Risk Management Procedures

This procedures manual sets out the specific guidelines used by Guardians management to enable the effective implementation of the principles contained in Risk Management Policy

Procedures Owner: Chief Risk Officer

Approved by CEO: 25 March 2024

Background

This procedures manual sets out the specific guidelines used by Guardians management to enable the effective implementation of the principles contained in the Risk Management Policy (the Policy).

Definitions

There is a standalone Glossary of Terms, located on the intranet which defines all investment and technical terms used in our policies and procedures. In this procedure the first instance of any such defined term is highlighted in **bold**. References to other documents are italicised.

Risk Matters

The frameworks in this document have incorporated the key themes from our Risk Matters cube. That is we, as individuals and as The Guardians, are:

- Quick to react to risk, opportunities and threats, and confident to raise bad news promptly
- Comfortable challenging attitudes, ideas or actions, and openly discuss and learn from past mistakes
- Strategy and risk appetite are aligned and there is a common understanding of risk and risk management
- Leadership exemplify positive risk behaviours, encourage positive risk behaviour and commit to ethical principles
- Understand risks being taken, are empowered to take on risk and consider its broader impacts
- Appropriate training and guidance is provided on risk management, and the tools and processes are fit for purpose.

Enterprise Frameworks

The Guardians maintain and adhere to frameworks to give effect to Section 4.1 of the Risk Management policy.

Schedule 1: Fraud, Bribery and Corruption

Fraud, Bribery and Corruption: ensures we minimise the potential for fraud and unethical or corrupt behaviour, and ensures any instances are identified and properly managed.

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.

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

1. The Chief Risk Officer is the designated Fraud Control Officer. The Chief Risk Officer maintains a Whistleblowing and Fraud Response Plan that is reviewed annually. 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 Risk, Head of Internal Audit and General Counsel

1.1 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

1.2 All gifts and hospitality must comply with the guidance outlined in the Guardians Employee Code of Conduct (part of the People & Culture Policy).

Facilitation payment

1.3 Facilitation payments are usually another name for a bribe.

1.4 We do not make, and will not accept, facilitation payments of any kind.

1.5 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.

1.6 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 Strategy and Shared Services.

1.7 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 Strategy and Shared Services at the first available opportunity.

Sponsorships and Donations

1.8 Payments for sponsorships can only be made in accordance with the criteria outlined in our Communications and Engagement Policy.

1.9 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.

1.10 Investments, Investment Partners and Suppliers

1.11 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 Direct and Externally Managed Investment Policy and Procurement and Outsourcing Policy is adhered to.

Whistleblowing

1.12 We operate a Whistleblowing procedure in accordance with the requirements of the Protected Disclosures (Protection of Whistleblowers) Act 2022 to protect employees who report serious wrongdoing against retaliatory action. Refer to the Employee Code of Conduct (part of the People & Culture Policy) for more information or the Whistleblower and Fraud response Plan (on the intranet)

Reporting and Prosecution

1.13 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 Whistleblowing procedure referred to above, including the confidential external whistleblowing 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 Chair of the Board or the Audit Committee.

1.14 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 Chief Executive Officer.

1.15 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.

1.16 A Whistleblowing and Fraud Response plan is in place which outlines the process the Guardians will follow when responding to a potential fraud event. The Whistleblowing and Fraud Response Plan also outlines who is expected to do what in the event that a suspected fraud is reported.

1.17 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.

1.18 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.

1.19 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.

1.20 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.

1.21 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.

1.22 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

1.23 Management are responsible for ensuring all staff are trained and regularly updated regarding their responsibilities in preventing and detecting fraud, bribery and corruption.

1.24 The General Manager Risk is responsible for making sure fraud training occurs at least every two years.

Fraud, Bribery & Corruption Risk Assessment

1.25 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

1.26 Actions to improve controls are agreed and implementation monitored through the standard audit tracking process.

Schedule 2: Learning Opportunities

Internal Learning Opportunities: Completing Learning Opportunity Reports enables continuous improvement of risk management practices by operating an open, honest, no-blame culture and ensure Learning and Opportunity reports are submitted, analysed and actions resolved on a timely basis.

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.

2.1 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

2.2 A "near miss" is an event that has not lead to an actual loss but could have.

2.3 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.

2.4 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:

- People and Culture related issues are covered by the *People & Culture 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

2.5 We will complete an LOR where:

- Financial impact >=$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.

2.6 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

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

- For Learning and Opportunities where the risk is considered not “High” 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. These will be noted as reviewed and “not High”;
- A full report will 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 & Risk Committee.

2.8 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.

Schedule 3: Business Continuity

Business Continuity Management: aims to protect the welfare and safety of staff at all times, protect our resources and our reputation. It also ensures we have the ability to provide timely key resources to continue to operate critical business processes.

3.1 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.

3.2 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).

3.3 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.

3.4 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.

3.5 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).

3.6 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.

3.7 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 Technology.

3.8 We test our BCM capability at least annually, in accordance with the testing programme managed by the Head of IT.

Schedule 4: Model Oversight

Model Oversight: *the process allows us to minimise our exposure to model risk as well as setting standards for the business to ensure long term a more robust model environment.*

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.*

4. The definition of models also includes critical complex spread sheets identified by the Business or Risk Committee which could potentially expose the Guardians to material risk.

4.1 Material models are those that are identified as key controls and/or support key investment/business decisions.

Model Oversight Framework

4.2 A list of all models and key spreadsheets (as determined by the business) will be maintained by the Risk team. The list will be updated on an annual basis by the Risk team. Models will be included in a formal review process where there is materiality and/or complexity risk to the Guardians.

4.3 Models not included in the formal review process will be maintained in the models list noted above.

4.4 The high level structure of the review framework is:

1) <u>Model Inputs</u>: Data quality, Input control, Ongoing monitoring, Data licensing.
2) <u>Model Calculation</u>: Theoretical construction, Key assumptions and limitations, Model design/code/process validation.
3) <u>Model Outputs</u>: Outcomes analysis, performance and stability, Output control, Ongoing monitoring.
4) <u>Model Operation</u>: Documentation, Version control/change control, Access control, Skills, Business continuity plans.

4.5 Model reviews must be completed using the model review template, available on the Risk Committee intranet page. The template sets minimum standards for models are adhered to.

4.6 A set of good practice guidelines for models has been developed. Refer to guidelines on SuperCharged under Working at the Guardians in the Risks, Opportunities, Audits Section, called Model Risk standards.

Model Risk Assessment

4.7 A model's risk will be assessed for materiality and complexity.

Model materiality is based on:

- Maximum size of the investment decisions that model output feeds into;
- Maximum size of the business decisions (other than investment) that the model

output feeds into; and

- Frequency of use of the model.

Model complexity is based on:

- What system does the model run on;
- Is the model developed by a third party;
- How many staff are able to rewrite the model; and
- How many staff are able to use the model.

Model review frequency, approach and certification

4.8 The Risk team, in agreement with the business, will assess the materiality of the risk of the models used by the business. The Risk team will agree with the General Manager Risk annually a selection of those models to be reviewed.

4.9 The resources for the proposed review will be determined by the Risk team in liaison with the General Manager with ownership of the model. Any proposal to use internal reviewers will ensure that the reviewer are of appropriate skill, capability and independence for the review of the model.

4.10 Where a new model has been developed, or an existing model upgraded, with the assistance of the Data Analytics team and has been certified as meeting the model development standards by the Head of Data Analytics, the model will have a three year period of non-review by the Risk team. That certification will be void if there is a LOR raised on the model by the model developer or a user.

Committee Oversight

4.11 The Risk Committee shall oversee the Model Review Framework to ensure the effective operation of model oversight processes. The outputs from the review of models will be tabled and reviewed by the Risk Committee annually 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, groups or Internal Audit that have a specific interest in the effective operation of the model.

Schedule 5: Responsibilities

GM Risk will:	• ensure this policy is kept current and relevant to the activities being undertaken (including schedules 1-4, 10, 13) • ensure this policy is reviewed every five years • ensure that the form of compliance certification is reviewed at least annually • report compliance certification six monthly, to the Audit & Risk Committee • ensure fraud training is conducted at least every two years ensure schedule 7 (fraud risk framework) is kept current and relevant to the activities being undertaken
Head of Risk will:	• 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 • Ensure Schedule 11 (model oversight framework) is kept current and relevant to the activities being undertaken
GM Technology will:	• 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
Fraud Control Officer will:	• review Fraud, Bribery & Corruption Risk Assessment every two years
Head of Technology Services will:	• 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
General Counsel will:	• 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 People & Culture will:	• maintain records of relevant mandatory training • review key person risk at least annually • report assessment of key person risk annually to the ERPC