GOVERNANCE POLICY

Risk Management Policy

POLICY:	Risk Management Policy
VERSION:	1.1
DATE IN FORCE:	May 2020
PLANNED REVIEW:	May 2022

Purpose

The purpose of this policy is to provide a risk management framework that ensures all significant risks associated with InternetNZ Group's strategic objectives are effectively identified, assessed and managed.

The framework will identify what are our true key risks, i.e. those that if realised would:

- Impact the realisation of InternetNZ's strategy; and/or
- Significantly challenge the trust and confidence stakeholders place in InternetNZ.

Scope and Context

This policy applies to all management, staff, and others employed by InternetNZ Group from time to time. It covers functions performed internally as well as those operated by external organisations under contract to InternetNZ Group.

Risk is inherent in all aspects of the InternetNZ Groups activities and whilst many of these risks cannot be eliminated, they can, however, be identified, quantified and controlled.

Risks that impact on the strategic objectives of the InternetNZ Group can offer both opportunity and threat. This policy is designed to provide the InternetNZ Group personnel with a framework in order to minimise threats.

Key Objectives

InternetNZ'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;
- Provide assurance to the shareholder and stakeholders that an effective risk management programme is in place.

Framework for Managing Risk

The Risk Management Framework comprises of four key components:

Risk Assessment

Risk assessment is designed to:

- Enable identification of the existence of the risk, where this risk sits within (or outside) the risk radar (as depicted in Appendix 1).

- Provide sufficient detail to explain and communicate the nature of the risk;
- Ensure risk information is relevant and meaningful to those who will read it; and
- Act as a management tool to enable
    - The Audit and Risk Committee and Council to define Risk Appetite and Risk tolerance for the organisation.
    - InternetNZ to achieve strategic objectives, rather than as an exercise in compliance.

Risk Tolerance

A formal risk tolerance is established to set agreed criteria for assessing risks and the level of risk that can be tolerated to achieve the organisation's strategic objectives.

As depicted in Appendix 1, the risk tolerance is expressed in terms of three risk rating zones:

- INZ Colour Light Grey (Minor/insignificant risks) – Risks within these zones are automatically tolerated.
- INZ Colour Dark Grey (Moderate risks) – Some Moderate risks may be tolerated, where additional treatment is not cost justified, in return for specified benefits.
- INZ Colour Black (Extreme/major risks) – Generally these risks are not tolerated and an immediate mitigation is required.

Risk Definitions

For the purpose of this policy, a risk is a condition or action that may affect the outcome of a planned activity. For continuity planning, the affected activities are the critical business functions and services; for security, the affected entities are InternetNZ Group's information and physical assets.

Risk definitions, in terms of consequence are required to ensure that risks can be consistently assessed and risk mitigation appropriate to the risk consequence can be identified.

The risk definitions will then be used in order to rate their consequence and to compare different risks with different impacts.

Reporting and review

Management will provide a quarterly report to the Audit and Risk Committee for residual Extreme/Major and Moderate Level risks that includes:

- Risk Radar
- Risk Register

Management will specifically note any key information that requires the attention of the Audit and Risk Committee, following the risk assessment. This is likely to include:

- Identification of new risks and mitigation of prior risks reported;
- Risks that have changed (i.e. increased/decreased from moderate to extreme, minor/insignificant to moderate, etc.); and
- Identification of key groups of risks and the broad controls in place for these.

Review of Policy

The Council will review this policy every two years in accordance with the Council's protocol for the review of all policies.

NOTE FOR COUNCIL MAY 2020 - not included in published Policy

Risk Process

A separate Risk Process that sets out how this policy is implemented is under development in conjunction with the Audit & Risk Committee. We expect it to be complete in the middle of 2020.

Appendix 1

internetnz

Risk radar