GOVERNANCE POLICY

Risk Management Policy

Policy:	**Risk Management Policy**
Version:	**1.3**
Date in force:	**February 2024**
Planned Review:	**February 2026**

Purpose

This policy aims to provide a risk management framework that ensures all significant risks associated with InternetNZ strategic objectives are effectively identified, assessed, and managed.

The framework enables us to help identify our key risks, i.e., those that, if realised, would result in one or more of the following:

- Impact the InternetNZ ability to maintain the security, stability, and resilience of the .nz domain name space.
- Impact the realisation of InternetNZ strategy.
- Significantly challenge the trust and confidence stakeholders place in InternetNZ.

Scope and Context

This policy applies to all InternetNZ employees, contractors and governors and encompasses internal operations and externally contracted functions.

'Risk', within this policy, is defined as any adverse condition or event that could negatively impact the success of our services or activities. This includes, but is not limited to:

- Continuity planning - where risks primarily concern the availability of critical business functions and services.
- Security - where risks pertain to the safety and integrity of the InternetNZ information and physical assets.
- Health and Safety - where risks include workplace accidents, non-compliance with safety regulations, and potential employee health hazards.

To facilitate the application of this policy across different levels of risk in the organisation, we have established three roles for risk governance. In the context of key InternetNZ risks, these roles are documented in Appendix 3:

- **Risk Leadership Team**: Leaders directing risk management strategy and priorities, integrating risk management into organisational processes.
- **Risk Governance Committee**: This group oversees risk management activities, ensures compliance, and reviews risk mitigation efforts.
- **Risk Oversight Board**: The top-level body responsible for overarching risk oversight, aligning risk management with organisational goals and providing strategic guidance.

Recognising that risk is an inherent aspect of our activities, this policy aims not to eliminate risks but to effectively identify, assess, and manage them. The approach focuses on risks that impact our strategic objectives, offering a framework to enable the organisation to capitalise on opportunities while minimising threats.

Key Objectives

InternetNZ Group's risk management objectives are to:

- Develop a "risk aware" culture that encourages personnel to identify risks and opportunities in a planned and coordinated manner and to respond to them with cost-effective actions;
- Ensure continuity for critical operations by anticipating and managing risks that could cause major disruptions.
- Assure stakeholders that an effective risk management programme is in place.

Framework for Managing Risk

The Risk Management Framework comprises of four key components:

Risk Identification

The identification stage helps the organisation identify current and emerging risks and where they sit within the risk matrix through:

- Discovery of potential risks:
    - Surveillance of the operational and external environment.
    - Gathering insights from stakeholders.
    - Analysing data and trends to anticipate future risks.
    - Conducting focused sessions to identify and evaluate risks.
    - Reviewing industry reports, conferences and best practices to understand risks similar organisations face locally and globally.
- Running an initial triage of the risk to:
    - Assess initial likelihood and severity.

    - Assess the need for an out-of-cycle review.
- Capturing these in the risk register for further analysis.

While the Risk Leadership Team is primarily responsible for risk identification, we expect everyone across the InternetNZ to raise actual or potential risks they identify for consideration.

Risk Assessment and Analysis

Following identification, the risk assessment stage focuses on a more detailed evaluation of each risk in the risk register, including:

- Clear articulation, ensuring the information is understandable and valuable for relevant stakeholders.
- Streamlining and distinguishing risks by ensuring each risk is sufficiently distinct while avoiding overly broad risks that hinder effective assessment and mitigation.
- Categorisation of risks based on likelihood and severity, ensuring alignment with our established criteria detailed in Appendices 1 and 2, wherever feasible. This approach:
    - Enables consistent assessment
    - Helps identify risk mitigation strategies proportionate to these risks' potential impact and probability.
    - Supports comparative analysis.

Effective assessment and analysis should enable risk to serve as a strategic management tool, supporting:

    - The Risk Governance Committee and Risk Oversight Board in establishing risk appetite, risk likelihood, and tolerance criteria.
    - InternetNZ in achieving strategic objectives and maintaining critical infrastructure rather than acting as an exercise in compliance.

The Risk Leadership Team is responsible for a consistent risk assessment and analysis approach, sourcing expertise across the organisation to provide necessary context.

Risk Controls and Response

The risk control and response stage manages controls and responses for identified risks through:

- Development of controls/mitigations for each identified risk, tailored to likelihood and impact.
- Assessment of control implementation status and effectiveness, ensuring this is captured alongside each control.
- Strategic allocation of resources to address high-priority risks.
- Continuous monitoring and adjustment of mitigation strategies to ensure ongoing effectiveness and relevance.

The Risk Leadership Team is responsible for ensuring the availability of necessary information to facilitate effective controls and mitigations and for strategically allocating resources to operationally manage these risks.

Reporting and Review

The reporting and Review stage establishes a process for reporting risk management activities and facilitating periodic reviews:

- InternetNZ staff will provide the Risk Governance Committee and Risk Oversight Board access to the Risk Register's high-level reporting interface and supply snapshots at specific points in time for documentation purposes.
- InternetNZ staff will schedule routine reviews with the Risk Governance Committee or Risk Oversight Board to assess the effectiveness of the risk management approach and risk register.
- InternetNZ staff will identify any critical information that requires the attention of the Risk Governance Committee or the Risk Oversight Board following the risk assessment. This information is likely to include:
    - Identification of new risks and mitigation of prior risks reported.
    - Risks that have changed, for example, increased from moderate to extreme.
    - Identification of key groups of risks and the broad controls in place for these.
- The Risk Leadership Team and Risk Governance Committee are jointly responsible for bringing specific areas of concern to the attention of the Risk Oversight Board.

Review of Policy

The Council will review this policy every two years per the protocol for reviewing all policies.

Appendix 1 - InternetNZ Likelihood Criteria

Category	Rare	Unlikely	Possible	Likely	Almost Certain
Definition	The consequence would occur only in exceptional circumstances, eg less than 1% chance of occurring in the next 24 months.	The consequence is unlikely to occur in most circumstances, eg 1% - 30% chance of occurring in the next 24 months.	The consequence could conceivably occur in some circumstances, eg 30% - 60% chance of occurring in the next 24 months.	The consequence has a reasonably high chance of occurring in many circumstances, eg 60% - 80% chance of occurring in the next 24 months.	The consequence is expected to occur in most circumstances, eg 80% + chance of occurring in the next 24 months.

Appendix 2 - InternetNZ Risk Tolerance Criteria

Category	Insignificant	Minor	Moderate	Major	Extreme
Strategic	• Minor complaints about INZ's or DNC's capability, service delivery or infrastructure	• An aspect of INZ's or DNC's capability, service delivery or infrastructure is deemed unsuitable • Minor impact on growth of new .nz registrations	• A noticeable aspect of capability, service delivery or infrastructure are deemed unsuitable • Multiple years of declining .nz domains (<10%)	• Multiple years of declining .nz domains (10–20%) • Failure to deliver strategic objectives and key operational objectives • Failure to maintain the security, stability and resilience of .nz	• InternetNZ deemed unsuitable to manage the domain name registry • Multiple years of declining .nz domains (>20%)
Service	• Short unplanned outage of registry up 4 hours • Minor localised environmental event resulting in lack of access to files and facilities for less than one day	• Unplanned registry outage between 4 to 12 hours • Temporary loss of access to office premises and facilities for up to two days. • Temporary loss of one registry site for up to 2 days	• Unplanned outage to registry between 12 to 24 hours • Disruptions to .nz domain resolution for less than one day • Loss of access to office premises and facilities for up to 1 week.	• Unplanned registry outage between 1 day and 1 week • Disruptions to .nz domain resolution for 1–2 days • Data integrity problems affecting DNS and/or registry	• Registry unavailable for an extended period with no ability to restart as part of BCP • Total loss of .nz domain name resolution

Category	Insignificant	Minor	Moderate	Major	Extreme
Financial	• Less than $250,000 financial impact on performance of the organisation within one year.	• Between $250,000 to $500,000 financial impact on performance of the organisation within one year.	• Between $500,000 and $1,000,000 financial impact on performance of the organisation within one year.	• Between $1,000,000 to $2,000,000 financial impact on performance of the organisation within one year.	• Greater than $2,000,000 financial impact on performance of the organisation within one year.
External and Reputation	• Minor disagreements with stakeholders	• Relationship issues with key stakeholders cause delays to major decisions • Relationship issues with suppliers cause delays to major decisions or disruption to service • One-off negative media coverage	• Ongoing relationship issues that impact on achievement of objectives • Ongoing relationship issues with suppliers that impact on achievement of objectives • Significant one-off event or series of events resulting in sustained negative media coverage and perception	• Relentless/sustained reputation issue • Severe breakdown of relationships with suppliers resulting in changes in appointments • A one-off event or series of events that result in loss of confidence from one or more key stakeholders • A single key person being publicly replaced	• Public severance of relationships with suppliers • A number of key personnel (Council, Management or Representatives) replaced • Loss of government support possibly leading to withdrawal of mandate to operate .nz

Category	Insignificant	Minor	Moderate	Major	Extreme
Legal	• Isolated contractual disagreements with suppliers	• Significant contractual disagreement with suppliers	• Warrant to examine and/or copy records issued • Unexpected audit by a government department. • Litigation with one registrar	• Litigation with key suppliers • Injunction or legal action impedes ability to function normally • Key equipment and/or files are removed by court order	• Litigation with the government • Injunction freezes assets or operations
People	• Workplace incident with no injuries and no loss of work hours • Minor stress issues or dissatisfaction	• Workplace incident requiring First Aid or medical treatment and loss of work hours • Significant stress issues experienced by one staff member	• Prolonged loss of work hours • Significant injury • Significant stress issues affecting two or more staff members impacting ability to function	• One staff member lost without notice • Several staff lost with notice • Significant stress issues affecting two or more teams impacting ability to function • Office facilities shut down	• Workplace incident with life threatening injuries or loss of life • Majority of staff lost with/without notice • Significant stress issues affecting organisation impacting ability to function

Appendix 3 - InternetNZ Risk Governance Structures

Role	InternetNZ	DNCL
Risk Leadership Team	Te Kāhui Tumu (TKT)	
Risk Governance Committee	Audit and Risk Committee	DNCL Board
Risk Oversight Board	InternetNZ Council	