

Policy Template

SAMPLE POLICY

# Risk Management Policy

<Month Year>

# Contents

- 1. Purpose ..... 3
- 2. Scope ..... 3
- 3. Risk Governance ..... 3
- 4. Risk Management Process ..... 3
- 5. Integration with other systems and processes ..... 4
- 6. Risk Categories ..... 4
- 7. Risk Register ..... 4
- 8. Risk Reporting ..... 4
- 9. Risk Management Performance ..... 5
- 10. Risk Appetite ..... 5
- 11. Interagency and State Significant Risks ..... 5
- 12. Review and approval ..... 5
- 13. References and related documents ..... 6

<b>Date of issue/update</b>	Created: <dd month year > Last reviewed and/or updated: <dd month year >	Version	<1,2 etc>
<b>Policy owner</b>	Example: Human Resources Manager		
<b>Approved by</b>	<Executive GM, insert division> or <Committee>	<dd month year >	
<b>Audit &amp; Risk Committee sign off needed?</b>	Yes            or            No	<dd month year >	

# 1. Purpose

Outline the purpose of the risk management policy.

**Example:**

The purpose of the risk management policy is to provide guidance regarding the management of risk to support the achievement of corporate objectives, protect staff and business assets and ensure financial sustainability.

# 2. Scope

Specify who this policy applies to.

**Example:**

This policy applies to all [organisation name] activities. It forms part of [organisation name] governance framework and is applies to all employees, contractors and volunteers.

# 3. Risk Governance

Provide an overview of the risk governance structure of the organisation. Indicate who is involved in risk management and what their responsibilities are.

**Example:** See below

<b>Board</b>	Provides policy, oversight and review of risk management
<b>Audit and Risk Committee</b>	Oversees regular review of risk management activities
<b>Chief Executive Officer</b>	Drives culture of risk management and signs off on annual risk attestation
<b>Risk Manager</b>	Continuously improving risk management policy, strategy and supporting framework
<b>Managers</b>	Ensure staff in their business units comply with the risk management policy and foster a culture where risks can be identified and escalated
<b>Staff and Contractors</b>	Comply with risk management policies and procedures

# 4. Risk Management Process

Outline the steps involved in the risk management process. Make reference to the risk management procedure for practical guidance on the process.

**Example:**

When undertaking a risk management process the following steps must be taken: establish the context, identify the risk, analyse the risk, evaluate the risk, treat the risk and monitor and review the risk. Refer to the risk management procedure for details on how to perform each step in the process.

## 5. Integration with other systems and processes

Describe how risk management is integrated and embedded into organisational processes.

**Example:**

Risk management is factored into business planning, performance management, audit and assurance, business continuity management and project management.

## 6. Risk Categories

Specify risk categories to be included in the risk register and in risk reporting.

**Example:**

Risk categories may include strategic, financial, environmental, safety, people and reputation.

## 7. Risk Register

Specify the purpose of the risk register. Include details on the types of risks to be included on the risk register (e.g. operational or strategic), the criterion for adding and removing risks from the register, who will review the risk register and how often it will be reviewed.

## 8. Risk Reporting

Outline the risk reporting requirements. The purpose of risk reporting is to create awareness of key risks, improve accountability for the management of risk and the timely completion of risk treatment plans. Details as to who prepares reports, who reviews reports and how often reports are reviewed should be included.

**Example:**

The strategic risk register is prepared by the Chief Risk Officer and reviewed by the Audit Committee on a quarterly basis.

## 9. Risk Management Performance

Outline how the performance of risk management will be measured. Measuring performance is a key monitoring activity to assess how effective risk management is at supporting corporate objectives.

**Example:**

Risk management performance indicators may include the number of internal audits completed per annum, the number of internal audit findings accepted by management, the timeliness of remediating internal audit findings, the reduction in the number of extreme risks in the risk register.

## 10. Risk Appetite

Articulate the organisations risk appetite through a risk appetite statement. The risk appetite statement influences and guides decision making, clarifies strategic intent and ensures choices align with the capacities and capabilities of the agency.

**Example:**

There is no standard or universal risk appetite statement. Refer to pg. 22 of VMIA's Risk Management Guideline for assistance on how to develop a risk appetite statement.

## 11. Interagency and State Significant Risks

State the organisations approach to identifying and managing interagency and state significant risks.

**Example:**

Refer to pg. 51 of VMIA's Risk Management Guideline for guidance on how to identify and manage interagency and state significant risks.

## 12. Review and approval

State how often and who will review the risk management policy. Review of the risk management policy should take into the account progress made against the risk management improvement plan, which is a blueprint for how the risk management policy is implemented across the organisation.

### 13. References and related documents

<b>Associated policies</b>	Risk Management Improvement Plan Risk Management Procedure Risk Register
<b>References /statutory references</b>	AS/NZS ISO 31000:2009 – <i>Risk management - Principles and guidelines (20 November, 2009)</i>  HB436  <Insert statute in italics> <i>Example: Public Administration Act 2004</i>  <b>VGRMF – to be included</b>
<b>Attachments</b>	Example: Procedure or Form