# Risk Management Policy

## 1. Purpose

The purpose **of risk management** is the creation and protection of value. It improves performance, encourages innovation, and supports the achievement of objectives. Risk management includes both threats and opportunities.

Auckland Transport (AT) recognises that early and systemic identification, analysis and assessment of risks and the development of plans for controlling and mitigating **risk** are necessary to preserve its assets and to meet its objectives consistently, safely, and efficiently.

The purpose of this policy is to:

- Provide the direction for effective and consistent risk management throughout AT across all aspects of its business.
- Demonstrate the commitment to a culture of well-informed risk-based decision making.
- Highlight key roles and responsibilities for risk management.

## 2. Scope

Risk management is the responsibility of everyone who works for and with AT.

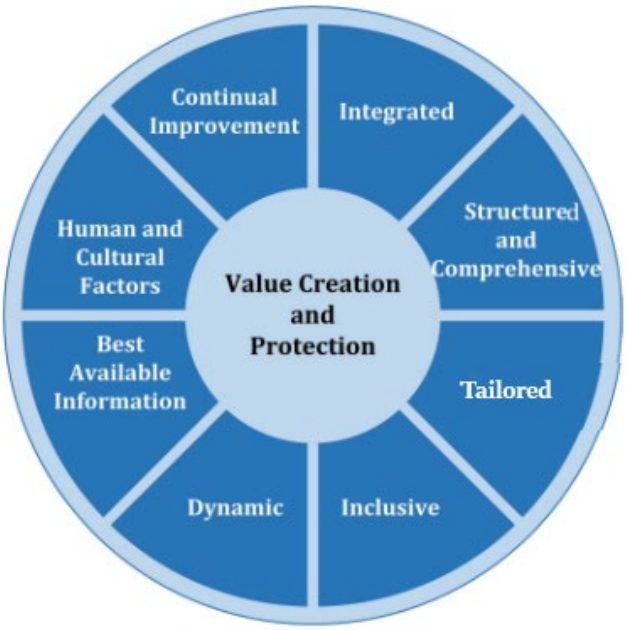
This policy applies to all sources of risk to AT achieving its objectives and is relevant to:

- All AT employees.
- AT representatives:
  - Contractors & consultants (in accordance with the terms of the supplier agreement with AT),
  - Agency temps (in accordance with the terms of the supplier agreement with AT),
  - Staff on secondment from other organisations/agencies,
  - Volunteers.
- The Board of Directors.

Risk management applies in the context of all:

- The social, cultural, political, legal, regulatory, financial, technological, economic, and environmental factors, whether international, national, regional, or local,
- External shareholders' and stakeholders' relationships, perceptions, values, needs and expectations,
- Relationships with internal stakeholders, considering their perceptions and values,
- Key drivers and trends that affect or may affect AT,
- Internal and external contractual relationships and commitments,
- AT assets including people, data, and information,
- Internal and external interdependencies and interconnectedness.

# 3. Policy Principles




The AT risk management approach is applied in accordance with the following principles:

1. **Risk management is integrated.**

   Risk management is a dynamic and iterative process that is an integral part of all AT's organisational activities, and is part of the organisation's purpose, governance, leadership and commitment, strategy, objectives, and operations.

2. **Risk management is structured and comprehensive.**

   AT implements a systematic, comprehensive, and structured approach to risk management to ensure consistent results.

3. **Risk management is tailored.**

   The AT risk management framework and processes are proportionate to the external and **internal context** and risk and related to the objectives of the organisation.

4. **Risk management is inclusive.**

   AT accomplishes informed risk management with the appropriate and timely involvement of **stakeholders** to ensure their input is considered when risks are identified and assessed. This results in improved awareness and informed risk management.

5. **Risk management is dynamic.**

   Risk management takes place in the context of the objectives and activities of the organisation and risks can emerge, change, or disappear and changes occur in the operating environment. AT anticipates and responds to those changes and other events in an appropriate and timely manner.

6. **Risk management includes the best available information.**

   The inputs to risk management are based on historical and current information, as well as on future expectations. AT considers any limitations and uncertainties associated with the information and future. Information must be timely, clear, and available to stakeholders.

7. **Human and cultural factors.**

   The variable and dynamic nature of human behaviour and culture is considered throughout the risk management process.

8. **Continual Improvement.**

   AT risk management is subject to a process of continual improvement as the organisation matures its risk management practices, acknowledges, and addresses **control** gaps reported by audits and reviews, and as new and emerging risk best practice is identified.

# 4. Definitions

| Term | Definition |
|---|---|
| Control<br>(ISO 31000) | Measure that maintains and/or modifies risk[1] |
| Internal context<br>(ISO 73) | Internal environment in which AT seeks to achieve its objectives |
| Risk<br>(ISO 31000) | The effect of uncertainty on objectives |
| Risk appetite<br>(ISO 73) | The amount and type of risk AT is prepared to pursue or retain. |
| Risk management<br>(ISO 31000) | Coordinated activities to direct and control AT with regard to risk.<br><br>The planned and systematic approach to the identification, evaluation and control of risks which threaten the achievement of AT's objectives |
| Risk management framework | The set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring reviewing, and continually improving risk management throughout AT.[2] |

[1] Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.

[2] The foundations include the policy, objectives, mandate and commitment to manage risk. The organisational arrangements include plans, relationships, accountabilities, resources, processes and activities. The risk management framework is embedded within the organization's overall strategic and operational policies and practices. AT has risks frameworks developed specifically for information technology, fraud, safety, procurement, project and programme management and asset management all of which comply with and supplement the overarching Operational Risk Management Framework.

| Term | Definition |
|---|---|
| Risk management process (ISO 73) | The systematic application of policies, procedures, and practices to the tasks of managing the risk lifecycle, specifically establishing the content, identifying, analysing, evaluating, communicating, treating, and monitoring risk |
| Risk tolerance (ISO 73) | AT's or stakeholder's readiness to bear the risk, after risk treatment, in order to achieve its objectives[3] |
| Stakeholder (ISO 73) | A person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity[4] |

# 5. Roles and Responsibilities

| Role | Responsibility |
|---|---|
| All employees and representatives | • Complete the Introduction to Risk Management training eLearning module in ThinkTank.<br>• Adhere to and comply with this policy, the risk management framework, and related procedures.<br>• Understand the risks relevant to their area of responsibility and follow the associated processes and procedures. |
| Management | • Complete Risk Management Framework eLearning Module in ThinkTank.<br>• Actively lead and promote risk aware culture within their business areas and groups.<br>• Responsible for the implementation of risk management in their area/s of responsibility.<br>• Responsible for the system of effective internal controls across their area/s of responsibility.<br>• Report on risk management performance to the appropriate ELT. |
| The Chief Executive Officer (CEO) and Executive Leadership Team (ELT) | • Actively lead and promote a positive risk management culture across the organisation.<br>• Accountable for the implementation of risk management across the business areas under their control.<br>• Accountable for the system of effective internal controls across the business areas under their management.<br>• Resolve conflicting objectives that may arise from the risk management process.<br>• Identify and agree the key risks to the organisation achieving its objectives and set the performance measures for AT.<br>• Endorse the Risk Management Policy.<br>• Report on risk management performance to the Board of Directors. |

[3] Stakeholder, legal, or regulatory requirements can influence risk tolerance.

[4] This can be an individual or group that has an interest in any decision or activity of Auckland Transport.

| Role | Responsibility |
|---|---|
| The Board | The core role of the Board is to ensure that the organisation's objectives are achieved while meeting the appropriate expectations and interests of relevant stakeholders. Managing risk is an essential enabler for this role.<br>The role of the board is to:<br>• Set the organisation's risk appetite and its policy for managing risk; and<br>• Ensure their decisions take risk into account; and<br>• Foster a culture that is consistent with the organisation's appetite for risk; and<br>• Ensure the organisation has the structures and processes to support decision-making and manage risk; and<br>• Set an appropriate governance structure for risk and risk management, including, where appropriate, board and executive level committees and delegated authorities; and<br>• Require the executive to demonstrate that the framework for managing risk is effective and appropriate for the organisation; and<br>• Require the executive to provide information to allow the board to understand the risks that may have material impacts on the organisation's objectives, and the effectiveness of current controls. |
| The Finance & Assurance Committee (FAC) | • Review and endorse the Risk Management Policy for approval by the Board; and<br>• Review and endorse the risk appetite levels for approval by the Board; and<br>• Monitor the organisation's management of risks through review of regular risk reporting by management. |

# 6. Supporting Information

| | |
|---|---|
| **Legislative compliance** | This Policy supports Auckland Transport's compliance with all applicable legislation, the obligations to its shareholder and stakeholders and the obligations under the Treaty of Waitangi/Te Tiriti o Waitangi. |
| **Supporting documents** | • Organisational Risk Management Framework |
| **Related documents** | • AT Asset Management Policy<br>• AT Board Charter<br>• AT Business Plan 2023/2024<br>• AT Health, Safety and Wellbeing Policy<br>• Auckland Plan 2050<br>• Auckland Transport Statement of Intent<br>• CCO Governance Manual<br>• Finance & Assurance Committee Charter<br>• Information Security Policy |

| | |
|---|---|
| | • ISO 31000:2018 Risk Management - Guidelines<br>• AS/NZS ISO 31000:2009 Risk Management – Principles and guidelines<br>• ISO 73:2009 Risk Management Vocabulary<br>• SA HB 436.1:2020 Risk Management Guidelines - Companion to AS ISO 31000:2018 Part 1 Boards and Executives |

# 7. Non-Compliance

Risk management supports the compliance with multiple governance, legal, regulatory, government and shareholder requirements. Non-compliance perceived or otherwise, with those requirements can lead to increased scrutiny, investigations and reviews, penalties and in extreme circumstances prosecution and fines.

# 8. Approval & Review Details

**Policy Owner:** Head of Risk & Assurance

**Policy Contact:** Risk Services Manager

**Endorsed by:**

**Approved by:**

Chief Executive

Auckland Transport Board

**Effective date:** xx 2024

**Next review date:** xx 2027

AT reserves the right to review, amend or add to this policy at any time upon reasonable notice to employees and representatives.