ENTERPRISE RISK MANAGEMENT POLICY

Dates	Policy Takes Effect: 1 March 2022 Policy is Due for Review: 1 March 2024
Approved	KiwiRail Board Meeting: 1 March 2022
Implementation Officer	CFO
Relevant To	All KiwiRail employees. This includes fixed term and temporary or contract employees.
Related Documents	ISO 31000:2018 National Rail Standards System 4 (NRSS) COSO Framework 2017 KiwiRail Enterprise Risk Management (ERM) Manual Delegated Financial Authorities Policy
Publication	KiwiRail Intranet
Policy Supersedes	N/A

Introduction

All business activities involve risk; therefore, it is important that everyone within the organisation takes the same structured and focused approach to managing business risk.

Risk management is a basic concept involving a formal process whereby those risks which threaten the achievement of Strategic, Project and Operational objectives are identified, evaluated, & cost-effectively treated.

As part of the overall Enterprise Risk Management Process, Internal Audit will be engaged to provide assurance to the Board of Directors and GSEC that the risk management process is embedded and effective. As part of this process risk mitigation strategies will identified for review to ensure that KiwiRail has robust response to all risks.

Policy Statement

KiwiRail is committed to providing customers with a quality service and conducting its business in a safe, healthy and environmentally responsible manner.

To protect our employees, the environment, our assets, earnings, markets and reputations we will manage risk as an essential component of operational excellence.

To ensure this, the risk management process will be embedded as a continuous process, demanding awareness and action from all employees at all levels to minimise risks.

Risks will be managed and controlled through KiwiRail's risk management process, which is committed to:

- Identifying the impacts of its activities, or in some cases lack of activity, and the sources of risk;
- Quantifying the relative impacts and risks; and
- Making every effort to control, reduce or remove the impacts of the risks identified by the implementation of practical and cost-effective risk control measures.

Ownership

The KiwiRail Board has the ultimate responsibility for Enterprise Risk Management and has delegated day-to-day operational responsibility to the Chief Executive Officer.

The Risk Audit & Assurance Committee (RAAC) of the Board has the overview of Enterprise Risk Management within its Terms of Reference.

The Executive Team has responsibility for the development and maintenance of the risk management process, risk register and risk mitigation strategies. This team needs to be aware of the risks that may negatively impact KiwiRail's ability to deliver its operational and strategic goals.

The Risk & Assurance Team, with the support of the Risk Steering Group, has responsibility for the development and maintenance of the KiwiRail's risk management framework. This includes ensuring that risks are comprehensively assessed with individual risk registers being regularly reviewed by responsible parties within the business.

This team is also responsible for ensuring that any risk mitigation strategies developed are in place, robust and fit for purpose. This will involve utilising the Internal Audit function to provide appropriate assurances to the Executive Team, RAAC and Board of Directors that KiwiRail's risks are being properly managed.

The Risk Steering Group will provide assurance to the Board of Directors, Executive Team and RAAC about the suitability and relevance of the risk management structures and arrangements.

Divisional/Business Unit Leadership Teams are responsible for ensuring that risks within each of their areas of operations have been identified and quantified, with appropriate risk mitigation strategies developed to manage, minimise or remove the risk identified.

All KiwiRail employees are encouraged to support the activities required to protect KiwiRail people, customers, and assets whilst ensuring their own personal safety.

Risk Management Principles

KiwiRail will follow the following Risk Management Principles to ensure that the process[1] remains valid and relevant:

a) **Integrated** – Risk management is an integral part of all organisational activities.

b) **Structured and comprehensive** – A structured and comprehensive approach to risk management contributes to consistent and comparable results.

c) **Customised** -The risk management framework and process are customised and proportionate to the organisation's external and internal context related to its objectives.

d) **Inclusive** – Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.

e) **Dynamic** – Risks can emerge, change or disappear as an organisation's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.

f) **Best available information** – The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.

g) **Human and cultural factors** – Human behaviour and culture significantly influence all aspects of risk management at each level and stage.

h) **Continual improvement** – Risk management is continually improved through learning and experience

[1] *Principles apply to the process set out in the KiwiRail ERM Manual*

Goals and objectives for risk management

The primary goals for KiwiRail's risk management framework are to support the achievement of maximum sustainable value from all the activities of the organisation, to enhance the understanding of the potential upside and downside of factors that can affect the organisation, and to increase the probability of success of, and reduce both the potential of failure and the level of uncertainty associated with, achieving the objectives of the organisation. Principles that guide KiwiRail's risk management approach will (be):

- Create and protect value.
- Integral part of all organisational processes.
- Part of decision making.
- Address uncertainty explicitly.
- Systematic, structured, and timely.
- Based on the best available information.
- Tailored to meet KiwiRail's strategic and operational objectives.
- Consider human and cultural factors.
- Transparent and inclusive.
- Iterative, and responsive to change.
- Facilitate continual improvement of the organisation.
- Develop and implement strategies to improve risk management maturity alongside all other aspects of their organisation.

Risk Appetite

The amount of risk that KiwiRail is prepared to accept, tolerate, or be exposed to at any point in time.

The risk appetite and any risk appetites for subsidiary units or functions will be set by the Board and GSEC, and communicated to the relevant management teams.

The risk appetite will:

- provide direction and boundaries on the risk that can be accepted within the organisation, how the risk and any associated reward is to be balanced and the likely response;
- considers the organisation's operating environment, understanding of value, cost effectiveness of management, rigor of controls and assurance process;
- recognises that the organisation might be prepared to accept a higher than usual proportion of risk in one area if the overall balance of risk is acceptable;
- defines the control, permissions and sanctions environment, including the delegation of authority in relation to approving the organisation's acceptance of risk, highlighting of escalation points and what the escalation process is for risk outside acceptance criteria.