. This report is provided to the Audit Committee, which decides on further distribution of the report and/or actions required.
- 7.21 Where investigations show the disclosure is upheld, the matter is dealt with in accordance with the procedures for handling suspected fraud cases as recommended by the Police or Serious Fraud Office. Where sufficient evidence is found, the person will be prosecuted to the full extent of the law. This means the individual could be dismissed, with matters of a criminal nature being reported to the Police or Serious Fraud Office or other relevant body and pursued through the legal system.
- 7.22 The decision to prosecute rests with the Police or Serious Fraud Squad or other relevant body: it is not for the Chief Executive Officer or the Board to decide whether or not a person should be prosecuted. Any incident of fraud will be fully investigated, even if the person resigns. No arrangement will be made to accept a resignation in exchange for dropping the investigation.
- 7.23 The assets and property of a convicted fraudster will be pursued, whenever and wherever possible and practicable, in attempts to recover the amounts lost in relation to the fraud: both the actual fraudulent amount and costs associated in recovering the loss.

Training

- 7.24 Management are responsible for ensuring all staff are trained and regularly updated regarding their responsibilities in preventing and detecting fraud, bribery and corruption.
- 7.25 The General Manager Finance and Risk is responsible for making sure fraud training occurs at least every two years.

Fraud, Bribery & Corruption Risk Assessment

- 7.26 On an bi-annual basis the Fraud, Bribery & Corruption Risk Assessment will be reviewed by the Fraud Control Officer in conjunction with key staff and the design effectiveness of controls in the following area evaluated:
- Fraud prevention
 - Fraud detection
 - Fraud Exposures
 - Intentional manipulation of financial statements
 - Misappropriation of tangible assets
 - Misappropriation of intangible assets
 - Bribery and Corruption
- 7.27 Actions to improve controls are agreed and implementation monitored through the standard audit tracking process.

Approved by Chief Executive on July 2014, and reviewed on 7 August 2015 and 15 September 2015, 21 June 2016, and 27 August 2019

Schedule 8: Operational Risk - Tax Risk Management Framework

Background

- 8.1 Under New Zealand income tax legislation the Guardians is exempt from income tax, however it is subject to indirect taxes such as GST, FBT etc.
- 8.2 The Fund is not a legal entity in its own right, however for New Zealand tax purposes the Government's income derived from the Fund is subject to income tax in New Zealand calculated pursuant to the company tax rules. It is also subject to foreign tax depending on whether or not it has a taxable presence / taxable income in a foreign jurisdiction. The Fund's performance is measured on a post foreign tax / pre-New Zealand tax basis.
- 8.3 The Crown's tolerance for risk in tax planning is best expressed in Treasury's *Owner's Expectations Manual – Crown Ownership Monitoring Unit* (July 2012). The Guardians has adopted the principles outlined in the Owner's Expectation Manual (refer to paragraph 7.7.3) as the basis for determining the Fund's tax risk profile.
- 8.4 There is a Co-operative Compliance Agreement between the Guardians and Inland Revenue which was last renewed in September 2019 and remains in force until terminated in writing by either the Commissioner of Inland Revenue or the Chief Executive Officer of the Guardians.

Objectives

- 8.5 The tax function assists the Fund to meet its strategic objectives by providing tax support and advice on a timely and proactive basis minimising tax payable within the prescribed parameters set out in the Minister of Finance's letter. The correct amount of tax must be paid in all jurisdictions in compliance with tax law and practice including ensuring that:
- Sovereign immunity is claimed wherever possible;
 - Double taxation agreement relief is claimed wherever possible;
 - Foreign tax payable is minimised within the prescribed tax risk parameters;
 - All required tax payments and withholdings of tax are accurately calculated and made on a timely basis;
 - Foreign tax refunds are obtained on a timely basis;
 - Use of money interest and penalties are minimised;
 - All required tax returns, registrations, elections, notices of information or other disclosures are prepared accurately and are submitted on time;
 - Records required to be kept by tax legislation or any other relevant law are kept and preserved.

Tax advice in respect of new investment initiatives

- 8.6 Each major transaction and new initiative will be supported by an investment due diligence checklist covering specific tax issues. This tax checklist broadly covers the following topics:
- Investment structure;
 - Financing;
 - Cash repatriation of income and capital; and
 - Tax compliance.

Approved by Chief Executive on 13 June 2011, reviewed 7 August 2015, 21 June 2016

Schedule 9: Operational Risk - Internal Learning Opportunities Process

9.1 Learning Opportunities can provide an indication of a weak control environment, or failure to apply existing policy and may indicate an opportunity for improvement.

9.2 An internal Learning Opportunity includes a single event or number of events (i.e. repeat errors, losses, failures) which indicates a weakness in our control environment. These include events that have occurred or may occur (i.e. near misses) that can give rise to:

- Financial loss / gain
- Reputation damage
- All theft of Guardian assets or information

Before starting a report, discuss with Manager Enterprise Risk first who will assist in clarifying the need for a report. This includes discussing whether to log reports for potential events in other parts of the business

9.3 A “near miss” is an event that has not lead to an actual loss but could have.

9.4 The Learning Opportunities Process enables us to quickly report potential issues and to take appropriate action to ensure they don’t happen again. Important features include:

- Not about apportioning blame (issues are not reported against individual business units);
- Giving all staff the confidence to raise issues that could significantly impact the business, whether the issues come from their area or not;
- People raising issues are not automatically responsible for resolving them;
- Adopting an ‘If in doubt discuss with the Manager Enterprise Risk’ approach.

9.5 Examples of potential Learning Opportunities:

Financial loss / gain

- Data entry or pricing errors (e.g. proper instruction or deal ticket executed with material errors, including wrong amounts / wrong recipients that are only identified by accident or after failure of the transaction)
- Unauthorised transactions (e.g. sending instructions without the correct approvals)
- Hacking or viruses
- Fines due to regulatory or tax breaches
- Under researched product requiring further unplanned development
- Failures, errors or significant ongoing deficiencies in key models
- IT system failure, telecoms or power failure
- Initiatives cancelled or failed implementation due to poor project management
- Misuse or theft of Guardian assets or information

Reputation damage

- Adverse media comment on our competence or transparency
- Loss or disclosure of confidential information
- Entering into contracts without authorisation
- Censure (e.g. State Services Commission, OAG, Auditors, IRD)
- Criminal actions of staff
- Negligent actions of senior staff
- Significant reputation-damaging behaviour by investment manager or major supplier

Note:

- Human Resources related issues are covered by the *Human Resource Policy*.
- Issues formally managed through another effective “business as usual” incident

process (e.g. Custodial errors or Treasury pre / post trade breaches) are not subject to this Internal Learning Opportunity report process.

Learnings Opportunities Process

9.6 We should complete an LOR where:

- Financial impact \geq \$50K financial impact (Actual or Potential) or
- There is a “Material” reputational impact (Actual or Potential)

There also may be situations where it is appropriate to prepare a Learning Opportunity report for items below these thresholds where there is a systemic issue or there is a broader learning opportunity for the organisation.

9.7 The following describes the process for identification and reporting of a Learning Opportunity:

Identification: A potential LOR event is identified by a team member;

Assessment: The facts and details surrounding the LOR event are identified and the potential impact on the organisation are assessed to determine whether an LOR is required. The Manager Enterprise Risk will decide what type of report is required (if any).

If it is determined that an LOR should be done:

Analysis: The affected processes and control weaknesses are identified and analysed to identify the root cause.;

Remediation: Where possible, actions are put in place to resolve any immediate adverse consequences. Further remediation actions may be formulated and assigned to address the root cause;

Monitoring and Closure: Remediation actions are monitored and reported to relevant stakeholders until completion

9.8 Where it is determined that a Learning Opportunity report should be prepared:

- For Learning and Opportunities where the risk is considered “Moderate” and below a short form summary report may be prepared. In some cases it may be determined that a report is not required and the item is logged directly into the LOR database;
- A full report should be done for Learning Opportunities that are rated “High” and above. These reports are reviewed and signed off by the Chief Executive Officer. LOR’s rated “Extreme” and above are forwarded to the Risk Committee and the Audit Committee. In some cases it may be determined that a report is not required and the item is logged directly into the LOR database;

9.9 Where matters may potentially give rise to litigation or other legal issues the matter should be referred to the General Counsel and procedures agreed and followed in order to preserve legal privilege.

Approved by Chief Executive on July 2014, 21 June 2016, 17 December 2019, and 13 March 2020

Schedule 10A: Operational Risk - Business Continuity Management

Business Continuity Management

- 10.1 Business Continuity Management (BCM) is an over-arching framework that aims to minimise the impact of operational disruptions to our business. It not only addresses the restoration of information technology (IT) infrastructure, but also focuses on the rapid recovery and resumption of critical business functions.
- 10.2 A major disruptive event may be: Natural (e.g. flood, hurricane, earthquake); Accidental (e.g. fire, contamination); Commercial (e.g. loss of supply of critical services); or Wilful (e.g. sabotage, vandalism, arson, terrorism).
- 10.3 To the extent that it is practical and cost effective, we implement the good practice BCM model described in BSI ISO 22301:2012 Business Continuity.
- 10.4 BCM capability comprises three key components:
- Crisis Management Team – The team, who manage the response and recovery of our operations in the event of a disaster;
 - Business Recovery – Recovery of critical business operations within an acceptable time frame; and,
 - Technology Recovery – Recovery of supporting IT systems, network infrastructure and communications systems, supporting critical business processes.
- 10.5 These components are supported by:
- People – A clear chain of command, team structures, clear terms of reference supported by official mandates and delegations, trained people and high levels of awareness, understanding and commitment;
 - Infrastructure – Access to pre-arranged alternative locations, systems, communications, resources or providers to enable recovery and resumption of critical business functions; and,
 - Plans – Crisis management plans, review, testing and maintenance of the BCM programme and Business Continuity Plan (BCP).
- 10.6 We recognise the importance of our service partners for day-to-day operations, particularly the custodian. Assurance will be sought and given from key service partners that they have the requisite BCM capabilities in place to ensure adequate service levels in the event of a disaster within their operations.
- 10.7 We review the Business Impact Analysis and update the BCP (or plans) within 90 days of any major operational or system changes or at least on an annual basis. This will be managed by the General Manager Operations.
- 10.8 We test our BCM capability at least annually, in accordance with the testing programme managed by the Head of IT.

Approved by Chief Executive on 13 June 2011 and 21 June 2016

Schedule 10B: Information Security Framework

Information security governance and direction

- 10.9 The Guardians' direction and plan for addressing information security risks are documented in an information security strategy, which is refreshed annually. The strategy provides direction and an annual high-level plan for both control activities and assurance activities, with consideration to new emerging risks.
- 10.10 The strategy and its annual plan are informed by current security risks and our threat profile, as assessed and managed by management using the Guardians' risk management process, and informed by the risk appetite expressed by the Board. The IT risk register includes information security risks, among other IT risks.
- 10.11 The Chief Executive Officer has allocated responsibility for Information Security to the Risk Committee and this is captured in the Terms of Reference for the Risk Committee.
- 10.12 The Chief Information Security Officer (CISO) is the Head of IT. The IT Security Manager (ITSM) is a dedicated role within the IT Team. The responsibilities of the CISO and ITSM are documented in section 3 of the NZISM and PSR.
- 10.13 Additional oversight and direction of information security is provided by a Security Working Group with membership, processes, and responsibilities defined in its Terms of Reference.
- 10.14 Additional governance over security is established for major projects through project boards.

Information security management and operations

- 10.15 Security expectations, processes, and procedures are communicated to staff through a set of policies, standards or baselines, and Standard Operating Procedures (SOPs).
- 10.16 The NZ Information Security Manual (NZISM) has been developed by the Government Communications and Security Bureau. In 2014 the Protective Security Requirements (PSR) were published and these provide further guidance for agencies on securing information and assets. The NZISM and PSR are not mandated for the Guardians to follow, but as the NZISM and PSR reflect the latest good practice guidance for security, the Guardians will consider applying their requirements when designing and assessing processes and controls.
- 10.17 Although the Guardians uses its own information classification system, the information that is held and used by the Guardians is up to the level of "Restricted" according to the New Zealand Government Classification System. The NZISM contains control requirements for handling and processing of information up to the "Restricted" level. The Guardians establishes controls to meet the control requirements for "Restricted" where possible. Controls typically are either:
 - a. General security controls, from governance, to management, to daily operations. These may cover all systems or specific systems (people and process controls).
 - b. Controls built into the design and configuration of a system (technology controls).
- 10.18 The Guardians has established a set of information security control domains based on control areas typically assessed by the Government Chief Digital Officer (GCDO) and controls typically applied by New Zealand Government agencies to mitigate risks.
- 10.19 Guardians has set target maturity levels for most of the security domains, based on an assessment of the threat landscape and the inherent risks to the Guardians' information.

- 10.20 Key controls are selected for each control domain based on a target cyber security maturity level for that domain. These controls are documented in the Guardians' controls catalogue.

Information security assurance

- 10.21 Guardians management obtains assurance that the key controls in the catalogue are designed and operating effectively through:
- a. A system of routine assurance activities based on an annual schedule (annual information security assurance plan). The General Manager Operations and Head of Risk will sign off the annual assurance plan.
 - b. General controls audits designed to examine the design and effectiveness of each key control, to the extent it has not been assessed in other assurance activities.
 - c. Audits of specific information systems, as part of the system certification and accreditation process.
 - d. Independent reviews of baseline standards and how they are applied within systems.
 - e. A detailed review of security metrics and the results of assurance activities at the monthly IT Security Working Group meeting, which includes the GM Operations, Head of IT, staff with security responsibilities, and the Internal Auditor (for oversight).

Approved by Chief Executive on 21 June 2016, 27 August 2019, and 11 March 2020

Schedule 11: Operational Risk - Model Oversight Process

- 11.1 The purpose of this schedule is to provide guidance on the effective oversight of material models used by the Fund to manage and minimise our exposure to model risk.
- 11.2 A model is defined as:
A model consists of three components: an information input component, which delivers assumptions and data to the model; a processing component, which transforms inputs into estimates, recommendations or positions; and a reporting component, which translates the estimates into useful business information. Models meeting this definition might be used for analysing business strategies, informing business decisions, identifying and measuring risks, valuing exposures, instruments or positions, conducting stress testing.
- 11.3 The definition of models also includes critical complex spread sheets identified by the Business or Risk Committee which could potentially expose the Fund to high risk.

Model Oversight

- 11.4 A list of all models and key spreadsheets (as determined by the business) will be maintained by the Fund. The list will be updated on an annual basis. Models will be included in a formal review process where the inherent risk is moderate or above.
- 11.5 Models not included in the formal review process will be maintained in the models list noted above.
- 11.6 All components of a model included in the formal review process will be subject to validation i.e. input, processing, reporting and operation.
- 11.7 Model reviews should be completed using the model review template, available on the Risk Committee intranet page. The template ensures minimum standards for models are adhered to.
- 11.8 Given the higher inherent risks relating to managing changes in spreadsheets, a set of good practice guidelines for spreadsheets has been developed. Refer to guidelines on the Risk Committee intranet page.

Model Risk Assessment

- 11.9 A Models risk will be assessed in accordance with the Risk Assessment Framework in the Risk Management Policy.

Model review frequency & approach

- 11.10 All models assessed with a risk of moderate and above will be subject to periodic review by the Risk Committee. Models assessed as low risk will be reviewed periodically on a sample basis as determined by the Risk Committee.
- 11.11 The Risk Committee will determine the frequency of review for each specific model identified for periodic review. The frequency and nature of review required for a model can vary depending on the control environment in which the model operates. Reviews will be conducted by people agreed by the Risk Committee.
- 11.12 The resources for the review will be determined by the Risk Committee in liaison with the General Manager with ownership of the model. And will ensure that the reviewer

are of appropriate skill, capability and independence for the review of the model.

Committee Oversight

- 11.13 The Risk Committee shall oversee the model review process to ensure the effective operation of model oversight processes. The outputs from the review of high and moderate risk models will be tabled and reviewed by the Risk Committee to ensure reviews completed are sufficiently objective and robust. It may be appropriate for reviews completed of some models to also be reviewed by other Committees or groups that have a specific interest in the effective operation of the model.

Schedule 12: Legislative and Regulatory Risk - Legislative Compliance Framework

- 12.1 The Legislative Compliance Framework encompasses the activities implemented (or to be implemented) to help ensure we comply with our legal obligations. The Framework adopts the Compliance Programme principles outlined in the New Zealand Standard NZS/AS 3806:2006.
- 12.2 Our legislative compliance programme has the following components:
- **Operational Policies and Procedures.** These are the activities we do, and controls that we have, that are designed to ensure we comply with our legal obligations (covered in Schedule 3). This includes recording specific transaction risks in operational risk assessments and utilising the document execution form before we enter into legal documents. Appendix A shows the relevant legislation that applies to us and our investments and the relevant policies, procedures and supercharged information portals that are in place to meet these obligations.
 - **Identification:** This is the process by which we identify existing legislative compliance risks and changes and proposed changes to legal obligations that affect our business and operations. This is explained in sections 12.3 – 12.6 below.
 - **Monitoring, assessment, changes and reporting:** This is the way we identify and report any non-compliance with our legal obligations. This is explained in our Risk Management Framework (Schedule 3 of this policy)

Identification

- 12.3 This is the process by which we identify compliance risks as part of the wider risk management framework.
- 12.4 As part of the Guardians risk register the General Counsel maintains a section that details legislative compliance risks that have been identified. This register is used to develop certifications and policies.
- 12.5 The General Counsel identifies changes and proposed changes to our legal obligations that affect our business and operations by the following methods:
- a formal arrangement with external professional legal advisers to provide notification of changes and proposed changes to our legal obligations;
 - use of internal legal, accounting and other professional staff to notify changes and proposed changes to our legal obligations;
 - identification and discussion of legislative changes by the Risk Committee;
 - from time to time internal working groups are set up to focus on specific regulatory reform areas;
 - reviewing for your information and other material published by regulators, industry sources and professional advisers; and
 - online subscription services;
 - discussions and information exchanges with counterparties, custodians and clearing brokers;
 - attending legal forums and seminars;
 - via the legal team membership to In House Lawyers Association New Zealand; and
 - encouraging all staff to bring to the attention of the General Counsel and the legal team of any changes and proposed changes to our legal obligations. The 6 monthly policy attestation contains a positive affirmation that staff have notified the legal team whether they have become aware of new or proposed changes to laws,

regulations or industry codes that may impact on their business unit.

- 12.6 The General Counsel responds to changes and proposed changes to our legal obligations in accordance with the Policy Framework section of Schedule 3 (Risk Management Framework). The legal team produces a legal regulatory dashboard that contains details of changes or proposed changes and how they will apply to us. This is presented to the Risk Committee every 6 months and the Audit Committee annually.

Quality Assurance

- 12.7 We review the compliance programme at least every two years to ensure its continued suitability, adequacy and effectiveness. The Head of Internal Audit will be consulted as part of the review. The review will be reported to the Board.
- 12.8 Each review includes recommendations for compliance with our legal obligations that we have identified; and changes to operational processes, considered appropriate.

Appendix A: Legal Obligations and Policies Compliance

The following is a list of New Zealand legislation that applies to us and may apply to our New Zealand governed investments. Overseas jurisdictions will often have equivalent legislation.

The summary of New Zealand legislative considerations set out below does not purport to be comprehensive or to provide legal advice. If you require any advice on these matters please contact the legal team.

Our Legislative Obligations	How Embedded (Relevant Policies, Procedures, Supercharged)
Governing Legislation	
<ul style="list-style-type: none"> Companies Act 1993 (for Guardians subsidiaries) 	Delegations, Risk Management
<ul style="list-style-type: none"> Crown Entities Act 2004 (Conflicts of Interests, Board Duties, Board Membership and Procedure) 	Board Code of Conduct and Board Charter
<ul style="list-style-type: none"> Crown Entities Act 2004 (Delegations, Authorities, Directions) 	Human Resources, Communications, Risk Management, Travel and Sensitive Expenditure, Procurement and Outsourcing, Externally Managed Investments, Direct Investments, Portfolio Completion & Internally Managed Securities, Strategic Tilting, Derivatives, Investment Risk Allocation
<ul style="list-style-type: none"> Crown Entities Act 2004 (Reporting) 	Communications, Diversity and Inclusiveness
<ul style="list-style-type: none"> Crimes Act 1961 (Anti Bribery laws) 	Procurement and Outsourcing, Travel and Sensitive Expenditure, Board Charter and Code of Conduct (Employee and Board)
<ul style="list-style-type: none"> New Zealand Superannuation and Retirement Income Act 2001 (including Minister's Directions and Consents) (Delegations and Authorities) 	Human Resource, Communications, Risk Management, Travel and Sensitive Expenditure, Procurement and Outsourcing, Externally Managed Investments, Direct Investments, Portfolio Completion & Internally Managed Securities, Strategic Tilting, Derivatives, Investment Risk Allocation
<ul style="list-style-type: none"> New Zealand Superannuation and Retirement Income Act 2001 (including Minister's Directions and Consents) (Reporting/Board Procedure) 	Board Code of Conduct, Board Charter and Communications
<ul style="list-style-type: none"> Official Information Act 1982 and other similar laws in other jurisdictions 	Communications (including Schedule 4: Responding to Official Information Act requests) , Investment Risk Allocation, Procurement

Our Legislative Obligations	How Embedded (Relevant Policies, Procedures, Supercharged)
	and Outsourcing, Travel and Sensitive Expenditure, Direct Investments
• Ombudsman Act 1975	Communications, Procurement and Outsourcing
• Public Records Act 2005 and Public Finance Act 1989 (Record Keeping)	Communications (including Schedule 5: Document and Record Management) Investment Risk Allocation, Procurement and Outsourcing, Travel and Sensitive Expenditure, Direct Investments
• Secret Commissions Act 1910	Procurement and Outsourcing, Board Charter and Code of Conduct (Employee and Board)
• State Sector Act 1988 (s57 Standards of Integrity and Conduct)	Human Resources (Employee Code of Conduct), Communications, Diversity and Inclusiveness
Tax and Accounting Legislation	
• Financial Reporting Act 2013	Risk Management, Communications, Derivatives, Direct Investments, Portfolio Completion
• Goods and Services Tax Act 1985	Risk Management, Derivatives, Direct Investments
• Income Tax Act 2007 and Double Tax Relief Agreements	Risk Management, Derivatives, Direct Investments
• Public Audit Act 2001	Risk Management, Communications, Procurement and Outsourcing, Travel and Sensitive Expenditure
• Public Finance Act 1989	Risk Management, Communications
• Tax Administration Act 1994	Risk Management, Derivatives
• Tax law applying to relevant foreign jurisdictions	Risk Management
Employment Related Legislation	
• Accident Compensation Act	Human Resources
• Criminal Records (Clean Slate) Act 2004	Human Resources
• Crown Entities Act 2004 (s117 CEO appointment, s118 to be a good employer and s119	Human Resources

Our Legislative Obligations	How Embedded (Relevant Policies, Procedures, Supercharged)
Application s84 to 84B of State Sector Act 1988 re superannuation)	
• Employment Relations Act 2000	Human Resources, Flexible Work Practices Schedule
• Employment Relations Amendment Act 2014	Diversity and Inclusiveness
• Equal Pay Act 1972	Human Resources
• Health and Safety at Work Act 2015	Human Resources, Health and Safety Process, Schedule 6, Human Resources section of the Supercharged intranet site, Diversity and Inclusiveness
• Holidays Act 2003	Human Resources
• Human Rights Act 1993	Human Resources, Procurement and Outsourcing, Diversity and Inclusiveness
• Injury Prevention, Rehabilitation and Compensation Act 2001	Human Resources
• Juries Act 1981	Human Resources
• KiwiSaver Act 2006	Human Resources
• New Zealand Bill of Rights Act 1990	Human Resources
• Parental Leave and Employment Protection Act 1987	Human Resources, Diversity and Inclusiveness
• Protected Disclosures Act 2000	Human Resources (Employee Code of Conduct)
• Privacy Act 1993	Human Resources, Privacy Policy Schedule. Communications, Diversity and Inclusiveness
• Smoke-free Environments Act 1990	Human Resources
• Statutory Paid Parental Leave Scheme 2003	Human Resources, Diversity and Inclusiveness
• State Sector Act 1988 (CEO Employment)	Human Resources

Our Legislative Obligations	How Embedded (Relevant Policies, Procedures, Supercharged)
<ul style="list-style-type: none"> Wages Protection Act 1983 and Minimum Wage Act 1983 	Human Resources
<ul style="list-style-type: none"> Waitangi Day Act 1976 and ANZAC Day Act 1966 	Human Resources
Legislation that may be specific to investment or other transactions	
<ul style="list-style-type: none"> Anti-Money Laundering and Countering Financing of Terrorism Act 2009 [Guardians have an exemption which expires 30 June 2018] 	Externally Managed, Direct Investments, Derivatives
<ul style="list-style-type: none"> Commerce Act 1986 	Risk Management, Externally Managed, Direct Investments, Procurement and Outsourcing
<ul style="list-style-type: none"> Companies Act 1993 	Risk Management, Externally Managed, Direct Investments, Expenditure/Outsourcing, Derivatives
<ul style="list-style-type: none"> Contracts (Privity) Act 1982 	Risk Management, Externally Managed, Direct Investments, Expenditure/Outsourcing, Portfolio Completion & Internally Managed Securities, Derivatives
<ul style="list-style-type: none"> Contractual Remedies Act 1979 	Risk Management, Externally Managed, Direct Investments, Expenditure/Outsourcing, Portfolio Completion & Internally Managed Securities, Derivatives
<ul style="list-style-type: none"> Copyright Act 1994 and Confidentiality Obligations 	Risk Management, Externally Managed, Direct Investments, Travel and Sensitive Expenditure, Procurement and Outsourcing, Portfolio Completion & Internally Managed Securities, Communications
<ul style="list-style-type: none"> Electronic Transactions Act 2002 	Procurement and Outsourcing
<ul style="list-style-type: none"> Employment related legislation 	Externally Managed, Direct Investments,
<ul style="list-style-type: none"> Environment related legislation 	Externally Managed, Direct Investments
<ul style="list-style-type: none"> Fair Trading Act 1986 and law of representations 	Externally Managed, Direct Investments, Portfolio Completion & Internally Managed Securities, Derivatives, Procurement and Outsourcing
<ul style="list-style-type: none"> Financial Advisers Act 2008 and Financial Service Providers (Registration and Dispute 	Externally Managed, Direct Investments, Portfolio Completion & Internally Managed Securities

Our Legislative Obligations	How Embedded (Relevant Policies, Procedures, Supercharged)
Resolution) Act 2008 [NB Guardians are exempt from NZ requirements]	
• Frustrated Contracts Act 1944	Externally Managed, Direct Investments, Portfolio Completion & Internally Managed Securities, Derivatives
• Our Governing Legislation	Externally Managed, Direct Investments, Portfolio Completion & Internally Managed Securities, Derivatives
• Illegal Contracts Act 1970	Externally Managed, Direct Investments, Portfolio Completion & Internally Managed Securities, Derivatives
• Limitation Act 2010	Procurement and Outsourcing
• Overseas Investment Act 2005 (NZ) and Foreign Investment Review Board (FIRB) (Australia) and other similar laws in other jurisdictions	Externally Managed, Direct Investments, Portfolio Completion & Internally Managed Securities, Derivatives
• Protected Disclosures Act 2000	Human Resources
• Reserve Bank of New Zealand 1989 (Non-bank deposit takers)	Externally Managed, Direct Investments, Portfolio Completion & Internally Managed Securities
• Secret Commissions Act 1910	Externally Managed, Direct Investments, Portfolio Completion & Internally Managed Securities, Code of Conduct (Board and Employee)
• Property Law Act 2007	Externally Managed, Direct Investments, Derivatives
• Financial Markets Conduct Act 2013 (including futures regulation) and NZX Rules	Externally Managed, Direct Investments, Portfolio Completion & Internally Managed Securities, Code of Conduct, Securities Trading Procedure – Insider Trading, Substantial Security Holder and Market Manipulation (Board and Employee) , Strategic Tilting
• Takeovers Act 1993 and Takeovers Code	Externally Managed, Direct Investments, Portfolio Completion & Internally Managed Securities, Derivatives
• Tax and Accounting legislation	Externally Managed, Direct Investments, Portfolio Completion & Internally Managed Securities

Our Legislative Obligations	How Embedded (Relevant Policies, Procedures, Supercharged)
Investment Vehicle Structures	
• Co-operative Companies Act 1996	Externally Managed, Direct Investments
• Companies Act 1993	Externally Managed, Direct Investments
• Limited Partnerships Act 2008	Externally Managed, Direct Investments
• Incorporated Societies Act 1908	Externally Managed, Direct Investments
• Insurance (Prudential Supervision) Act 2010	Externally Managed, Direct Investments
• Life Insurance Act 1908	Externally Managed, Direct Investments
• Partnership Act 1908	Externally Managed, Direct Investments
Other	
• Flags, Emblems and Names Protection Act 1981	Communications
• Dumping and Countervailing Duties Act 1988	Procurement and Outsourcing

Approved by Chief Executive on 21 July 2014 and amended 8 December 2016

Schedule 13: Reporting Framework

Report	Reporting frequency required and to whom	Minimum information required
Performance against relevant risk limits (as per Risk Appetite Statement)	At each Board meeting	<ul style="list-style-type: none"> Actual risk against appetite.
Audit plan	Annually to the Audit Committee	<ul style="list-style-type: none"> Scope and timing of planned audits.
Audit reports	To subsequent Audit Committee meetings.	<ul style="list-style-type: none"> Objectives and scope; Observations and recommendations; Follow up activity.
Strategic Plan	Annually to the Leadership Team and Board	<ul style="list-style-type: none"> Mission, vision, values, strategies, change plans, financial forecasts, key risks.
Progress with Strategic Plan implementation	Biannually to the Leadership Team and Board	<ul style="list-style-type: none"> Progress with key initiatives and status.
Key person risk	Annually to the EPRC	<ul style="list-style-type: none"> Key roles, speed cover is required, mitigation and short term options to cover
Fraud incidents and planned investigations	Incidents advised immediately to the CEO, reports of proposed investigation to CEO and subsequent Audit Committee	<ul style="list-style-type: none"> Details of concern; Proposed investigation timeline; Any interim action.
Fraud investigation reports	To CEO and subsequent Audit Committee	<ul style="list-style-type: none"> Names and responsibilities of those involved; Details of the fraud, cause and remedial action taken; Any planned next steps.
Tax position	Quarterly to the Audit Committee	<ul style="list-style-type: none"> NZ tax payments and effective tax rate; Disputes or significant transactions; Foreign tax position.
Learning Opportunities	To CEO, Risk Committee and subsequent Audit Committee (if extreme or above impact rating)	<ul style="list-style-type: none"> Details of incident, causes, action being taken.
Learning Opportunities	Quarterly summary to the Audit Committee	<ul style="list-style-type: none"> Summary of incidents in the quarter, action taken to resolve, any material outstanding items.
Compliance certification	Six monthly to the Audit Committee	<ul style="list-style-type: none"> Compliance with policies
Legislative Compliance Framework Review	At least every 5 years, directed by Head of Internal Audit to the Audit Committee	<ul style="list-style-type: none"> Report on continued suitability, adequacy and effectiveness of framework.
Policy breaches	If material: immediately to RC and Board Otherwise: to subsequent RC, AC and Board meetings	<ul style="list-style-type: none"> Details of breach and remedial action taken
Material changes to Schedules of this policy	To subsequent RC and Board meetings	<ul style="list-style-type: none"> Details and reason for change.
Acceptance of High or Moderate Residual Risks	To the Risk Committee and Board meeting (High Risk only) following acceptance in accordance with the risk register review timetable.	<ul style="list-style-type: none"> Risk description Risk rating Controls or mitigations (if any) Rationale for acceptance

		<ul style="list-style-type: none"> • Who has accepted the risk
Acceptance of “Low” Residual Risks	To the Risk Committee following acceptance in accordance with the risk register review timetable	<ul style="list-style-type: none"> • Risk description • Risk rating • Controls or mitigations (if any) • Rationale for acceptance • Who has accepted the risk
Cyber Security Risks	Quarterly to the Risk Committee, Leadership Team, and Board	<ul style="list-style-type: none"> • Capability maturity status • Near misses or incidents • Status of key controls
Enterprise Risks	Biannually to the Risk Committee and Board	<ul style="list-style-type: none"> • Top risks • Emerging risks • Key risks identified by business units • Project risks • Operational Risk Assessments

Approved by Board on 16 June 2012, amended 6 August 2019, and 26 February 2020