NMIT RISK MANAGEMENT FRAMEWORK

MOKAMOKA WHAKAAETANGA | APPROVAL DETAILS

Section	Executive		
Approval Date	20.05.2026	**Sponsor**	Director Finance, Facilities and Risk
Next Review	01.01.2029	**Approved by**	Council

NGĀ WHAKATIKATIKA | AMENDMENT HISTORY

Version	Effective Date	Created/ Reviewed by	Reason for review / comment
1	01.01.2026	Transition Lead	New

This Framework gives effect to the NMIT Risk Management Policy and provides guidance for implementation of the NMIT Risk Management Policy through the procedures and requirements specified in this document.

All principles stated in the Policy apply to this Framework.

Tirohanga Whānui | Overview

The purpose of this Risk Management Framework is to outline how NMIT will implement the Risk Management Policy and manage risk at NMIT. This means outlining our commitment, responsibilities, processes and practices to support kaimahi to manage risk consistently and collectively as part of their day-to-day decision-making and business practices.

Mandate and Commitment

Risk management principle and objectives

The Risk Management Policy sets our risk management principles which highlight our commitment to managing risk. It also identifies our objectives in managing risk that aim to support NMIT achieve its purpose, goals and objectives.

Organisational risk appetite

Risk appetite is defined as the amount of risk that an organisation is willing to pursue or retain in order to achieve its organisational objectives. Our organisational risk appetite will be developed with the NMIT governing board and Senior Leadership Team and reviewed at least every three years.

Risk management governance structure

Our risk management governance structure provides oversight of the risks and risk management practice of NMIT. The structure includes:

- The NMIT governing board is ultimately accountable for the organisation's risk management. The Board provides independent oversight and direction to the Chief Executive and Senior Leadership Team on organisational performance including risk management.
- Other NMIT governing board sub-committees that have oversight and provide specialist advice and support on specific subject area risks and risk management activities.
- Academic Quality arrangements that oversee the quality of academic programmes.
- The NMIT Senior Leadership Team that manages the organisation's strategic, change and operational risks.

Change or transformation risks come into our risk management structure through risks arising from business led change nationally or escalated through operational risks from local change programmes and projects.

Roles and responsibilities for managing risk

Risk Management Team:

The NMIT risk team sits as a Support Services function. The function is led by the Director, Digital, Finance and Risk and provides tools, support, guidance and advice to:

- Develop and embed a consistent enterprise approach to risk management and build the risk management capability and culture of NMIT.
- Assist the Senior Leadership Team with their oversight of the enterprise risk profile, risk management practices and the overall effectiveness of the Risk Management Framework.

Specific risk management responsibilities at NMIT are outlined in detail in the risk management policy.

Ownership of Risks

Clear risk ownership is vital to making sure that the risks are being adequately managed. All staff are responsible for identifying; investigating; managing or escalating risks within their areas of responsibility.

The risk owner is accountable for ensuring the risk is managed appropriately. There may be multiple people who are required to collaborate with and support the risk owner in their risk management efforts.

Ngā Hātepe | Procedure

ENTERPRISE RISK MANAGEMENT LEVELS AND DOMAINS

This section outlines the key risk management levels and domains supporting the clarity and consistency of enterprise risk management across NMIT.

Risk levels

NMIT recognises three key levels of risk: Strategic, Change and Operational risk. These have distinct features, each described in the table below.

Risk Level	Description	Relates to plans / objectives
Strategic	• Risks that relate to the strategic objectives of NMIT. • Long-term in nature, of strategic importance and influential in achieving the strategic intent of NMIT. • Risks assessed in terms of consequence and likelihood often over several years. • The Board is accountable for these risks and to ensure they are managed.	• Strategic intentions • Organisation objectives
Operational	• Risks to the ability of NMIT to perform our day-to-day business activities and deliver on our business plans. • Risks assessed in terms of consequence and likelihood often within short time frames. • These risks are owned and managed within the applicable team with oversight, monitoring and reporting from the relevant individual senior leaders.	• Business plans and activities

Change	• Risks introduced as a result of the change activities of NMIT. • Risks to NMIT can be driven by internal or external change. • Risks assessed in terms of consequence and likelihood within the term of the project. • These risks are owned and managed by the applicable portfolio/ programme or project manager.	• Change (including project risks) • Organisation business plans and other additional activities

Risk domains

A domain is a broad category or functional area of risk that reflects a key aspect of an organization's operations, strategy, or environment. It represents a high-level grouping of related risks that typically align with how the organization is structured or how it delivers on its mission.

A sub-domain is a more specific area within a domain that identifies a distinct risk focus or process. Sub-domains allow for more granular classification, enabling detailed identification, assessment, and mitigation of risks within each domain.

The following table defines the domains, and associated sub-domains, within the NMIT risk management framework.

Domain	Sub-domain
Strategic	• Policy and Regulatory Alignment • Strategic Planning and Execution • Reputation and Brand Management • Governance and Leadership Stability • Stakeholder and Community Expectations • Mergers, Acquisitions, and Partnerships
Academic and Educational Delivery	• Curriculum Relevance and Quality • Industry Engagement and Employer Needs Alignment • Qualification Accreditation and Compliance • Teaching Quality and Staff Capability • Work-Based Learning / Apprenticeships Oversight • Assessment Integrity and Moderation • Student Progression and Achievement
Regulatory, Legal and Compliance	• Tertiary Education Quality Standards • Data Protection and Privacy Laws • Health and Safety Legislation • Financial Reporting and Audit Compliance • Immigration and Visa Regulations (for international students) • Contractual Obligations and Third-Party Agreements • Intellectual Property Management • Litigation and Disputes • Employment Law Compliance • Insurance Coverage and Claims Management
Financial and Funding	• Government Funding Models and Changes • Enrolment Revenue Volatility (domestic and international) • Cost Management and Budgetary Control • Fraud and Financial Mismanagement • Cash Flow and Liquidity • Capital Projects and Asset Investment Risk

Operational	• Facilities and Asset Management (Hard and Soft FM) • Timetabling and Course Delivery Logistics • Contract and Vendor Management • Student Records and Enrolment Systems • Administrative Efficiency and Process Reliability • Transport, Catering, and Accommodation Services
People, Culture, Health and Safety	• Staff Recruitment and Retention • Workforce Planning and Capability • Industrial Relations / Union Issues • Staff Health, Safety, and Wellbeing • Leadership Succession and Development • Culture and Ethical Conduct
Student Experience and Support	• Student Mental Health and Counselling Services • Bullying, Harassment, and Misconduct • Equity, Inclusion, and Accessibility • Academic and Pastoral Support Services • Accommodation and Welfare Oversight • Student Engagement and Feedback
Digital and Technology	• Cybersecurity and Data Breaches • System Resilience and Downtime • Learning Management Systems (LMS) Reliability • Digital Literacy and Access Equity • AI and Emerging Technology Governance • Business Continuity and Disaster Recovery
Environmental and Sustainability	• Sustainable Facilities and Carbon Emissions • Climate Change Adaptation and Preparedness • Energy and Waste Management • Compliance with Environmental Regulations • Sustainable Procurement Practices
External and Environmental	• Political and Economic Instability • Natural Disasters and Severe Weather • Epidemics and Pandemics (e.g., COVID-19) • Demographic Changes and Market Shifts • Technological Disruption in Education

RISK MANAGEMENT PROCESS

This section outlines at a high level the risk management process we use and is based on the international risk standard AS/NZ ISO 31000: 2018. The risk management process involves a sequence of coordinated steps and activities that support the effective management of risk. The key features of the risk management process are outlined below:

Risk context

Establishing the context helps us understand the wider picture of the risks and opportunities we need to manage. This includes understanding the internal and external operating environment and establishing relevant objectives based on our strategy to determine the scope of the risk assessment.

Risk assessment - Identifying risks

Risk management requires the proactive identification of risks and opportunities. This can be done a number of ways, including as part of our business-as-usual processes or through a dedicated risk identification exercise (which could be a meeting or workshop for example) or a focused examination of risks in a particular area of work. Once identified, in order to manage a risk effectively it is important we describe it a clear and unambiguous way.

Risk assessment - Analysing and rating risks

Risk management also includes analysis of any information that will help us understand how significant our risks are. This requires an understanding of existing controls and how effective they are. Controls are anything in place which helps modify or manage risk in some way. They include existing or current policies, procedures, practices or other actions.

Controls are designed to reduce the likelihood of an event or situation occurring and limit the impact of a risk occurring. There are generally three types of controls:

- Preventative - These controls attempt to defer or prevent undesirable events from occurring.
- Detective - These controls attempt to detect errors or irregularities which have already occurred.
- Corrective - These controls are put in place to limit the impact of the risk event. They reduce the impact once the risk event has already happened.

The level of analysis is based on the assessment and rating of the impact and likelihood of a risk occurring. Rating risks based on our analysis is supported by our Risk Rating Matrix (see next section), and Risk Register Template. The Matrix consists of an impact matrix and likelihood scale. The combination of impact and likelihood supports an overall risk rating range from 'Low' to 'Extreme' as set out in the matrix.

We use the matrix to assess our inherent (uncontrolled), residual (level of risk exposure with existing controls considered) and tolerable (target) risk exposure:

- The inherent (uncontrolled) risk rating assessment measures the consequence/impact and likelihood the risk would be if there were no controls in place or we were not actively managing the risk.
- The residual (current) risk rating assessment looks at the perceived or measured risk with existing controls and the application of action plans/initiatives currently in place to mitigate the risk.
- The tolerable (target) risk rating is the level that is the desired target level within the NMIT risk tolerance and risk appetite and takes account of additional controls, plans, or initiatives that would be required to achieve the targeted level.

Risk assessment - Evaluating risks

Risk evaluation assesses the information generated from risk identification and risk analysis against our current level of appetite or tolerance to determine if the risk is acceptable. This helps us decide whether to do something about the risk or not, and to prioritise which risks to do something about first. It should also take into account costs and benefits of any proposed actions, and the wider context, including legal, regulatory and other obligations.

Assessment of effectiveness of controls and mitigations

The following assessment criteria should be used to assess the overall effectiveness of the controls in place that are mitigating the risk.

(Note that the controls identified may not always exert the intended or assumed modifying effect, or may not yet be at a point where they are fully operational or effective.)

Rating	Level of protection/mitigation
Effective	• **Optimal levels of controls are in operation at all times.** • **Control practices are embedded in business processes.**
Partially Effective	• **Sufficient controls are in place for day-to-day operations but control practices are not fully embedded in business-as-usual processes yet.**
Non-effective	• **Insufficient Controls are in operation (i.e. yet to be implemented, not implemented effectively and/or additional Controls are needed).** • **Control breaches are common. No identified or planned Controls.**

Risk treatment

Risk treatment is the process of selecting and implementing the appropriate response to address the assessed risk. It involves an escalation process to determine who is best placed to make the risk treatment decision and the consideration of the most appropriate treatment options.

Risk escalation

Risk escalation applies the 'one up' principle where staff are expected to raise risks with their direct line-manager in the first instance. The extent that risks are accepted, managed or escalated is based on the residual (current) risk rating. The table below provides an overall guide that should be read in conjunction with the Risk Rating Matrix.

Risk Rating	Response	Description
Extreme	Treat and prioritise	• Council level oversight required. • Can be managed at senior leadership level with Council reporting required • Regular monitoring and review at least monthly required to ensure risks are unchanged and mitigations are effective. • Risk treatment is prioritised and required to reduce severity. • Relevant stakeholders are informed and where relevant engaged. • Resources to treat risks are prioritised.
High	Treat and focus	• Senior Leadership oversight required. • Can be managed at third tier management levels with Senior Leadership reporting required. • Regular monitoring and review at least quarterly required to sure risks are understood and mitigations are effective • Risk treatment may be required to reduce severity. • Relevant stakeholders are informed and where relevant engaged. • Resources to treat risks are expected to be sourced from within the Directorate or business area.
Medium	Treat and monitor	• Managed at third/fourth tier management level. • Regular monitoring and review at least six-monthly to ensure risks are understood and mitigations are in place.

		• Any resources to treat risks are expected to be sourced from within the business area where the risk was identified.
Low	Accept but watch	• Managed at district/local/line management level. • No further action required to manage these risks. • Regular monitoring and review at least annually or after change/event. • Any resources to treat risks are expected to be sourced from within the business area where the (risk(s) or incident(s) occurred.

Risk treatment response

Once determined or escalated to the appropriate risk owner, management response options need to be considered. Each option has associated implications and actions for the risk owner, and these are described in the table below.

Response	What it means
Accept	As the owner of the risk you are comfortable with the current level of risk and the controls in place, this may include proactively taking a defined level of risk in order to achieve a targeted opportunity. You decide (after careful consideration of advice, to accept the risk and commit to reviewing your decision at a frequency commensurate with the level of risk (see risk escalation table for guidance) .
Treat/reduce	As the owner of the risk, further actions should be taken to manage its impact and/or likelihood. You have considered the financial and non-financial cost and benefits of planned actions and decided to treat your risk. Additional actions and controls should be recorded in a Risk Register.
Transfer/share	As the owner of the risk, the risk should be moved to another party to manage. You have considered the financial and non-financial costs and benefits of transferring verses retaining the risk especially as this may introduce dependence risks or impact others. You decide to transfer the risk and commit to reviewing your decision at a frequency commensurate with the level of risk (see risk escalation table for guidance).
Avoid/eliminate	As the owner of the risk, the risk to business delivery is too great. You decide to avoid starting the activity or stop the activity.

Recording and reporting

Risks and risk conversations should be documented and recorded in the Risk Register. Managers/Leaders own and are responsible for ensuring regular risk conversations take place with their teams, that they are appropriately recorded and that their risks are reviewed and updated on a regular basis.

The NMIT Council and Senior Leadership Team will be provided quarterly risk reporting that informs them about the organisation's key strategic risks and any key 'Extreme' escalated change, enterprise and operational level risks, how they are being managed and how the Risk Management Framework is being applied.

Monitoring and reviewing

Management monitoring and review should occur throughout the risk management process, with a frequency that reflects the level of risk, as described in the 'risk escalation table' detailed above. This can occur in a range of ways including routine management or governance monitoring activities or specific assurance, audit or review activities to monitor and test controls to ensure they remain appropriate and work as they were intended. These monitoring and review activities will support accountability, ownership and stakeholder confidence that we are identifying and managing our risks effectively.

Communication and consultation

Communication and consultation should also occur throughout the risk management process. While the focus, scope and frequency of communication and consultation will vary according to the nature and rating of the risks, having an open engaging approach will take advantage of different knowledge, skills, and experiences. It will also ensure the interests and views of stakeholders are understood and considered.

RISK RATING MATRIX

The following risk assessment criteria will be used for risk analysis at NMIT. Risk analysis involves consideration of the sources of risk, the controls in place (and their actual effect), the consequences and the likelihood of those consequences being realised.

		Consequence				
Likelihood	**Description**	**Minimal**	**Minor**	**Moderate**	**Major**	**Severe**
Almost Certain	This event is expected to occur imminently (>95% chance of occurring)	Medium 5	High 10	High 15	Extreme 20	Extreme 25
Likely	Has occurred several times and is likely to occur again in near future (51-95% chance of occurring)	Medium 4	Medium 8	High 12	High 16	Extreme 20
Possible	There is evidence of this event occurring before (21-50% chance of occurring)	Medium 3	Medium 6	Medium 9	High 12	High 15
Unlikely	Events of this type could occur but may have no occurred before (5-20% chance of occurring)	Low 2	Medium 4	Medium 6	High 8	High 10
Rare	Events like this have not occurred and are not expected to occur (<5% chance of occurring)	Low 1	Low 2	Medium 3	Medium 4	High 5

Guidance on how we respond consistently to our rated risks is outlined in the Risk Escalation table on pp6-7 of this Framework. The following table and the table in the following section (Risk Consequence Assessment) provide further guidance in assessing likelihood and consequence by risk level and domain.

Our **Risk Rating Likelihood Scale** should be used to assess Strategic, Operational and Change Risks as outlined in the table below:

Likelihood	Risk Level		
	Strategic Risk	**Operational Risk**	**Change Risk**
Almost Certain	Strategic risk timeframes are often but not always longer reflecting their future delivery. **Often expected to be encountered some years in the future 2 – 5+ years**	Operational risk timeframes are often relatively short, reflecting their activity-based exposure. **Often expected between 1 – 2 years**	Change risk timeframes are dependent upon the length of the programme or project. **Within the change programme / project timeframe**
Likely			
Possible			
Unlikely			
Rare			

Risk Consequence Assessment

When determining consequence level, to safeguard from the unnecessary application of treatments and costs, the consequence rating applied should be the **most plausible**, not the most extreme, worst-case scenario.

The Risk Consequence Assessment table sets out the consequence assessment criteria for NMIT risk.

CONTINUOUS IMPROVEMENT

This section highlights how NMIT will monitor, review and continually improve our approach to risk management.

Measuring success

Given the organisational maturity of NMIT, the early focus of the Risk Management Team will be to implement and embed this Framework across the organisation. Once NMIT has moved beyond this early-stage maturity, the effectiveness of this Framework and our Risk Management Policy will be measured by considering the following:

- Individual Business area risk registers have been documented and updated at least on a quarterly basis.
- Evidence of whether risk management actions or initiatives for extreme rated risks are successful in reducing or managing risk levels (through ensuring regular review of plans and initiatives).
- Evidence that risk associated with opportunities are accepted and managed.
- Emerging risks are identified.
- Effectiveness of this Framework, including but not limited to risk awareness, compliance with obligations, business continuity preparedness, insurance cover and evidence of continuous improvement annually.

Independent Review and Assurance

A range of internal and external sources of independent reviews and assurance may be commissioned from a range of functions across NMIT. These can include reviews of key functional controls, processes and procedures, like the annual financial audit for example. This work will help inform the ongoing maturing and improvement of our approach to risk management.

Formal Review

This Framework will be formally reviewed on a three-yearly cycle to ensure it remains relevant and incorporates what we learn about our risk management practice. However, as our governance and organisational structure and business processes mature alongside the finalising the organisational risk appetite, this Framework will need to reflect these developments to ensure it remains up to date. As a result, we expect an update of this Framework will be needed within the next 12-18 months.

RISK MANAGEMENT DEFINITIONS

The following key definitions have been adapted from international standards ISO 31000: 2018 and COSO 2017. Further risk management terms and definitions are outlined in the Risk Management Policy.

Term	Definition
Cause	Existing or possible reasons that a risk exists and/or could occur.
Consequence / impact	Potential outcome or result associated with a risk event if or when it occurs or does not occur. Outcome of an event affecting objectives.
Emerging risk	These risks could potentially be significant but may not be fully understood, they are difficult to quantify and may have a high loss potential.
Inherent risk	Level of risk based on the likelihood of it occurring and the potential impact of the identified consequences if it were to occur with no controls in place.
Issue / incident	Issues/incidents are essentially risks that have eventuated. Issues/ incidents provide valuable insight, in which it allows us to learn from our experiences. These insights can assist you in your identification, analysis and evaluation of risks.
Likelihood	The chance of a risk event or condition occurring.
Objective	A future state that an individual or team's efforts or actions are intended to attain or accomplish; a goal, aim, target, outcome or output.
Risk	The effect of uncertainty (positive and/or negative) on objectives. Note that this means that the event has **not** occurred but has the potential to occur – an event that has occurred is defined as an issue/incident.
Residual (current) risk	Level of risk based on the likelihood of it occurring and the potential impact of the identified consequences if it were to occur with current controls in place.
Risk appetite	The amount of risk that an organisation is willing to pursue or retain in order to achieve its organisational objectives.
Risk control	Any action that maintains and/or modifies a risk.
Risk culture	Our attitude, actions and behaviour that determine the way we identify, understand, discuss and act in relation to risk.
Risk management	Co-ordinated activities (including culture, processes structures and information) to direct and control an organisation with regard to risk.
Risk maturity	Expresses how well developed the organisation's capability and culture are in relation to managing risk.
Risk rating matrix	The risk rating matrix is a risk management tool used to assist in the analysis and evaluation of risks based on their likelihood and consequences.

Risk owner	Position or entity with accountability and authority to manage a risk.
Risk rating	The overall rating obtained where impact and likelihood intersect on the risk matrix.
Risk response	The decision on how to respond to the risk in its current state.
Risk tolerance	The amount of deviation from an organisation's risk appetite that will be endured.
Tolerable (target) risk	Level of accepted risk based on the likelihood of it occurring and the potential impact of the identified consequences if it were to occur with appropriate controls in place.
Treatment plan (action plan) / initiative	A treatment plan (action plan)/initiative is further action that you plan on taking in order to prevent, reduce, manage or modify your risk to an acceptable level – this could be one action plan or multiple plans. Treatment plans (action plans)/initiatives are different to controls – whereas controls are the things you currently do; treatment (action plans) plans refer to the thing you plan to do.

Risk Consequence Assessment

This consequence assessment scale is used to evaluate the most plausible impact should a risk event occur, taking into account the current operating environment and existing controls. The assessment should not reflect the most extreme or worst-case scenario, but rather a credible and realistic outcome if the risk materialises.

When determining consequence, risk owners should:

- Select the primary risk domain most closely aligned to the nature of the risk.
- Consider impacts on learners (ākonga), staff (kaimahi), operations, compliance, finances, reputation, and sustainability as relevant.
- Choose the consequence level that best represents the likely scale, duration, and severity of impact.
- Where impacts span multiple domains, record secondary impacts in the risk narrative or notes.

RISK DOMAIN	MINIMAL	MINOR	MODERATE	MAJOR	SEVERE
STRATEGIC	Negligible impact on strategic objectives or stakeholder confidence.	Short-term or localised impact on non-critical initiatives; easily recoverable.	Material delay or underperformance against strategic objectives; some loss of confidence.	Significant failure to deliver strategic priorities; sustained reputational impact.	Strategic viability threatened; widespread loss of confidence requiring major intervention.
ACADEMIC AND EDUCATIONAL DELIVERY	No material impact on teaching quality or learner outcomes.	Localised delivery or assessment issues with minimal learner impact.	Repeated issues affecting learner progression, completion, or employer confidence.	Major quality or integrity failure placing programmes or accreditation at risk.	Systemic academic failure resulting in loss or suspension of approvals.
REGULATORY, LEGAL AND COMPLIANCE	Minor non-compliance with negligible consequence.	Low-level breach resolved without penalty.	Material breach requiring formal notification or investigation.	Major breach with significant penalties or litigation exposure.	Serious systemic breach threatening licence, funding, or ability to operate.
FINANCIAL AND FUNDING	No material financial impact.	Minor variance managed within existing budgets.	Material variance requiring budget reprioritisation.	Significant impact requiring cancellation or deferral of programmes.	Financial sustainability threatened; extraordinary intervention required.
OPERATIONAL	No disruption to normal operations	Short-term or localised disruption.	Disruption affecting multiple processes requiring workarounds	Significant disruption across sites or services.	Severe operational failure preventing delivery of core services.

RISK DOMAIN	MINIMAL	MINOR	MODERATE	MAJOR	SEVERE
PEOPLE, CULTURE, HEALTH AND SAFETY	No injury or material wellbeing impact.	Minor injury or short-term wellbeing impact.	Injury or wellbeing issue requiring medical treatment.	Serious injury, psychosocial harm, or major cultural failure.	Fatality or systemic wellbeing failure threatening continuity.
STUDENT EXPERIENCE AND SUPPORT	No material impact on student wellbeing or support.	Localised support disruption; minor complaints.	Noticeable decline in experience affecting engagement or retention.	Significant welfare incident or systemic support failure.	Critical incident causing severe harm and loss of trust.
DIGITAL AND TECHNOLOGY	Isolated technology issue with no service impact.	Short-term system disruption with limited impact.	System outage affecting multiple users or services.	Major system failure or security breach.	Sustained loss of critical systems or data.
ENVIROMENTAL AND SUSTAINABILITY	No measurable environmental impact.	Minor, contained environmental incident.	Incident requiring remediation or reporting.	Significant environmental harm requiring regulator engagement.	Major environmental damage with long-term impact.
EXTERNAL AND ENVIRONMENTAL	Negligible impact from external events.	Short-term external disruption.	External shock causing measurable impact.	Major external event significantly affecting delivery.	Prolonged external crisis threatening organisational viability.

RISK TOLERANCE AND ACCEPTABILITY

This matrix is used to determine risk rating by combining the consequence and likelihood levels. The assessment is used to determine the severity of the risk and identify those which are unacceptable to the organisation and require management attention and further treatment. It also forms the basis of ongoing monitoring.

	CONSEQUENCE				
LIKELIHOOD	Insignificant	Minor	Moderate	Major	Extreme
Almost Certain	Medium	Medium	High	Very High	Very High
Likely	Low	Medium	High	High	Very High
Possible	Low	Medium	Medium	High	High
Unlikely	Very Low	Low	Medium	Medium	High
Rare	Very Low	Very Low	Low	Low	Medium

Ngā Haepapa | Responsibilities

Roles and responsibilities are detailed in the NMIT Risk Management Policy.

Ngā Hononga ki Tuhinga kē | Links to other documents

NGĀ KAUPAPA-HERE E HANGAI ANA | RELATED POLICIES

NMIT Risk Management Policy