Risk Management Policy
Te Kaupapa Here Aroā Tūraru

This policy covers the Guardians Risk Appetite and its risk frameworks to implement effective controls, and frameworks to ensure risks are managed effectively and in compliance with our governance and legislative requirements. Specific guidelines for applying the principles set out in this Policy are contained in the Risk Management Procedures.

GUARDIANS OF OUR FUTURE

Policy Owner:

General Manager, Risk

1. Purpose and Scope

1.1 This policy covers the Guardians Risk Appetite and its risk frameworks to implement effective controls, and frameworks to ensure risks are managed effectively and in compliance with our governance and legislative requirements.

1.2 This policy is part of the Guardians' governance framework that is designed to meet the legislative requirements of the New Zealand Superannuation Fund (the Fund) and the Elevate NZ Venture Fund (Elevate). Investment risk is further defined in the *Investment Risk Allocation Policy*. Investment operational matters are covered in the investment related policies and procedures and may also be subject to the Risk Assessment Framework.

2. Definitions

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

3. Policy

3.1 **Risk governance:** Taking and managing risk is an integral part of doing business and the Board is committed to effective governance of its operations in the pursuit of its objectives. The Board's core intention in the risk appetite statement sets out our approach to risk.

"The Board is willing to take risk to achieve the Guardians' Purpose; it expects the Guardians to continue to use all reasonable measures, without imposing excessive costs or constraints, for its management of the four categories."

The risk appetite recognises that risk, internal and external, to our business is likely to come from a range of causes. For these risks, how the Guardians respond falls into four broad categories: Culture, Governance, People, and Processes.

3.2 **Risk Appetite Statement and associated frameworks**: The Policy contains four schedules:

- Schedule 1 sets out the full **Risk Appetite Statement** and details the roles of the Board and Management.
- Schedule 2 sets out the **Risk Management Framework** to ensure we operate within our agreed Risk Appetite. The risk management process will be evident whenever key decisions are made. The risks are identified and evaluated with effective responses and control activities are developed for these risks. There will also be appropriate monitoring and timely re-evaluation of risks. Creating and maintaining a culture consistent with our risk management framework is an important element of risk management, as are our selection and recruitment processes.
- Schedule 3 sets out the **Risk Assessment Framework** to assist us with determining our risk appetite and how we will respond to risks we have identified based on the four categories set out in the Risk Appetite Statement. Ensuring a consistent approach to our risk assessment is an important element of the framework. The framework ensures that the risk categories are defined and the questions we need to ask ourselves are set out. The Guardians have core

expectations and appropriate monitoring, maintenance and reporting of our risk appetite assessments.

- Schedule 4 covers the **Guardians' Policies Framework** - the development, implementation and maintenance of policies are key to our control environment and compliance programme. These are the 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.
- Schedule 5 is the **Reporting Framework** and provides visibility on what is reported to the Board, who is accountable, the frequency and the minimum information that must be provided.

4. Procedures, Standards and Related Policies

4.1 Management will establish, maintain and adhere to procedures that incorporate the principles set out in this Policy and that are appropriate to the Fund or Elevate and consistent with the relevant statutory investment mandate. Management will attest that the Guardians' policies and procedures remain up to date, complete and are being applied.

4.2 For details of all the procedures referred to in to 4.1 of this policy and guidance on their application staff should refer to the associated Risk Management Procedures located on the Guardians' intranet.

4.3 The *Investment Risk Allocation Policy* contains the principles related to investments risks and the investment constraints set out by the Board. The *Communications and Engagement Policy* defines our "no surprises" policy to keeping the Board and Minister of Finance informed of any material or significant events.

5. Reporting

5.1 The reporting framework for this Policy is set out in Schedule 5.

6. Policy Approval and Review

6.1 This policy was reviewed by the Board on 23 November 2023 and 22 February 2024 and approved on 22 February 2024. This policy and procedures will be reviewed every five years as part of the cycle for reviewing Guardians policies and procedures. The next review will be in 2028.

7. Delegations

7.1 The *Delegations Policy* governs the delegation of authority for matters relevant to this policy.

Schedule 1: Risk Appetite Statement

1. The Risk Appetite Statement

1.1 The Board has set the following as its Risk Appetite Statement:
The Guardians of New Zealand Superannuation has developed into, and has a strong ambition to remain, a world class organisation with a purpose that reflects its intergenerational focus.

In setting out its risk appetite the Board recognises that risk, internal and external, to its business is likely to come from a range of causes. For these risks, how we respond falls into four broad categories: Culture, Governance, People, and Processes.

The Board is willing to take risk to achieve the Guardians' Purpose; it expects the Guardians to continue to use all reasonable measures, without imposing excessive costs or constraints, for its management of the four categories.

Our risk appetite will be determined by the Guardians' Purpose and Vision, with Investment Risk managed by the adoption of the Reference Portfolio and approved Investment Constraints; and Enterprise Risk is managed by the Risk Assessment Framework.

1.2 The Guardians' Purpose is - "Sustainable investing delivering strong returns for all New Zealanders".

1.3 The Guardians' Vision is - "An inclusive team creating a better future through investment excellence".

2. Role of the Board of the Guardians

2.1 The Board is responsible for setting risk appetite and providing risk governance oversight at the Guardians, (the management of risk sits with the Guardians' management). For this, it has developed a process for delegating authority to the CEO and beyond. This ensures that there is accountability for risk within management at the Guardians and that there is a response plan in place to act upon risks in a timely manner.

2.2 The Board expects that management operates a "no surprises" approach for risk and also expects that the Leadership Team will seek Board input if it does not have the Board's delegated authority to respond to certain types of risk.

2.3 The Board has agreed a set of Policies that sets out what is reserved to the Board and what has been delegated to Guardians management. The CEO and the management team attest that management has complied with these Policies on a semi-annual basis.

3. Role of Management of the Guardians

3.1 The Risk Appetite Statement guides management in:

- operating the Guardians;
- managing and administering the Fund and Elevate in accordance with the requirements of their respective Act; and
- delivering on the strategic objectives of the Guardians as set by the Board.

3.2 The management of risk sits with the Guardians' management.

4. Assessing risks against Risk Appetite

4.1 The Board's Risk Appetite Statement is applicable across the activities of the Guardians.

4.2 The Board expects Management to manage, measure and monitor the actual risk profile of the Guardians and Fund against its Investment Constraints detailed in the Investment Risk Allocation Policy and using the Risk Governance Frameworks detailed in this Policy.

4.3 The Board also actively monitors the health, safety and environmental governance compliance of certain investee companies as specifically reported to the Board in the annual Direct Assets Health and Safety Report.

4.4 Management will identify key risk indicators (and perform stress testing and scenario testing where appropriate) to assist the Board to assess the Fund, Elevate and Guardians' exposure to the key risks that it has identified.

4.5 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.

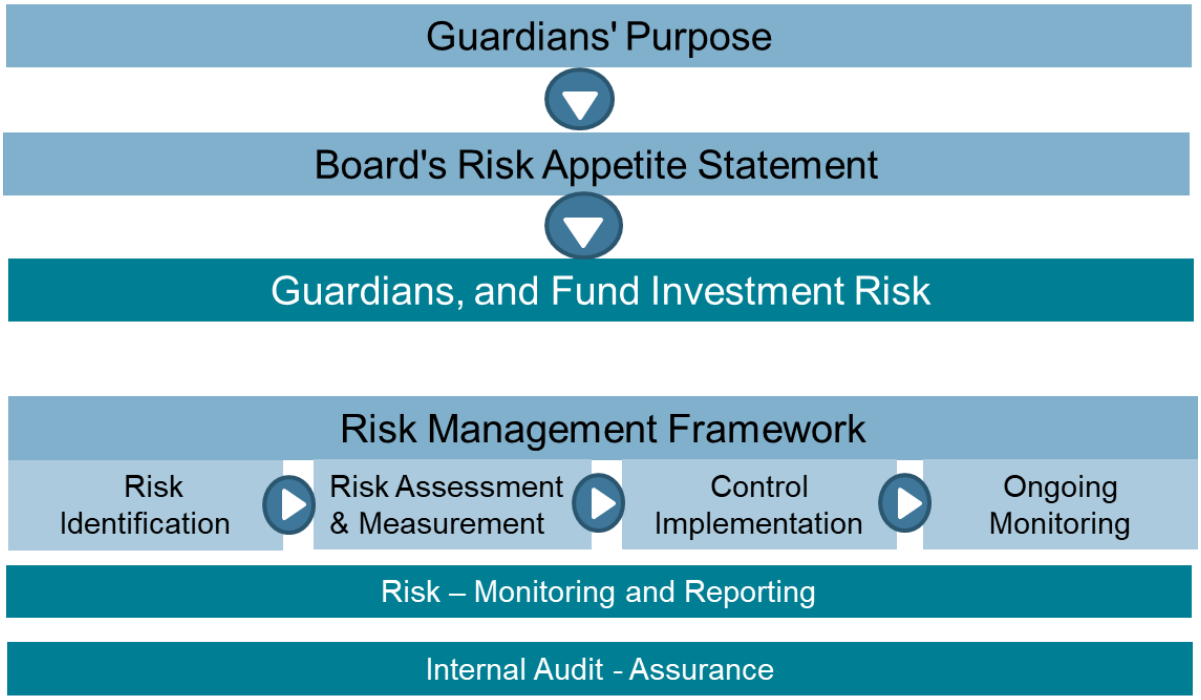
4.6 The Board requires Management to effectively communicate the Risk Appetite Statement to all staff and contractors at the Guardians and external stakeholders.

4.7 To ensure the Guardians and the Fund are operating within the Risk Appetite Statement, Management has developed reporting to show it has operated within the Investment Constraints and used the Risk Assessment Framework to reach decisions about risk appetite for Enterprise risks.

Schedule 2: Risk Management Framework

Risk Management is to ensure we operate within our agreed Risk Appetite (Figure One – Risk Management). The risk management process will be evident whenever key decisions are made. The risks are identified and evaluated with effective responses and control activities are developed for these risks. There will also be appropriate monitoring and timely re-evaluation of risks. Creating and maintaining a culture consistent with our risk management framework is an important element of risk management, as are our selection and recruitment processes.

1 Figure One: Risk Management



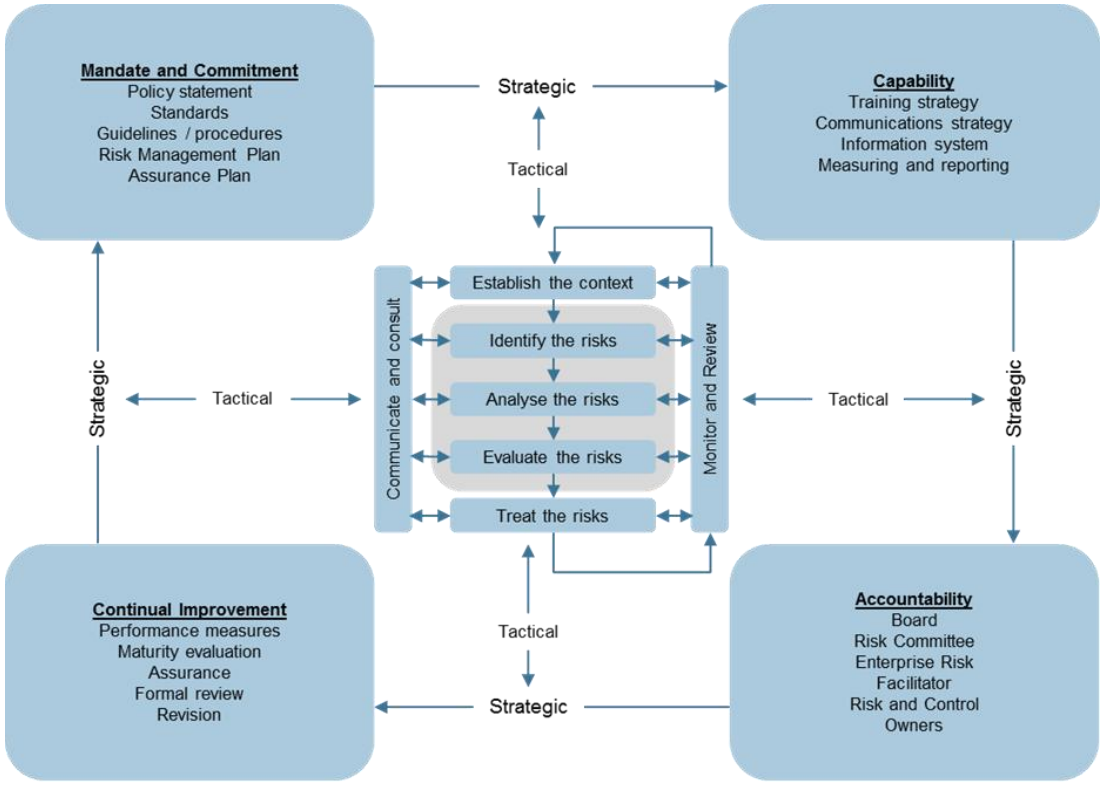
1.1 Our approach to risk management is based on the following core elements:

- The Board establishes the risk appetite; this is captured in the risk appetite statement.
- The risk appetite is reflected in policies that are approved by the Board and is given effect by Management through the development, maintenance, and adherence to of procedures for each of the policies.
- Management ensures the policies are implemented and maintained for identification, monitoring, measurement, and management of all relevant risks.
- Internal Audit and Risk functions provide assurance to the Board and Audit Committee of performance against internal controls and risk management systems.
- Periodically we will assess the Guardians' risk culture, reporting on outcomes and acting where necessary.

1.2 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.

1.3 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 Two.

2 Figure Two: Risk Management Framework Process



2.1 At the core of our risk management framework is the process of risk identification, risk analysis, risk control effectiveness and risk appetite determination. all overlaid with a strong risk culture 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

2.2 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

2.3 The materiality of these events is determined by using the Risk Assessment Framework on our stated objectives and ability to respond to them. Risk Analysis is undertaken through the Enterprise Risk Report, Business Unit Risk Registers, Business environment scans, emerging risks assessments, New Investment Initiatives (Operational Risk Assessments) and Project Risk Assessment.

Stage 3 Control effectiveness rating

2.4 This stage is to analyse the effectiveness of existing controls in managing risks. Controls may include policies, procedures, standards, processes and codes of practice.

2.5 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 Risk Appetite Application

2.6 Risk appetite involves assessing the level of risk for each identified risk after consideration of how we will respond to the risk.

2.7 The **Risk Assessment Framework** is outlined in Schedule 3 of this Policy.

2.8 To promote transparency and clear accountability, the process we use for managing the acceptance of enterprise risk is set out below:

a. The materiality of risk will determine who has the power to accept our appetite for the risk. Those authorised to determine our risk appetite is set out in the Delegations Policy.

b. For consistency our Risk Assessment Framework is used for determining risk appetite.

c. The relevant General Manager ensures all material risks are updated into the business unit's risk register.

d. Transaction or project specific risks are recorded in either the operational risk assessment (ORA) for the transaction, the Project Plan for a major project or programme initiative (e.g. IT project) or other relevant documentation supporting the transaction.

e. Where risk is deemed material, in addition to the risk owner recording the item in the business unit's risk register, Enterprise Risk ensures the risk is considered for inclusion into the Enterprise Risk Report for review by the Risk Committee and, subsequently, the Board.

f. Risk assessment documentation is to be kept in an Approved Information Management System which is accessible by the relevant General Manager and

to the Risk team to clearly evidence the acceptance of the risk by the approver and the reasons for the acceptance. .

g. The authority to determine material risk appetite is role specific and cannot be delegated by a General Manager or Head of Business Unit to any other person.

h. The application of risk appetite is periodically reviewed in accordance with the timeframe specified in the Risk Committee business unit risk register review calendar. The application of risk appetite should be reviewed at least bi-annually.

i. As part of the six-monthly risk review cycle, Enterprise Risk Reports are updated to include material risks and other relevant risks that have been accepted by a business unit.

2.9 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 rests with the Risk Committee.

2.10 The Risk Committee is composed of relevant subject matter experts from within the appropriate functional areas of the Guardians and when assessing risks it aims to identify risks that individual business units might not identify (by reason of not seeing the whole-of-Guardians perspective) and to ensure risks are treated consistently across Business Units.

Training

2.11 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.

2.12 The Risk Committee evaluates the risks referred to it in terms of materiality of risk as well as effectiveness of existing controls or treatments, and where necessary, the implementation of additional controls. It recommends appropriate courses of action directly to the relevant business units, who are then responsible for incorporating the required risk mitigating activities into their business plans. The Risk Committee monitors implementation of its recommendations.

2.13 If new controls and treatments cannot be accommodated within existing resources they are referred to the Leadership Team for resourcing and prioritisation.

2.14 The Risk Committee will oversee the periodic risk culture survey and the implementation of any recommendations or opportunities for improvement.

Schedule 3: Risk Assessment Framework

Risk Assessment assists us with determining our risk appetite and how we will respond to risks we have identified based on the four categories set out in the Risk Appetite Statement. Ensuring a consistent approach to our risk assessment is an important element of the framework. The framework ensures that the risk categories are defined and the questions we need to ask ourselves are set out. The Guardians have core expectations and will maintain appropriate monitoring and reporting of our risk appetite assessments.

The Guardians has adopted a framework for how it responds to risk based on the categories articulated in the Risk Appetite Statement. In the Risk Appetite Statement, the Board expects *"the Guardians to continue to use all reasonable measures, for its management of the four categories",* they are Culture, Governance, People, and Processes. The Risk Assessment Framework helps achieve consistency across the Guardians. The following guidelines assist with the self-assessment of our risk appetite:

Why should the Guardians be concerned?

- How does this align with our objectives or priorities?
- Is there something unique/new?
- Have we done this before? but don't ignore changes to environment since last considered
- Are the measures in place or required reasonable and achievable without excessive cost or constraint?
- Do we have/need measures to respond to events outside our control?
- Have we considered the 2nd or 3rd order impacts arising?

The key principles to help this happen:

- High quality conversations about things that matter, as early as possible
- Get the right people in the room*
- Don't avoid risk, optimise it. We want to be deliberate in our risk-taking
- Always consider down-stream and wider impacts across the Guardians
- Document key points from the conversation and actions decided

* *This should include risk 'owner(s') + others with a valuable perspective (multiple perspectives and objectivity to minimise bias) and those who will be impacted by those decisions or choices.*

It is important to consider the "materiality" of the risk in the decision that is being made. In following the guidelines and principles above, we expect people to use their judgement. It is important to consider the impact on the Guardians or the Fund or Elevate as to who should make the final decision and the right people have been engaged on the risk appetite being taken. As a decision maker you must be aware of your own level of **Authority** and **Responsibility.**

Guidance on some areas that the Guardians are not looking to take risk in:

- Conflicts of interest
- Health and Safety
- Gifts and Hospitality
- Personal securities trading

The Risk Assessment Framework articulates the attributes of the categories in the Risk Appetite Statement, what questions management must ask itself as a minimum in assessing the risks, and what our core expectations are. These are outlined in the following table.

Response	Attribute	Question	Core Expectation
Culture	Culture, Values of a world class organisation	Does our leadership promote a culture of risk informed decision making on clear understanding of acceptable/unacceptable risks and consistent with our values	Organisational behaviours and values clearly support risk informed decision making
	Continuous improvement	Does drive continuous improvement in risk management	There is a regular review cycle to identify improvements and a formal process to document, share and reflect on lessons learned
Governance	Leadership, Policies and Authorities	Is there clear accountability and authority	Governance framework in place that explicit assigns individual roles and authorities for managing risks
	Strategic Focus areas risk management	Is there effective anticipation & management of risk as we develop our strategic priorities	Strategic priorities and risks are explicitly identified and documented in the Strategic Plan together with planned responses
	Managing risk in relationships	Are there effective arrangements to manage risk for/from our stakeholders and partners	This is a process that addresses how to identify, assess and manage risks, including arrangements for risk ownership and sharing of information
	Business resilience	Are there effective mechanisms to respond	Disruptive events or scenarios are tested for on a regular basis and there are mechanisms in place to respond to a range of events or scenarios

Response	Attribute	Question	Core Expectation
People	Roles and responsibilities	Do staff clearly understand roles and responsibilities for managing risk	Roles and responsibilities are documented, communicated for all areas and are consistently reflected in job descriptions
	Resources, skills and training	Are resources sufficient & are staff adequately trained and experienced	Roles are adequately resourced with assessment of skills, appropriate inductions and training needs undertaken on a regular basis
	Change and transformation	Is there a whole of Guardians' approach to managing risk for significant change initiatives	There is risk assessment process for approving and managing significant change initiatives based on a Guardians' wide view of the risks related to change and transformation
Processes	Assessment and Mitigation	Are there effective processes for identification, assessment and mitigation of risk	Assessment processes are applied consistently across the Guardians and mitigation plans aligned to risk appetite
	Control Effectiveness	Are there frameworks in place to provide assurance of risk controls	Assurance is provided over mitigation plans and control effectiveness is assessed by Enterprise Risk and/or Internal Audit
	Monitoring and reporting	Does monitoring and reporting support decision making and management action	Board and Leadership Team receives: 1) risk information aligned to business outcomes to support decision making and management action; and 2) sufficient information to assess how the Guardians risk appetite is being applied
	Technology and infrastructure	Do we have fit for purpose technology and/or business systems	Infrastructure, systems and data are suitable for the strategic priorities of the Guardians

Schedule 4: Guardians' Policies Framework

Policies: *the development, implementation and maintenance of policies are key to our control environment and compliance programme. These are the 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.*

Policy statements are approved by the Board and may only be altered by the Board. Management is responsible for developing and adhering to standards and procedures to meet the requirements of those statements. The Board has full visibility of those standards and procedures covered by policies set out in the legislation through the annual review of the Statement of Investment Policies, Standards and Procedures.

Responsibility for Policies

4.1 Each policy has an 'owner', either a General Manager or the CIO. Owners are responsible for initiating and co-ordinating changes to their policy as required to ensure it remains up to date considering 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 or GM Corporate Affairs. Changes to policy statements or policy schedules (other than schedules approved by the CEO) are then reported to the Board for approval as required by the policy.

4.2 Policies are fully reviewed by the policy owner in accordance with the policy review timetable set by the Board. Inside that review timetable the policy owner also:

- Attests six monthly to the Chief Executive Officer their policy and related procedures remain up to date and complete; and
- Certifies that a review has been completed for the annual Statement of Policy, Standards and Procedures legislative requirement. A policy owner may rely on certifications by subject matter experts and other staff as to the accuracy and completeness of the content.

4.3 General Counsel is responsible for maintaining a record of policy owners.

Monitoring and Assessment of Policy Compliance

4.4 All staff have the following objectives in their role descriptions:

- Demonstrate appropriate knowledge and use of all Guardians' systems and processes.
- Understand and comply with all Guardians' policies and procedures, including those relating to risk management and compliance practices.
- Champion the Guardians' values and constructive culture at all times.

4.5 All staff attest to their manager, compliance with key policy requirements as set out in the six-monthly Attestation form. The form of attestation is developed and reviewed annually by the Head of Risk. Attestations include cross references to the relevant policies.

4.6 The Chief Executive Officer certifies to the Audit Committee compliance by the Guardians with the policies on a six-monthly basis, and that the policies and procedures remain up to date, complete and are being applied.

4.7 In addition to attestation, we 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

4.8 All policies are available to all staff on our intranet, and to the Board and the public on our internet site (redacted where necessary). Whenever a new policy is published or an existing policy is materially updated, all staff are informed as part of a communication plans.

Training

4.9 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. Periodic policy reviews also consider whether refresher training is necessary. Training may include presentations to new employees as part of induction, refresher seminars or on the job coaching.

4.10 Staff are required to complete mandatory training on several topics on an annual basis. The General Manager Human Resources maintains records of completion of relevant mandatory training. Failure to complete mandatory training is a gate to bonus payments.

Schedule 5: Reporting Framework

Report	Accountability	Reporting frequency required and to whom	Minimum information required
Policies and procedures	Policy owners	Six monthly to the Audit Committee	• Policy owner attestation
Investee company health and safety	CIO	Annually to the Board	• Risk assessment of the H&S of our investee companies
Fraud incidents and planned investigations	General Manager Risk	Incidents advised immediately to the CEO, reports of proposed investigation to CEO and subsequent Audit Committee	• Details of concern; • Proposed investigation timeline; • Any interim action.
Fraud investigation reports	General Manager Risk	To CEO and subsequent Audit Committee	• Names and responsibilities of those involved; • Details of the fraud, cause and remedial action taken; • Any planned next steps.
Learning Opportunities	Manager, Enterprise Risk	To CEO, Risk Committee, and subsequent Audit Committee (if material)	• Details of incident, causes, action being taken.
Learning Opportunities	Manager, Enterprise Risk	Quarterly summary to the Audit Committee	• Summary of incidents in the quarter, action taken to resolve, any material outstanding items.
Compliance certification	Manager, Operational Compliance	Six monthly to the AC	• Compliance with policies
Policy breaches	Head of Risk	Immediately to RC and Board. Otherwise: to subsequent RC, AC and Board meetings	• Details of breach and remedial action taken
Application of the Risk Appetite Statement	Head of Risk	Annually to the Board and Risk Committee	• The operationalisation and application of the Risk Assessment framework
Enterprise Risk	Manager, Enterprise Risk	Biannually to the Risk Committee, Audit Committee and Board	• Strategic risks • Emerging risks • Material risks identified by business units
Risk registers by business unit	General managers, CIO	At least bi- annually to the Risk Committee as determined by the Risk Committee	• Business environment scan • Control Articulation and Control Effectiveness Review risk
Business continuity	General Manager, Technology	Annually to the Crisis Management Team	• Summary of BCP tests held in the period. • Material changes to the BCP
Scheduled reporting to Risk Committee as per the Risk Committee calendar	Chair, Risk Committee	Annually to the Audit Committee	• Summary of reporting to the Risk Committee