TE TANGO AKATEREANGA MONI O TE IPUKAREA
MINISTRY OF FINANCE & ECONOMIC MANAGEMENT
GOVERNMENT OF THE COOK ISLANDS

FRAMEWORK

April 2025

About this Framework

This Framework sets out the structured **process** used to identify potential threats to the Ministry and to define the **strategy** for eliminating or minimising the impact of risk.

Risk Management is an enabling function that adds value to the activities and increases the probability of success in achieving our strategic objectives. It's about managing uncertainty and creating an environment where surprises are minimised.

This guide should be read with the Cook Islands Government Risk Management Policy.

.

Contents

1. What is Risk Management?

1.1 Introduction and purpose

Risk management is the process of making and carrying out decisions that will minimise the adverse effects of risk. In terms of losses, risks are commonly referred to as exposures to loss or simply exposures.

Risk management is the responsibility of **all** staff. Successful risk management is about a culture of all staff working to balance the need for minimising the impact of risk while maximising opportunity and the need for innovation and development.

The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives.

The Government of the Cook Islands Risk Management policy sets out each agency's obligations to proactively identify, prevent and mitigate risks and minimise disruptions and losses to agency operations and services.

The Ministry of Finance and Economic Management (the Ministry) consists of seven divisions: Office of the Financial Secretary, Revenue Management, Development Coordination, Treasury, Cook Islands Statistics Office, Economic Planning Division and the Major Projects and Procurement Support Division. The Ministry is a complex and dynamic Government agency providing diverse finance and economic services to its customers in the Cook Islands. The Ministry faces the challenge of embracing continual change to maintain efficiency while servicing the Cook Islands citizens with diverse needs and expectations.

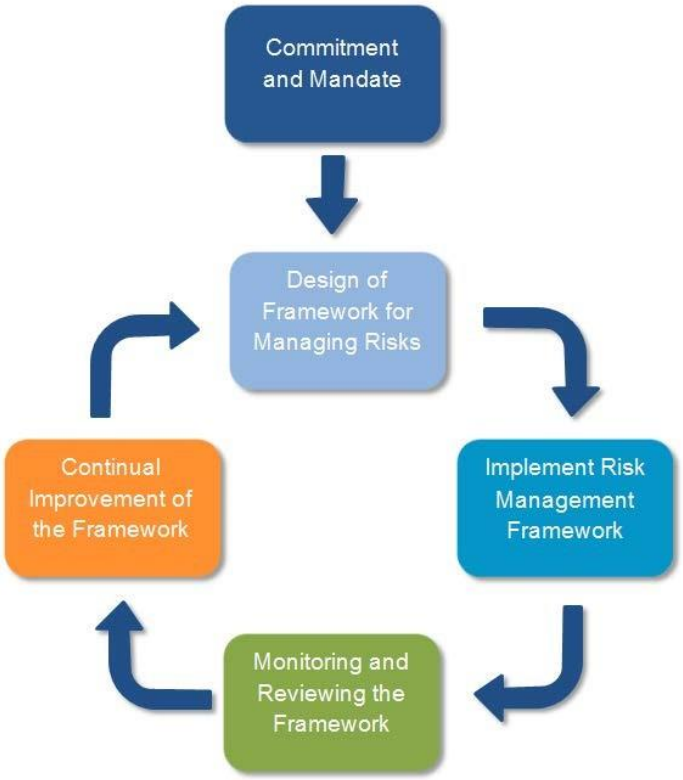
The Risk Management Framework has been established to support and facilitate positive change in the agency, allowing the Ministry to take advantage of opportunities and embrace innovation.

1.2 The Ministry's approach to managing risk

Our approach to managing risk:

- is iterative and assists us in setting our strategy, achieving our objectives and making informed decisions;
- is part of governance and leadership and is fundamental to how we are managed at all levels. It contributes to the improvement of management systems;
- is part of all activities associated with the Ministry and includes interaction with stakeholders;
- considers the external and internal context of the Ministry, including human behaviour and cultural factors.

The Ministry is committed to implementing a process by which strategic, operational and project risks are identified, communicated, monitored and regularly reported. To facilitate this, the Ministry has adopted the principles outlined in the Joint Australian New Zealand International Standard: Risk Management – Principles and Guidelines (AS/NZS ISO 31000:2018). This standard is considered 'best practice' within the risk management community. It includes the framework diagram illustrated, which has been implemented at the Ministry.



The Ministry's Leadership Team sets the acceptable risk level through the **Risk Appetite Statements**. These directives align with our strategy and will influence all evaluations of risk accepted by the Ministry.

1.3 The Ministry's risk management objectives

The Ministry's risk management objectives are to:

- **Improve decision-making** by incorporating effective risk assessment techniques into the decision-making process;
- Develop a **'risk aware' culture** that encourages all staff to identify and talk about risks;
- Provide a **simple process** for the early and systematic identification, analysis and assessment of risk and the development of plans for controlling and mitigating risk;
- **Integrate** risk management practices into all aspects of the Ministry's business activities and
- Enable **innovation** by increasing risk management competence.

2. Why do we manage risk?

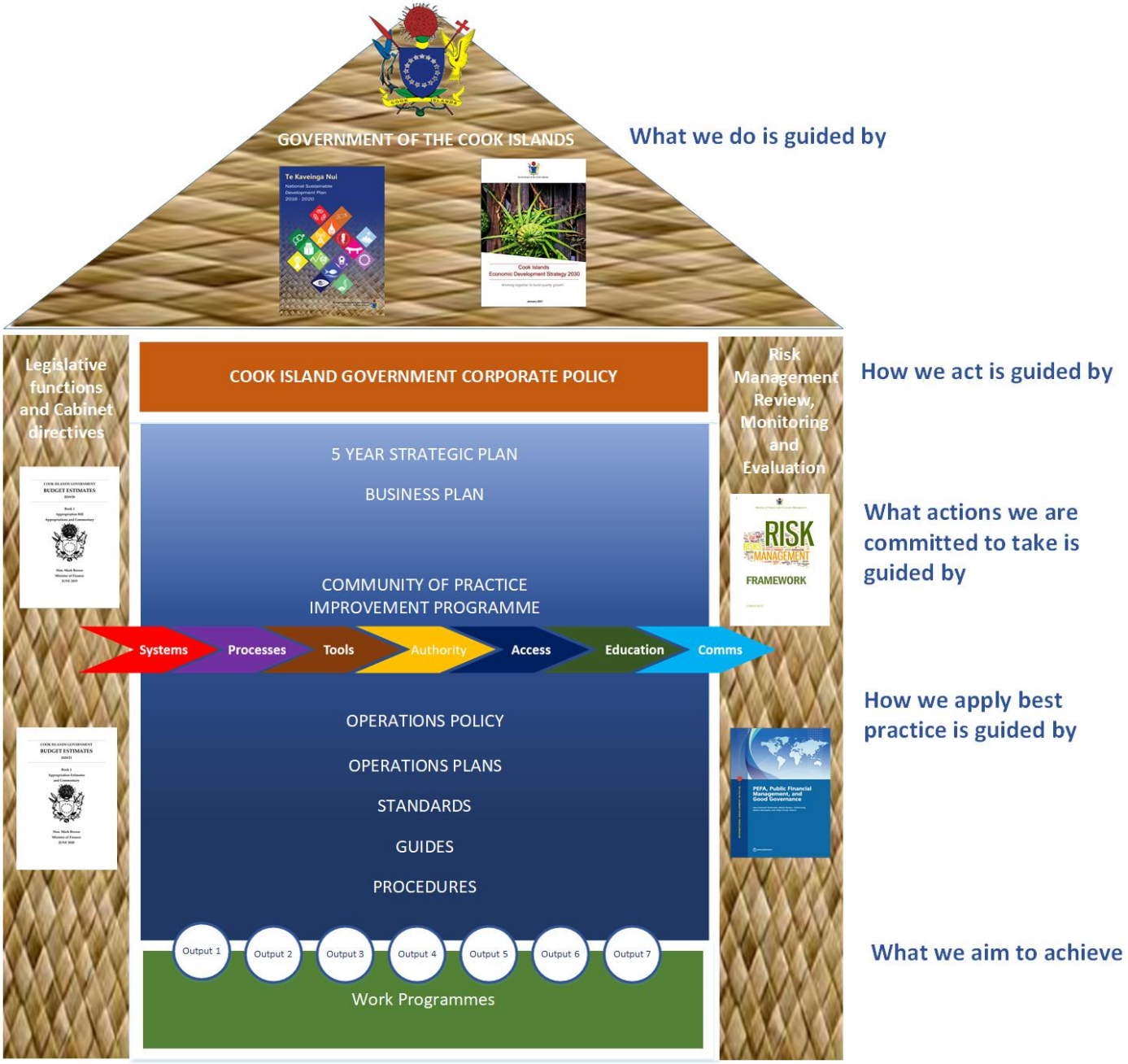
2.1 Risk management helps us to achieve our objectives

A key factor in realising the objectives of a strategy is the efficiencies gained from effective risk management. By incorporating risk management principles, agency leaders and business managers can understand and minimise the effects of risks on their goals and objectives by evaluating and treating risks.

The relationship between our Organisational Strategy and Risk Management is illustrated in the following diagram:

2.2 Risk management aligns with our organisational strategy

The diagram below shows the link between our National Sustainable Development goals and the Ministry's Strategy and how risk management aligns with them.



2.3 Risk management benefits

The development of effective risk management practices within the Ministry will assist in delivering the following benefits:

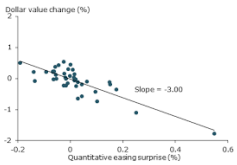
Attain long term goals

Make better decisions

Protect our assets

Enhance reputation

Improve performance



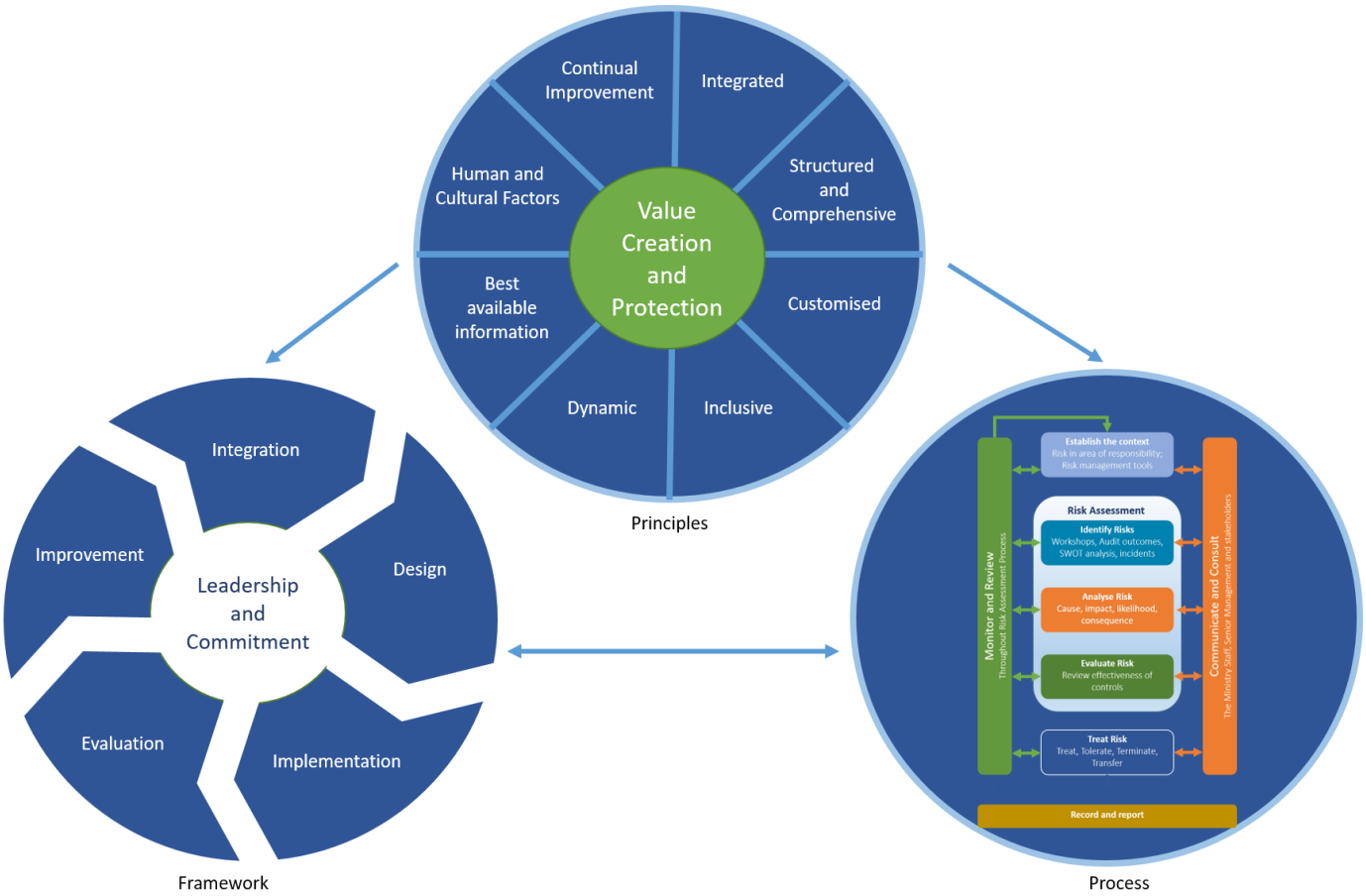
Reduce unwanted impacts and surprise events

Maximise opportunities

3. How do we manage risk?

3.1 Principles, Framework and Process

The Ministry has applied the Joint Australian New Zealand International Standard: Risk Management – Principles and Guidelines (AS/NZS ISO 31000:2018). Managing risk is based on the principles, Framework, and process outlined in this document and may need to be adapted or improved to manage risk efficiently, effectively, and consistently.



3.1.1 Principles

Effective risk management requires the elements of the Framework as follows:

- **Integrated** - Risk management is an integral part of all Ministry activities.
- **Structured and comprehensive** - A structured and comprehensive approach to risk management contributes to consistent and comparable results.
- **Customised** - The risk management framework and process are customised and proportionate to the Ministry's external and internal context related to its objectives.
- **Inclusive** - Appropriate and timely involvement of stakeholders enables their knowledge, views, and perceptions to be considered. It results in improved awareness and informed risk management.
- **Dynamic -** Risks can emerge, change or disappear as an organisation's external and internal context changes. Risk management anticipates, detects, acknowledges, and responds to those changes and events appropriately and timely.
- **Best available information** - The inputs to risk management are based on

historical and current information and future expectations. Risk management explicitly considers any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.

- **Human and cultural factors** - Human behaviour and culture significantly influence all aspects of risk management at each level and stage.
- **Continual improvement** - Risk management is continually improved through learning and experience.

3.1.2 Framework

The risk management framework aims to assist the Ministry in integrating risk management into significant activities and functions. The effectiveness of risk management will depend on its integration into the Ministry's governance, including decision-making. It requires support from stakeholders, particularly the Ministry's Leadership Team.

The Framework development encompasses integrating, designing, implementing, evaluating and improving risk management across the Ministry.

The Ministry will evaluate its existing risk management practices and processes, evaluate gaps, and address those gaps within the Framework. The individual components of the risk framework and how they work together will be customised to meet the Ministry's needs.

3.1.3 Leadership and commitment

The Managers, where applicable, will ensure that risk management is integrated into all business activities and demonstrate leadership and commitment by:

- customise and implement all components of the Framework;
- issue a statement or policy that establishes a risk management approach, plan or course of action;
- ensuring that the necessary resources are allocated to managing risk;
- assigning authority, responsibility and accountability at appropriate levels within the Ministry.

It will assist the Ministry to:

- align risk management with our objectives, strategy and culture;
- recognise and address all obligations, as well as its voluntary commitments;
- establish the amount and type of risk that may or may not be taken to guide the development of risk criteria, ensuring that we are communicated to the Ministry and its stakeholders;
- communicate the value of risk management to the Ministry and its stakeholders;
- promote systematic monitoring of risks;
- ensure that the risk management framework remains appropriate to the context of the Ministry.

The Managers are accountable for managing risk, while the Leadership Team is accountable for overseeing risk management and will:

- ensure that risks are adequately considered when setting the Ministry's objectives;
- understand the risks facing the Ministry in pursuit of its objectives;
- ensure that systems to manage such risks are implemented and operating effectively;
- ensure that such risks are appropriate in the context of the Ministry's objectives;
- ensure that information about such risks and their management is properly communicated.

3.1.4 Integration

Integrating risk management relies on understanding the Ministry's purpose, goals, and complexity. It is important that risk is managed in every part of our structure and that everyone in the Ministry is responsible for managing risk.

Governance guides the Ministry's course, our external and internal relationships, and the rules, processes and practices needed to achieve its purpose. Our structure translates governance direction into the strategy and associated objectives required to achieve desired sustainable performance levels and long-term viability. Determining risk management accountability and oversight roles are integral parts of the Ministry's governance.

Integrating risk management into the Ministry is a dynamic and iterative process that must

be customised to our needs and culture. It needs to be a part of, not separate from, our purpose, governance, leadership and commitment, strategy, objectives and operations.

3.1.5 Design

When designing the Framework for managing risk, we need to examine and understand it in both an external and internal context. It includes, but is not limited to:

External

- the social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, whether international, national, regional or local;
- key drivers and trends affecting the objectives of the organisation;
- external stakeholders' relationships, perceptions, values, needs and expectations;
- contractual relationships and commitments;
- the complexity of networks and dependencies.

Internal

- vision, mission and values;
- governance, organisational structure, roles and accountabilities;
- strategy, objectives and policies;
- the organisation's culture;
- standards, guidelines and models adopted by the organisation;
- capabilities understood in terms of resources and knowledge (e.g. capital, time, people, intellectual property, processes, systems and technologies);
- data, information systems, and information flows;
- relationships with internal stakeholders, taking into account their perceptions and values;
- contractual relationships and commitments;
- interdependencies and interconnections.

(a) Leaders' and managers' risk management commitment

The Leadership team and managers, where applicable, should:

- Demonstrate and articulate their continual commitment to risk management as stipulated by the Government of the Cook Islands Risk Management Policy or other forms that convey the Ministry's objectives and commitment to risk management;

- Ensure that the authorities, responsibilities and accountabilities for relevant roles with respect to risk management are assigned and communicated at all levels of the Ministry and should:

    - emphasise that risk management is a core responsibility and
    - identify individuals with the accountability and authority to manage risk (risk owners).

- Ensure allocation of appropriate resources for risk management, which can include, but is not limited to:

    - people, skills, experience and competence;
    - the Ministry's processes, methods and tools to be used for managing risk;
    - documented processes and procedures;
    - information and knowledge management systems;
    - professional development and training needs.

- Consider the capabilities of, and constraints on, existing resources.

(b) Establishing communication and consultation

The Ministry will establish an approved approach to communication and consultation to support the Framework and facilitate the effective application of risk management.

Communication involves sharing information with targeted audiences. The consultation also involves participants providing feedback with the expectation that it will contribute to and shape decisions or other activities. Communication and consultation methods and content should reflect stakeholders' expectations where relevant.

Communication and consultation should be timely; relevant information should be collected, collated, synthesised, shared, and appropriate; feedback should be provided, and improvements should be made.

3.1.6 Implementation

The Ministry will implement the risk management framework by:

- developing an appropriate plan, including time and resources;
- identifying where, when and how different types of decisions are made across the Ministry and by whom;
- modifying the applicable decision-making processes where necessary;
- ensuring that the Ministry's arrangements for managing risk are clearly understood and practised.

Successful implementation of the Framework requires the engagement and awareness of stakeholders. It will enable us to explicitly address uncertainty in decision-making while ensuring that any new or subsequent uncertainty can be considered.

Properly designed and implemented, the risk management framework will ensure that the risk management process is a part of all activities throughout the Ministry, including decision-making, and that any changes in external and internal contexts will be adequately captured.

3.1.7 Evaluation

To evaluate the effectiveness of the risk management framework, the Ministry will:

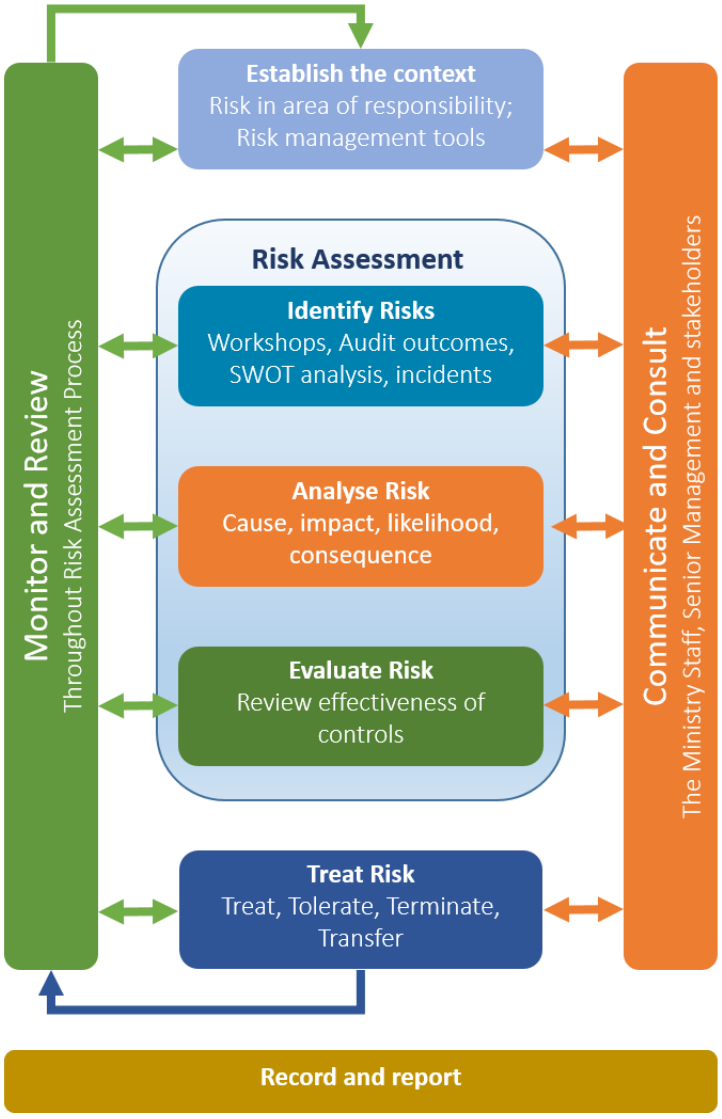
- periodically measure risk management framework performance against its purpose, implementation plans, indicators and expected behaviour, and
- determine whether it remains suitable to support achieving the objectives of the Ministry

3.1.8 Improvement

The Ministry will continually adapt and improve the suitability, adequacy, and effectiveness of the risk management framework and the integration of the risk management process. As relevant gaps or improvement opportunities are identified, the Ministry will develop plans and tasks and assign them to those accountable for implementation. Once implemented, these improvements should contribute to the enhancement of risk management.

3.2 Risk management process

This standard outlines the following Risk Management Process to ensure risks are dealt with uniformly and systematically. The process is illustrated and briefly explained below.



3.2.1 Establishing the context

Establishing the context means understanding the Ministry's objectives, defining internal and external factors that could be a source of uncertainty and setting the scope and risk criteria for the remaining risk management process.

3.2.2 Identify risks

The most common risk identification and assessment techniques include but are not restricted to:

- risk workshops;
- on-site inspections and audits;
- questionnaires and checklists;
- SWOT (strength, weakness, opportunity, threat) analysis;
- team meetings, project (toolbox) meetings, and site meetings

3.2.3 Analyse risk

It involves analysing the identified risks against the agency context to establish the potential impact on the event's objectives and its objectives and likelihood. A single event can have multiple impacts; all identifiable possible impacts need analysis.

The risk analysis can be carried out either qualitatively, quantitatively, or a combination of both. For example, **the qualitative analysis** would require the likelihood of an incident to be measured as low, medium, or high. **Quantitative analysis** may require the likelihood measure to be in percentage form, e.g. a 20% likelihood of an incident. Irrespective of the method used, there must be a full understanding and a consistent analysis approach.

3.2.4 Evaluate risk

The evaluation process looks at the strength of the current controls to mitigate the extent of potential losses. A decision is required as to whether the current controls are sufficient or whether additional controls are necessary.

3.2.5 Treat risk

Risk treatment (or mitigation) is the process of modifying (positively) the risk in terms of its consequence and/or likelihood.

For each risk, consideration is to either:

- **Treat** – additional control measures to reduce consequence and/or likelihood;
- **Tolerate** – accept the current level of risk;
- **Terminate** – remove the source of risk;
- **Transfer** – transfer risk to a third party, generally through insurance or another entity. It should be noted that some risks (e.g. reputational risk) will remain.

3.2.6 Communicate and consult

Communication and consultation require involving internal and external stakeholders throughout the risk management process. Communication and consultation begin at the outset of establishing the 'ground rules and methodology required to achieve consistency throughout the process.

3.2.7 Monitor and review

Risks and associated controls and mitigation strategies should be regularly reviewed and monitored to understand how they are affected by the constant changes inherent in our business environment.

3.2.8 Record and report

The risk management process and its outcomes should be documented and reported through appropriate mechanisms. Recording and reporting aim to:

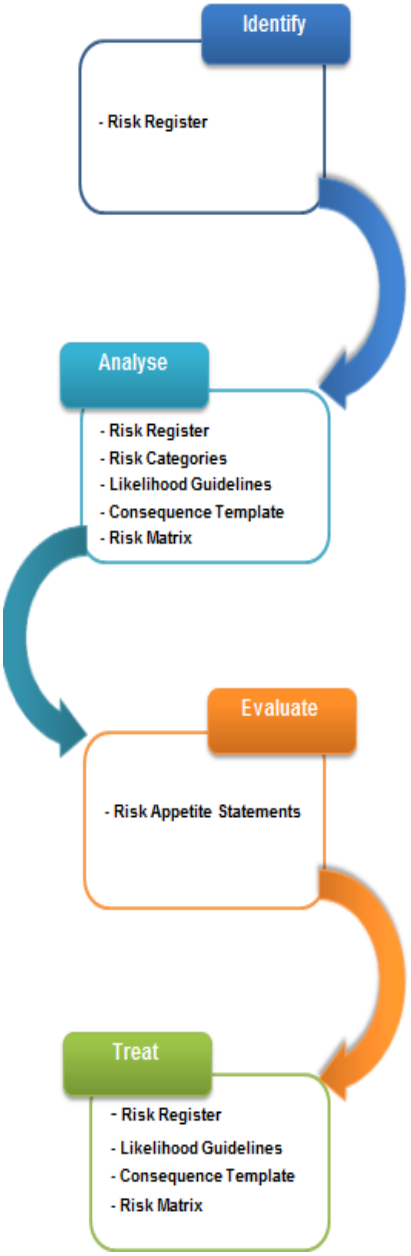
- communicate risk management activities and outcomes across the Ministry
- provide information for decision-making;
- improve risk management activities;
- assist interaction with stakeholders, including those responsible and accountable for risk management activities.

Decisions concerning the creation, retention, and handling of documented information should be considered, but they should not be limited to their use, information sensitivity, and external and internal context.

Reporting is an integral part of the organisation's governance and should enhance dialogue with stakeholders and support top management and oversight bodies in meeting their responsibilities. Factors to consider for reporting include, but are not limited to:

- differing stakeholders and their specific information needs and requirements;
- cost, frequency and timeliness of reporting;
- method of reporting;
- relevance of the information to organisational objectives and decision-making.

3.3 Turning theory into practice – Risk management tools



3.3.1 Risk register

The **Risk Register** is used to record, analyse and communicate risks. It should be used as a 'live' document and kept current as risks change. Detailed instructions for use are contained in the Risk Register document.

An example of the **Risk Register** is attached as **Appendix A**.

3.3.2 Risk categories

The Risk Register includes a requirement to define a risk category. Categorising risks is important for reporting purposes. It allows the risk owner to understand where higher risk concentrations sit within their business unit or project. Categorisation should be focused on description rather than a consequence. For example, a risk might be described as "poor governance", and the consequence is "reputational damage". The category, in this case, should be governance rather than reputation.

A full list of categories, definitions, and sources of threat is attached in **Appendix B**.

3.3.3 Risk consequence template and likelihood guidelines

Measuring risk is an important part of understanding its impact. Risks are measured in the Risk Register by estimating the likelihood and consequence and assigning a number rating (refer to **Appendices C and D**). These risk ratings are multiplied to give the risk score. The risk rating is recorded inherently (before controls) and residually (after controls).

3.3.4 Risk matrix

The Risk Matrix assigns colours and ratings to the risk scores, measuring from green (low) to burgundy (extreme). The Risk Matrix is attached as **Appendix E**.

3.2.5 Risk appetite statements

Risk appetite statements are a directive from the Ministry's Leadership Team to indicate their comfort levels for risk. They broadly fit into the risk categories. Mitigation actions should be based on the Risk Appetite Statements. Where residual risk ratings are higher than the risk appetite directives, mitigation strategies must be adopted to lower risk to the required level. If staff cannot apply a mitigation strategy and the risk cannot be tolerated, then the risk should be escalated to the leadership team for ownership and management. The Risk Appetite Statements are attached as **Appendix F.**

3.4 Risk reporting

Risks are captured on the centralised Ministry's Risk Register. It is to be owned, updated, and regularly maintained by each division and is subject to quarterly review by the Ministry's leadership team.

The risk register should be treated as a 'live document' and regularly updated rather than a quarterly report. Risk reporting through the business unit risk register can be a means of identifying risks that require escalation.

The Ministry has a legal and custodianship obligation to manage risks. Business unit reporting will include top current risks and emerging risks that could have a future influence on the Ministry. These risks are consolidated into a Ministry-wide summary quarterly and included in the leadership team's quarterly report.

A Top Risk report is maintained by the Leadership Team and updated quarterly. This report is influenced by the business unit reporting and the Ministry's Leadership Team's observation of external and strategic risk.

4. Related Legislation

- Public Services Act 2009
- Employment Relations Act 2012
- Ministry of Finance and Economic Management Act 1995-96
- Disaster Risk Management Act 2007
- Public Expenditure Review Committee Act 1995-96.

5. Related documents

This document is to be read in conjunction with other documents within the Cook Islands Government and the Ministry, which include but are not restricted to:

- Government of the Cook Islands Risk Management Policy
- MFEM Strategic Plan 2022-26
- Economic Development Strategy 2030
- HYEFU 20/21 Risk Categories:
  - Fiscal Risks
  - Global Economic Risks
  - Natural Disasters
- PEFA Review 2021.
- Project Management Assessing and Managing Activity Risk Guideline
- The Ministry's Disaster Risk Management Plan and Disaster Recovery Plan.
- The Ministry's Business Continuity Plans
- Technical Assistance Cook Islands Scoping Mission Report – Financial Resilience for Disaster Framework

6. Appendices

- Risk Register (Appendix A)
- Risk Categories (Appendix B)
- Risk Consequence Template (Appendix C)
- Risk Likelihood Guidelines (Appendix D)
- Risk Matrix (Appendix E)
- Risk Appetite Statements (Appendix F)
- Terms and Definitions (Appendix G)

6.1 Appendix A: Risk register

SAMPLE

Ref ID # Division and Unique No.	Risk Type	Risk and Impact Description	Risk Drivers (Causes of Risk)	Risk Category	Risk Owner (Title)	Risk Owner (Department / Team)	Inherent Risk (Before Controls)			Existing Controls (Current implemented controls)	Prevetative / Detective	Control Owner	Residual Risk (After Controls)			Risk Rationale	Additional Controls Required?	Review Date	Open / Closed
							Likelihood	Consequence	Risk rating (RAG)				Likelihood	Consequence	Revised Risk rating (RAG)				
MPPS 1	Business	External or internal project events may have a material impact on the health and safety or wellbeing of staff or cause death, which may result in emotional impacts on staff and public, low staff morale and reputation damage.	Inadequate Identification and communication of H&S Risks to staff and management Staff are not trained in the identification of hazards and risks.	Organisational Management	Manager	Major Projects Team	Rare	Minor	Low	Risk Manager process is in place to record H&S Risks and Incidents. These are reviewed by management as they are entered into the system and corrective action and controls are implemented where needed. Additional reviews are performed on a quarterly basis by the leadership team. Mandatory H&S safety training has been deployed and all staff are required to attend this course. Health and safety rep in place to assist staff that are experiencing difficulties as a result of an incident.	Detective Preventative Detective	Administrator, Major Projects and Procurement Support Division	Unlikely	Moderate	Moderate	With effective monitoring and reporting in place, managementt are able to better identify and address areas of risk, thus reducing the potential likelihood and impact of incidents that occur. Staff are also trained in this area, which creates a sense of awareness in staff to avoid potential hazards Health & Safety Rep allows for the impacts of incidents to staff be dealt with in a professional manner.	Continue to raise awareness of H&S risks and incidents through open communication channels with bi-weekly H&S updates provded to the Director	30/06/2019	Open

6.2 Appendix B: Risk categories

Risk Category	Category Description	Source of threat
Strategic	Failure to achieve strategic objectives.	• Budgeting (availability or allocation of resources) • Partnerships or relationships with third parties fail to deliver strategic outcomes. • Failure to invest appropriately • Insufficient capital investment or shortfall in revenue expected/planned. • Failure to develop the capability for research and innovation (exploit opportunities) • Failure to respond to national or significant disasters • Inadequate insurance/contingency provision for disasters like fire, floods, etc. • Failure to manage national pandemics • Failure to prevent civil action by employees/public servants and the public • Failure to invest in new and relevant technology to achieve objectives • Suppliers fail to meet contractual commitments (quality, quantity, timelines, etc.) • Business interruptions significantly affect business operations.
Political / Governance / Security	Negative impacts from decisions made for political purposes	• Change of Government and effect on policies, direction, objectives, strategy and plans • Adverse public opinion from government policies or decisions • Failure to mitigate negative media messaging • Political interference • Non-performance of duties of elected members and proprietary/compliance with relevant requirements / ethical considerations • Damage to the reputation of the Ministry, Cook Island Government or any of its elected members or officers • Absence of strategic communication between Ministers and agency heads • The security, safety and wellbeing of our stakeholders, customers and the public are jeopardised.

Risk Category	Category Description	Source of threat
Organisational Management	Failure of internal agency infrastructure, staff resources and operations	**Leadership and Direction** • Management incompetence or poor leadership • Underperforming agency • Inadequate operational policies and sound management practices • Under-performance of service providers or contractors • Absence of clear delegations of authority (e.g. recruitment remuneration, termination and financial) • Failure of business unit budgets or financial planning to include management, control and inability to meet financial commitments and strategies • Failure to establish a positive culture • Failure to establish effective business continuity mechanisms **People Development and Management** • Poor staff recruitment and remuneration practices • Unclear roles and responsibilities • Absence of performance management • Failure to plan for workforce requirements and training needs • Failure to manage employment disputes or misconduct **Financial and Resource Management** • Unethical practices and transactions • Wrongful or criminal deception intended to result in financial or personal gain. • Poor asset management results in loss or damage to assets owned or operated to provide services, including land, property, equipment and information. • Poor information management and collection of data • Poor internal controls to prevent fraud or misappropriation of funds • Inadequate health and safety practices for the agency and its stakeholders • Individual or group interests are given unwarranted priority • Failure to meet the needs, wants, and expectations of our customers with respect to service standards and service delivery • Absence of quality assurance measures in service delivery • Operation processes are not customer-centric and fit for purpose • Absence of agency communication plan • Lack of collaboration with stakeholders on strategy and service delivery of major projects and programmes

Risk Category	Category Description	Source of threat
Economic / Financial / Market	Negative impacts from the external operating environment	• Failure to address economic factors (such as exchange rates, interest rates, inflation) • Failure to meet projected tax and trading revenue targets • Global and regional market trends adversely affect the national economy
Legal and Regulatory	Exposure to litigation and damages awards	• Failure to obtain legal advice before making decisions • Failure to obtain appropriate approvals (e.g. building permits) • Unforeseen contingent liabilities • Failure to control intellectual property (as a result of abuse or industrial espionage) • Failing to comply with statutory or common law, delegations, regulations and contractual obligations • Failure to enforce legal, regulatory or contractual obligations • Inclusion of new or amended statutory environment
Climate Change or Environmental	Negative impacts from natural disasters and failure to protect or preserve the environment	• Natural disasters, e.g. cyclones, tsunamis, earthquakes and flooding • Artificial hazards/disasters, e.g. fires • Lack of environmental awareness practices (Reduce, reuse, recycle)
Technology, Equipment & Systems	Failure of technical assets and infrastructure.	• Inadequate ICT equipment • Poorly resourced ICT systems support • Centralised network failures • Business interruptions • Failures arise from the current provision of technology and changing demand/capacity. • Use or misuse/security of new or existing technology.

6.3 Appendix C: Risk consequence template and guidelines

Risk Category	Type	Insignificant 1	Minor 2	Moderate 3	Major 4	Extreme/Catastrophic 5
Strategic	**Business / Operational Interruptions**	No loss of operational capability and/or minimal disruption to service levels. Minimal loss of internal operational capacity.	Loss of operational capability in some areas and/or some disruption to service levels. Loss of internal operational capacity up to 1 week,	Serious loss of operational capability for over 6 weeks and /or disruption to service levels for 4-6 weeks. Loss of operational internal capacity 1-3 weeks.	Serious loss of operational capability for over 8 weeks and major disruption to service levels. Loss of internal operational capacity 4-6 weeks.	Serious loss of operational capability for 3 - 4 months and serious disruption to service levels. Loss of internal operational capacity >6 weeks.
	Customers	Unable to fully meet local expectations >95%.	Unable to fully meet local expectations >90%.	Unable to fully meet local expectations >85%.	Unable to fully meet local expectations >80%.	Unable to fully meet local expectations <80%.
	Delivery of Commitments	Planned delivery met >95%.	Planned delivery met >90%.	Planned delivery met >85%.	Planned delivery met >80%.	Planned delivery met <80%.
	Financial	No impact on achievement of output targets, business can continue as normal. Localised failure only. Financial loss <1% operating budget.	Up to 1% impact on targets. Limited to a single business area of the organisation. Financial loss 1-3% operating budget.	Up to 5% impact on targets. Financial loss 3-6% operating budget.	Up to 10% impact on targets. Financial loss 6-10% operating budget. Impact to multiple and diverse areas of the Government.	Greater than 10% impact on achievement of key performance targets. Financial loss >10% operating budget.
	Suppliers	Benefits will take longer to achieve than anticipated. No discernible change to status quo.	Some anticipated benefits not realised and/or achievable. Some changes to the operation of the partnership required - no change to agreement.	Partnering benefits not fully realised. Some changes to the partnership arrangement required.	No demonstrable benefit achieved by partnering. Significant change to the partnership arrangements required.	No interest in forming partnership or existing partnership fails. Contracts abandoned.
Political / Governance / Security	**Governance**	Rare occurrences of disregard of requirements stipulated under the Public Services Manual and relevant governance policies.	Infrequent disregard of requirements stipulated under the Public Services Manual and relevant governance policies.	Occasional disregard of requirements stipulated under the Public Services Manual and relevant governance policies.	Some disregard of requirements stipulated under the Public Services Manual and relevant governance policies.	Wide scale disregard of requirements stipulated under the Public Services Manual and relevant governance policies.
	Political	No or minor change.	Occasional changes to direction, objectives, strategies or policies.	Limited changes in direction, objectives, strategies or policies.	Significant changes to the Cook Islands Government direction, objectives, strategies and policies.	Complete reversal of direction. objectives, strategies and policies. Wide scale deferment or abandonment of significant projects in progress.
	Public perception (Reputation)	No significant adverse comment or media coverage. Letter to the Ministry and/or to Finance Secretary or Directors. Minimal public disquiet.	Adverse comment on local media (coverage 3 days +). Letters to Hom, complaints to Elected Members. Public disquiet limited to small sections of the community.	Adverse comment on local media (coverage 1 week +). Coverage in national media. Public disquiet one or more community	Adverse comment on local media (coverage 2 – 3 weeks). Coverage in international media. Public disquiet over majority of Rarotonga or Pa Enua e.g. major fraud issue	Adverse comment on local media (coverage for 4 weeks +) Coverage in international media >3 days. All plus “Commission of Inquiry”/questions in parliament. Widespread civil unrest.
	Security	The vulnerability is not of concern. Relevant security control or other remediation is fully implemented, assessed and effective.	The vulnerability is of minor concern, but effectieness of remediation could be improved. Relevant security control or other remediation is fully implemented and somewhat effective.	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security controls or other remediation is partially implement and somewhat effective.	The vulnerability is of a major concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implements; compensating controls are in place and at least minimally effective.	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.

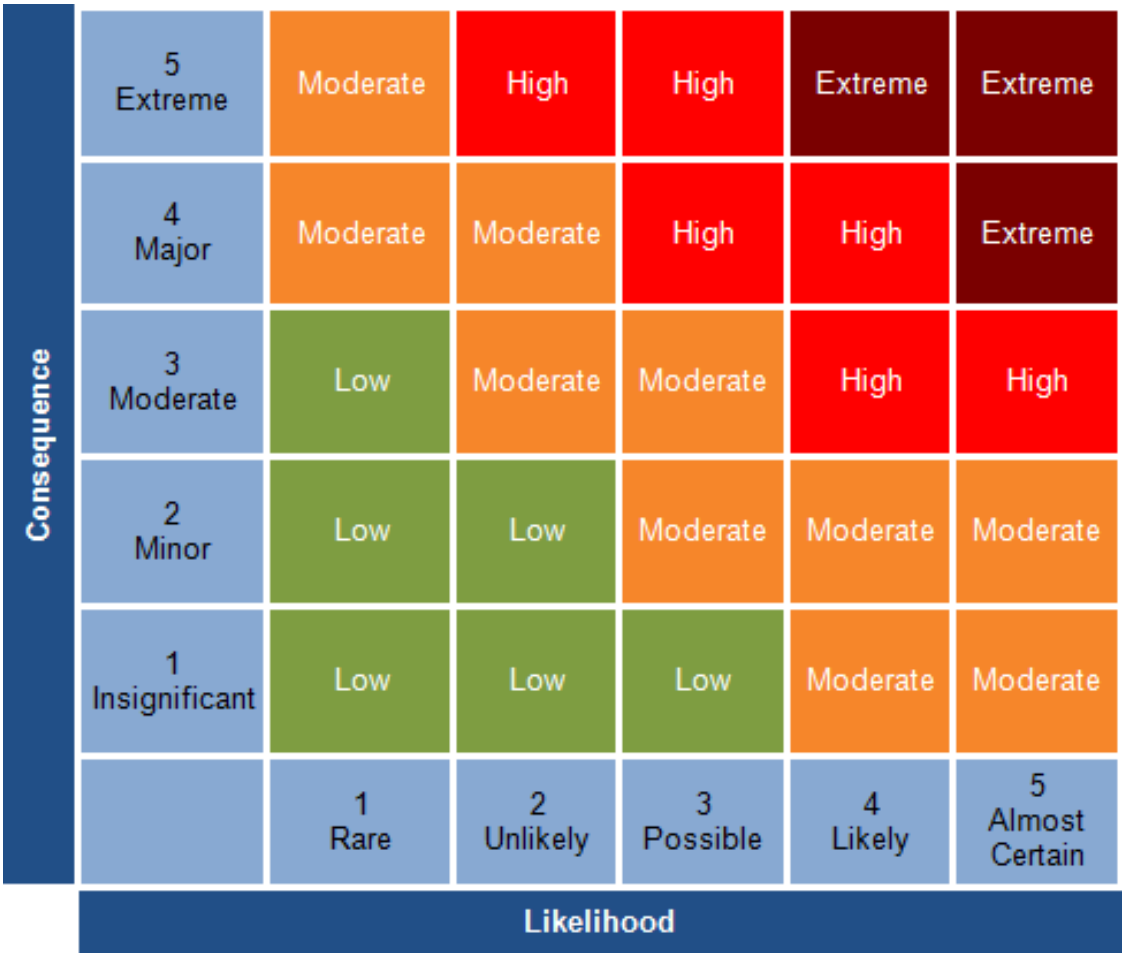
Risk Category	Type	Insignificant 1	Minor 2	Moderate 3	Major 4	Extreme/Catastrophic 5
Organisational Management	**Assets**	Damage to or loss of a minor asset, or minor damage to an asset. Assets not useable / available for short defined period.	Damage to, or loss of a asset <$10K. Assets not useable / available for short undefined period.	Damage to, or loss of an asset <$50K. Assets not useable / available for the long-term.	Damage to, or loss of an asset <$500K. Assets not useable / available for the medium term.	Damage to, or loss of a significant or high value asset >$1M. Total loss of asset that cannot be replaced.
	Health and Safety (Organisational and External)	Injury requires first aid treatment. Insignificant discomfort requiring intervention e.g. workstation assessment.	Injury or illness requires treatment by a medical or other registered practitioner.	Injury or illness results in at least three days of lost time. Notice issued by regulator or Health and Safety Representative.	Injury or illness results in thirty days lost time, or a permanent disability. The Ministry breaches law resulting in prosecution and penalties.	One or more fatalities. Considerable penalties and prosecutions. Multiple law suits and jail terms.
	Information / Data Management	Quality of information remains high <90% accurate and timely.	Quality of information remains high >80% accurate and timely.	Quality of information remains high >70% accurate and timely.	Quality of information not acceptable <70% accurate and timely.	Quality of information is not reliable and not timely.
	Processes	Processes are efficient and effective = >90%.	Processes are efficient and effective = >80%.	Processes are efficient and effective = >70%.	Processes are inefficient and ineffective = <70%.	Processes are inefficient and ineffective = <90%.
	Skills and knowledge	Permanent staff turnover equal to or 1.25 times industry average. Insignificant skill gaps.	Permanent staff turnover 1.25 – 1.5 times industry average. Few specialist skill gaps.	Permanent staff turnover 1.5 – 1.75 times industry average. Some specialist skill gaps.	Permanent staff turnover 1.7 – double industry average. Major specialist gaps.	Permanent staff turnover is more than double industry average. No internal or external specialist skills available.
Economic / Financial / Market	**Economic**	<0.01% of GDP.	0.01 - 0.09% of GDP.	0.1 - 0.99% of GDP.	1 - 9.99% of GDP.	>10% of GDP.
	Market Developments	Insignificant Global and regional market trends adversely affect the national economy.	Minor Global and regional market trends adversely affect the national economy	Moderate Global and regional market trends adversely affect the national economy	Major Global and regional market trends adversely affect the national economy	Extreme Global and regional market trends adversely affect the national economy
	Cultural / Community	No significant community (e.g. sociological or cultural) issues. Localised short-term reversible disruption to the community, resulting in no noticeable damage. e.g. <5 houses; < 2 businesses	Local community (e.g. sociological or cultural) concerns that can be dealt with. Localised minor reversible damage and disruption to the community, with no potential public safety issues or long-term effect. e.g. <10 houses; < 5 businesses	Significant community (e.g. sociological or cultural) concerns causing delays and modifications to plans. Localised medium-term (1 to 3 weeks) reversible damage and disruption, to the community, with some potential safety issues. e.g. <25 houses; < 10 businesses	Widespread significant community (e.g. sociological or cultural) causing significant delays and modifications to plans. Localised or widespread long-term (greater than 3 weeks) reversible or irreversible damage; disruption to community. e.g. <50 houses; < 20 businesses	Major community (e.g. sociological or cultural) concerns causing major re-think or complete failure of plans. Localised or widespread damage and disruption to the community (any duration), with potential for loss of life. e.g. >50 houses; > 20 businesses
Legal and Regulatory	**Privacy / Information**	Confidential / private information is disclosed but does not have any adverse effect.	Confidential / private information is acquired by an unauthorised person or group.	Some confidential / private information is disclosed to an unauthorised person or team.	Some confidential / private information is released to the media.	Widespread release of confidential / private information to the media.
	Legal Action	The Ministry's is sued for a sum <$10,000.	The Ministry's is sued for > $10,000 < $100,000.	The Ministry's is sued for > $100,000 < $250,000. Complaint to the Ombudsman or other statutory offices.	The Ministry's is sued for > $250,000 < $1,000,000. Legislative non compliance; prosecution or potential for a fine or significant criticism by Judiciary or Ombudsman. Adverse ruling by the Ombudsman or other statutory officer with power to investigate or make rulings.	The Ministry's is sued for > $1,000,000. Legislative non-compliance involving the potential for imprisonment of an Elected Member, HoM or Senior Officer. Judicial review of a Ministry decision on a matter relating to funding or rates.

Risk Category	Type	Insignificant 1	Minor 2	Moderate 3	Major 4	Extreme/Catastrophic 5
Climate Change or Environmental	**Environment (Natural and Built)**	Small localised and reversible environmental impact resulting in: - Slight, short-term damage to use of land and/or water; - Slight short-term damage to land and/or water ecosystems; - No noticeable species reduction; - Occasional inconsistency with the intent of legislation, NSDA, and the Ministry's Mission, Goals and Principles.	Contained and reversible (minimal) environmental impact resulting in: - Localised minor reversible damage to (use of) land and/or water; - Localised minor reversible damage to land and/or water ecosystems; - Temporary reduction in one species; - Minor erosion and/or damage to property; - Minor inconsistency with the intent of legislation, NSDA, and the Ministry's Mission, Goals and Principles.	Measurable damage to the environment; significant corrective action resulting in: - Localised, medium term reversible damage to land and/or water ecosystems; - Moderate reduction in one or more species; - Moderate erosion and/or damage to property. Recovery time 1 month; - Repeated inconsistency with the intent of legislation, NSDA, and the Ministry's Mission, Goals and Principles.	Irreversible localised damage (major) to the environment resulting in: - Widespread, long term reversible damage to land and/or water ecosystems; - Significant reduction in one or more species; - Severe erosion and/or damage to property. Recovery time up to 6 months; - Repeated and significant inconsistency with the intent of legislation, NSDA, and the Ministry's Mission, Goals and Principles.	Extensive irreversible damage (widespread) to the environment resulting in: - Widespread, irreversible damage to land and/or water ecosystems; - Permanent loss of one or more species; - Destruction of property / widespread flooding. Recovery time exceeding 6 months; - No recognition of the intent of legislation, NSDA, and the Ministry's Mission, Goals and Principles.
Technology, Equipment and Systems	**Technology**	Intermittent capacity and capability problems.	System capacity and·capability has some effect on performance.	System capacity and capability hinders performance to all users.	System capacity and/or capability cannot cope with demand for use.	Complete system failure or abandonment of system.
	Equipment	Occasional misuse of equipment but no system security threat posed.	Occasional misuse of equipment that poses a low level threat to system security or that could bring the Ministry into disrepute.	Frequent misuse of equipment that poses a low level threat to system security or that could bring the Ministry into disrepute.	Any misuse of equipment that poses a medium level threat to system security or high level threat to system security or that could bring the Ministry into serious disrepute.	Any misuse of equipment that poses a high level threat to system security or involves the use of equipment for criminal activities.
	Systems	Loss of systems / data in some operational areas.	Loss of key systems/ data disrupts local operations for <3 days.	Loss of key systems / data disrupts local systems for > 3 days.	Loss of key systems / data disrupts local systems for > 5 days.	Absolute loss of key data or disruption to local service provision > 7 days.

6.4 Appendix D: Risk likelihood guidelines

	General description	Frequency expression
Almost certain 5	Risk event expected to occur in most circumstances	90% chance within next 12 months; or 18 out of every 20 years
Likely 4	Risk event will probably occur in most circumstances	55% chance within next 12 months; or 11 out of every 20 years
Possible 3	Risk event should occur at some time	25% chance within next 12 months; or 5 out of every 20 years
Unlikely 2	Risk event could occur at some time	10% chance within next 12 months; or 1 out of every 10 years
Rare 1	Risk event may occur only in exceptional circumstances	Up to 4% chance within next 12 months; or once in 25 years

6.5 Appendix E: Risk matrix



6.6 Appendix F: Risk appetite statements

1. General Statement of Risk Appetite

Risk appetite is the level of risk the Ministry of Finance and Economic Management (the Ministry) is prepared to tolerate or accept in pursuing our strategic objectives. We aim to consider all options, respond to risk appropriately and make informed decisions that are most likely to result in the successful delivery of infrastructure and services while also providing an acceptable level of value for money.

We operate within a controlled environment. It includes risk and assurance oversight, governance oversight and a robust financial planning process, including the NSDA and annual agency Business Plans. The Cook Islands Audit Office provides external oversight. By formally outlining risk appetite statements, we clarify where comprehensive controls are required and enhance transparency.

The Ministry is a government agency that takes the delivery of services to our customers and communities at value for money seriously. We generally have a low appetite for risk-taking that will adversely affect our core objectives.

The Ministry will not accept risks impacting our people's safety and welfare, legal obligations, and economic and financial stability. We are willing to take well-defined risks at a low to moderate level, resulting in the achievement of our strategic initiatives and objectives.

While effective risk management identifies threats, it can also identify opportunities. We are willing to support initiatives optimising opportunities and innovation when the benefits outweigh the risks.

Our leadership team will manage, apply treatment plans, and monitor all risks above and beyond the appetite statements.

2. Appetite Assessment Table

Appetite	Description
High	The Ministry is willing to accept **high** risk to pursue a strategic opportunity that will result in a high level of return or benefit to the community or where required by statutory requirements. If the Ministry expects that: - The Ministry's viability, reputation and services **may be severely damaged** should the risk eventuate, **but** - control measures to mitigate the likelihood and consequence of the risk are in place and are actively monitored.
Moderate	If the Ministry expects that: - The Ministry's viability, reputation and services **may be affected in a major** way should the risk eventuate, **but** - Control measures to mitigate the likelihood and consequence of the risk are in place and are actively monitored.
Low	If Ministry expects that: - The Ministry's viability, reputation and services **will only be affected in a minor** way should the risk eventuate, **and** - Control measures to mitigate the likelihood and consequence of the risk are in place.
Very Low	The Ministry will pursue an objective or initiative if control measures can minimise risk to insignificant levels.
No Appetite	The Ministry is **not willing to** accept risks that may result in financial loss, injury, legal, regulatory non-compliance and fraud.

3. Detailed Risk Appetite Statements

3.1 Strategic

The Ministry recognises the importance of servicing the Cook Islands' needs and people and that our operations' ongoing development and innovation through detailed strategic planning is required.

Our priorities are engaging and enabling our communities, providing customer-friendly services, and building a high-performance culture. We recognise that to achieve this, and we must take advantage of opportunities and encourage innovation to achieve our strategic outcomes.

The Ministry aims to show leadership in the government sector in financial stewardship and delivering value for money to our customers, citizens, and communities.

- The Ministry has a **moderate** to **high** appetite for measured, assessed and treated risks that will enable innovation and deliver strategic outcomes.

- The Ministry has a **moderate** appetite for risks that involve partnerships or relationships with third parties to deliver strategic outcomes.

- The Ministry has a **very low** appetite for risks that would adversely affect the Government's financial planning.

3.2 Organisational Management

We are stewards of Cook Island Government assets, and we use all money and resources in a way that delivers the best value for money and builds trust with the people we serve. The Ministry is open and transparent in how we operate and make decisions, and we act with integrity and in accordance with the law at all times.

Our employees are key determinants of our success and are often the "face" of the Ministry to customers and stakeholders. Maintaining a well-trained, well-qualified workforce is a critical function of individual managers and directors.

The Ministry values a positive, inclusive culture and collaborates toward common goals. Our behaviours guide how we work and interact with others and help us to strive for excellence. We act in a way that builds trust and values individual contributions.

- The Ministry aims to maximise returns on our assets, so it has a **low** to **moderate** appetite for taking opportunity risks to increase returns from our assets and lower costs.

- The Ministry will only accept a **low** to **moderate** level of risk that will affect staff performance and engagement, where considerable gain can be made to the Ministry as a high-performance organisation and affect our organisational strategy.

- The Ministry has **no appetite** for risks that will compromise our people's health,

safety, and wellbeing or cause harm to them, including staff, customers, and our community.

- The Ministry has a **very low** appetite for discrimination, bias, bullying or unfair treatment of individuals or groups. We're comfortable to be ourselves at work.

3.3 Political / Governance / Security

The Ministry provides high-level economic and financial support services across the Cook Island Government with many stakeholders interested in our success in delivering our services to our customers, citizens and communities.

The Ministry is part of the Cook Islands Government, and we set very high standards for operating as an agency.

- The Ministry has a **very low** appetite for risks arising from inadequacies in governance frameworks, structures and processes and operational impacts from elections.

- The Ministry has a **low** appetite for risk that does not keep our customers, citizens and communities safe from hazards of civil and national security events.

- The Ministry has a **very low** appetite for risks or conduct that would affect our reputation, customers' trust and confidence and the communities we serve.

- The Ministry has a **low** appetite for risks relating to the non-delivery of commitments, including projects and political commitments, in the NSDA and our annual business plans.

- The Ministry has a **very low** tolerance for dishonesty, fraud, and corruption, and we have a shared responsibility to prevent and report any incidents of illegal behaviour.

3.4 Technology, Equipment and Systems

- The Ministry has a **low appetite** for disruptions to operations and processes. These business disruptions will only be accepted if they are unavoidable in a transformational change or strategic initiative and will not impact service delivery to customers and communities.

- The Ministry has a **very low** appetite for risks that will impact our technological capability to deliver our services.

3.5 Economic / Financial / Market

- The Ministry has **no appetite** for risks that would adversely affect the Government's credit rating and long-term economic and financial stability or breach any funding policies.

.

3.6 Legal and Regulatory

The Ministry is a complex organisation subject to numerous legal and regulatory obligations. We recognise the importance of complying with the law and any regulations.

- The Ministry has a **low** to **moderate** appetite for risk associated with innovation in our regulatory activity delivery.

- The Ministry has **no appetite** for non-compliance with the law, risks that will affect our ethical obligations or fraudulent activities.

Any potential or identified breaches of the law or regulations will be remedied as soon as practicable.

3.7 Climate Change or Environment

- The Ministry has a **very low** appetite for risks affecting our environment and sustainability objectives.

4. Review

The **Risk Appetite Statements** will be reviewed annually or following any significant event.

4.1 Appendix G: Terms and Definition

To ensure commonality and understanding of terminology, the following terms will be used by the Ministry staff:

TERM	DEFINITION
Communication and consultation	The Ministry conducts a continual and iterative process to provide, share or obtain information and engage in dialogue with stakeholders regarding risk management.
Establishing the context	The external and internal parameters must be considered when managing risk and setting the scope and risk criteria for the risk management policy.
Event	Occurrence or change of a particular set of circumstances.
External context	The external environment in which the Ministry seeks to achieve its objectives.
Impact	The consequence of an event affecting objectives.
Internal context	Internal environment in which the Ministry seeks to achieve its objectives.
Level of risk	The magnitude or combination of risks is expressed in consequences and likelihood.
Likelihood	Chance of something happening.
Monitoring	Continual checking, supervising, critically observing or determining the status to identify change from the performance level required or expected.
Review	The activity was undertaken to determine the subject matter's suitability, adequacy, and effectiveness in achieving established objectives.
Residual risk	Risk remaining after risk treatment.
Risk	The effect of uncertainty on the Ministry's objectives may be positive (opportunity) or negative.
Risk analysis	The process is to comprehend the nature of risk and determine the level of risk.
Risk assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk appetite	The amount of risk the Ministry must take to pursue its objectives.
Risk attitude	The Ministry's approach is to assess and eventually pursue, retain, take, or turn away from risk.
Risk Control	Measures that modify the risk.
Risk criteria	Terms of reference against which the significance of a risk is evaluated.
Risk evaluation	Comparing risk analysis results with risk criteria is used to determine whether the risk and / or its magnitude is acceptable or tolerable.
Risk identification	The process of finding, recognising, and describing risks is as follows:

TERM	DEFINITION
Risk management	Coordinated activities to direct and control the Ministry with regard to risk.
Risk management framework	Set of components that provide the foundation and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the Ministry.
Risk management plan	The risk management framework scheme specifies the approach, the management components, and the resources for risk management.
Risk management policy	Statement of overall intentions and directions of the Cook Island Government related to risk management.
Risk management process	Systematic application of management policies, procedures, and practices to communicate, consult, establish the context, and identify, analyse, evaluate, treat, monitor, and review risk.
Risk owner	Person or entity with the accountability and authority to manage risk.
Risk profile	Description of any set of risks.
Risk source	An element that, alone or in combination, has the intrinsic potential to give rise to a risk.
Risk tolerance	The amount of loss the organisation will bear should a risk materialise.
Risk treatment	The process to modify the risk.
Stakeholder	A person or organisation that can affect or perceive themselves to be affected by a decision or activity.