Risk Management Policy

GOVERNMENT OF THE COOK ISLANDS

Effective: August 2018

Policy Statement

This Policy requires agencies to proactively identify, prevent and mitigate risks, to minimise disruptions and losses, to Agency operations and services.

This Policy should be read together with other policies relating to risk management identified in this document.

Scope

This Policy applies to all Agencies and risk management is the responsibility of all staff.

Key risks identified fall under the following categories:

- Strategic - failure to achieve strategic objectives
- Political - negative impacts from decisions made for political purposes
- Organisational Management – failure of internal Agency infrastructure, staff and resources
- Economic/Financial/Market – negative impacts from the external operating environment
- Legal and Regulatory – exposure to litigation and damages awards
- Climate change or Environmental – negative impacts from natural disasters and failure to protect or preserve the environment
- Technical Risk – failure from technical assets and infrastructure

See Annex 01 for risks listed by category and Annex 02 for the Risk Management Process.

Principles

The Public Service Act 2009 identifies the following values for Public Servants to adhere to:

Honesty	acting honestly, being truthful, and abiding by the laws of the Cook Islands
Impartiality	providing impartial advice, acting without fear or favour and making decisions on their merits
Service	serving the people well through faithful service to the Government of the Cook Islands
Transparency	taking actions and making decisions in an open and transparent manner
Accountability	being able to explain the reason for actions taken and taking responsibility for those actions
Respect	treating the people, the Government of the Cook Islands and colleagues with courtesy and respect
Efficiency and effectiveness	achieving good results for the Cook Islands in an economical way

The duty to act as a good Employer requires employers to ensure the fair and proper treatment of Employees during employment and the provision of good and safe working conditions.

Legislation and Regulations

Public Service Act 2009, Employment Relations Act 2012, Disaster Risk Management Act 2007; Ministry of Finance and Economic Management Act 1995-96; Public Expenditure Review Committee Act 1995-96 and other relevant legislation.

Definitions

Agency means any public service department, instrument, or agent of the Government and includes a body corporate or organisation that is wholly owned or controlled by the Crown

Business Continuity Plan is a plan to ensure the Agency operations can continue after threats become a reality, such as power failure, computer hacking, or an emergency or disaster

Disaster means an actual event of high probable risk, involving serious disruption to the functioning of a community causing widespread human, material, economic or environmental loss, which exceeds the ability of the affected community to cope by using its own resources.

Disaster Recovery Plan is a set of procedures to recover or protect the Agency's infrastructure and assets to enable the restoration of operations after a disaster.

Emergency means an actual or imminent event that endangers or threatens life, property or the environment, and requires a significant coordinated response

Employee means, for the purposes of this Policy, any person who is an employee, contractor, intern or volunteer

Employer means the Public Service Commissioner and Heads of Agencies or their delegated authority

Event means either a disaster or an emergency

Public Service Commissioner means the Public Service Commissioner appointed under Article 73 of the Constitution and Section 5 of the Public Service Act 2009

Risk Management means the identification, analysis, assessment, control and prevention, minimisation or elimination of unacceptable risks

Risk Management Plan is the Agency's plan to foresee and analyse risks, estimate impacts and define responses to issues and should include a Risk Assessment Matrix.

Procedures

Employers are responsible for administering this Policy and ensuring all policies are easily accessible for Employees. Failure to properly administer the Policy reflects poorly on performance. Employees must read, understand and adhere to this Policy. Breaches of the Policy may be considered misconduct and be subject to disciplinary action (see Code of Conduct Policy).

Employer Obligations

Employers are responsible for:

- Establishing and instructing a Risk Management Committee to develop a Risk Management Plan and related plans i.e. business continuity and disaster recovery plans
- Ensuring risks are considered in resource allocation, decision making and corporate governance
- Promoting risk management and approving appropriate training
- Ensuring risk and compliance functions are reflected in employee roles
- Establishing and maintaining partnerships with relevant stakeholders to enhance risk management capacity and implement risk management plans

Risk Management Committee (RMC)

RMC members should have knowledge about risk governance and management, including the risks the Agency faces and strategies or procedures for managing them. Members with knowledge of the Agency operations, activities, processes and risks is an advantage, as well as the time, energy and willingness to serve as active contributors.

They must:

- Identify and analyse the impact of risks on stakeholders of the Agency (Annex 01)
- Prepare the Agency Risk Management Plan
- Prepare budgets for training, risk reduction and mitigation strategies e.g. insurance
- Coordinate staff training in risk management
- Prepare reports for Management in a timely manner
- Review risk management processes periodically and improve processes where appropriate

Manager/Supervisors

Managers/Supervisors are responsible for ensuring a systematic and integrated approach to risk management within each Division. They must:

- Implement the Risk Management Plan
- Identify, analyse, address and report significant risks within the Division
- Ensure that staff understand their responsibilities relating to risk
- Foster a positive risk-awareness culture within the Division
- Provide and/or support staff training in risk related matters

Employee Obligations

Employees must:

- Adhere to Risk Management Plans
- Assist in fostering a positive risk-awareness culture within the Agency
- Assist in identifying risk and report these to appropriate authorities promptly (refer to Disclosure - Whistleblower Policy)

Risk Management Plan

The Risk Management Plan should propose applicable and effective security controls or countermeasures to manage risks. A good Risk Management Plan should also contain a schedule for implementation and responsible persons for those actions.

Risk Management Plans should include

- Risk identification and assessment matrix and records of assessments
- Risk mitigation strategies and persons responsible for certain actions or tasks
- Monitoring and reviewing identified risks in a systematic and timely manner
- Identification of resources for disasters and emergencies
- Emergency evacuation procedures to ensure human safety
- Implementation of the Plan should follow planned actions for mitigating risks
- Identification of risks that can be avoided or accepted (retained)
- Details of insurance policies purchased

Risk Assessment Matrix

The ‘3X3’ matrix enables RMCs to identify and assess relevant risks or threats to the Agency operations and processes according to the likelihood of occurrence and impact if the threat became a reality. Extensive management is required for threats that are high in likelihood and impact. Where there is low likelihood and impact of the threat, the agency may accept the risk.

		Risk Assessment Matrix (3x3)		
Impact (Consequences/severity)	***High*** *(Agency cannot function or mandate needs change*	Considerable management and monitoring *e.g. power failure* or *central IT server breaks down*	Manage, monitor and report to senior management e.g. *central server or computer hacking*	Extensive management *e.g. serious fire/cyclone damage*
	Medium *(Agency can still function)*	Risk can be accepted with monitoring *e.g. delay in budget appropriation*	Manage, mitigate and monitor *e.g. insufficient/inadequate Agency resourcing*	Manage,monitor and report *e.g. unable to deliver Agency outputs*
	Low *(Normal)*	Accept risk Unforeseen contingent liabilities	Accept but monitor *e.g. operational costs continue to increase*	Manage, mitigate and monitor *e.g. Few sittings of Parliament*
		Low *(Normal or unlikely)*	***Medium*** *(Likely)*	***High*** *(Most likely*
		Likelihood (Likelihood/frequency)		

Business Continuity Plan (BCP)

A Business continuity plan includes processes and procedures of the agency that are essential for it to maintain operating during or after a disaster. It enables the agency to re-establish services to a fully functional level as quickly and as smoothly as possible. BCPs should be in place for critical employees, key processes, recovery of vital records, critical suppliers and ensure contact information for staff, vendors and key customers or stakeholders, are maintained.

BCPs comprise:

- Analysis of agency threats
- A list of primary processes and tasks required to ensure the agency operates
- Management contact information that is easy to locate
- Explanations of where employees should go in the case of emergencies or disasters
- Information on data back-ups and agency back up sites
- Collaboration and understanding from management and key employees within the agency

Disaster Recovery Plan (DRP)

As part of business continuity, agencies should have a range of DRPs. These plans are more technical and developed for specific groups or divisions within the agency to recover particular business operations or processes. The most common is the information technology (IT) DRP. IT DRPs would deliver services to the desktops of users, the agency should then have DRPs for other subsequent functions or services to end users.

Disaster Risk Management (DRM)

The national DRM Act provides a framework for government agencies and relevant stakeholders to effectively manage the impacts of disasters and emergencies. The Act establishes the national DRM council to formulate policies for disaster risk management and to endorse the National DRM Plan along with all sub-plans (refer to Annex 3). The council advises Cabinet on DRM matters and reviews the performance of stakeholders in implementing their roles and responsibilities under the National DRM Plan.

The DRM Act also establishes Emergency Management Cook Islands (EMCI) as the entity responsible for putting procedures in place for disaster risk reduction, mitigation, preparedness, response and recovery. EMCI is the secretariat and implementing arm of the national DRM council.

It is the responsibility of all government agencies to ensure they are aware of their roles and accountabilities identified in the national DRM plan. Lead agencies identified in the national DRM plan are responsible for developing DRM plans for specific hazards listed in the national plan. DRM plans should be included in the agencies overall risk management plan.

Review and Evaluation of the Plan

Initial risk management plans will never be perfect. Practice, experience, and actual loss results may necessitate changes or inform changes to the plan. Risk management plans should be updated periodically. Two primary reasons for this are:

1. To evaluate whether the reduction or mitigation strategies are still applicable and effective
2. To evaluate possible risk level changes in the agency operations or business environment

Monitoring the effectiveness of controls and risk at all stages of the risk management process is good practice (see Annex 02).

Other Provisions

All documentation relating to the risk management process and plan must be retained for audit purposes.

All records must be kept for at least seven years and only accessible by the employer and/or authorised staff. After the seven year period, the agency may destroy or archive the documentation in adherence with government official information management policies.

The Office of the Public Service Commissioner is responsible for reviewing and updating this policy and associated documents annually.

Associated Documents

Occupational Health and Safety Policy
Disclosure (Whistleblower) Policy
Code of Conduct Policy
Business Continuity Plan
Disaster Recovery Plan(s)

Other information

For policy queries contact the Office of the Public Service Commissioner on phone (682) 29421 or email: pscinfo@cookislands.gov.ck

Annex 01: Categories of Risk

This annex provides various examples of risk to assist in identifying relevant risks for the agency and mitigation strategies. They can be used as a guide to inform risk checklists for agencies.

Strategic Risk – Major Threats

Sources of threat that may give rise to significant strategic risk include:

- Budgeting (availability or allocation of resources)
- Partnerships failing to deliver desired outcomes
- Failure to invest appropriately
- Insufficient capital investment or shortfall in revenue expected / planned
- Failure to develop capability for research, and innovation (exploit opportunities)
- Failure to respond to a national or significant disasters
- Inadequate insurance/contingency provision for disasters such as fire, floods etc.
- Failure to manage national pandemics
- Failure to prevent civil action by employees/public servants
- Failure to prevent civil action by the public
- Failure to invest in new and relevant technology to achieve objectives
- Failure of suppliers to meet contractual commitments (quality, quantity, timelines etc.)

Political and market factors (for management of risk, security etc.) Political

- Change of government
- Change in government policies
- Adverse public opinion from government policies or decisions
- Failure to mitigate negative media messaging
- Political interference

Economic/Financial/Market

- 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

- 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)
- Failure to comply with legal, regulatory or contractual obligations
- Failure to enforce legal, regulatory or contractual obligations

Organisational Management

Leadership and Direction

- Management incompetence or poor leadership
- Under performing 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 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
- Failure to plan for workforce training needs
- Failure to manage employment disputes or misconduct

Financial and Resource Management

- Unethical practices and transactions
- Poor asset management
- 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
- Inadequate infrastructure to provide quality services
- Individual or group interests given unwarranted priority
- Absence of quality assurance measures in service provision
- Absence of strategic communication between Ministers and agency heads
- Absence of agency communication plan
- Lack of collaboration with stakeholders on strategy and service delivery

Climate Change or Environmental

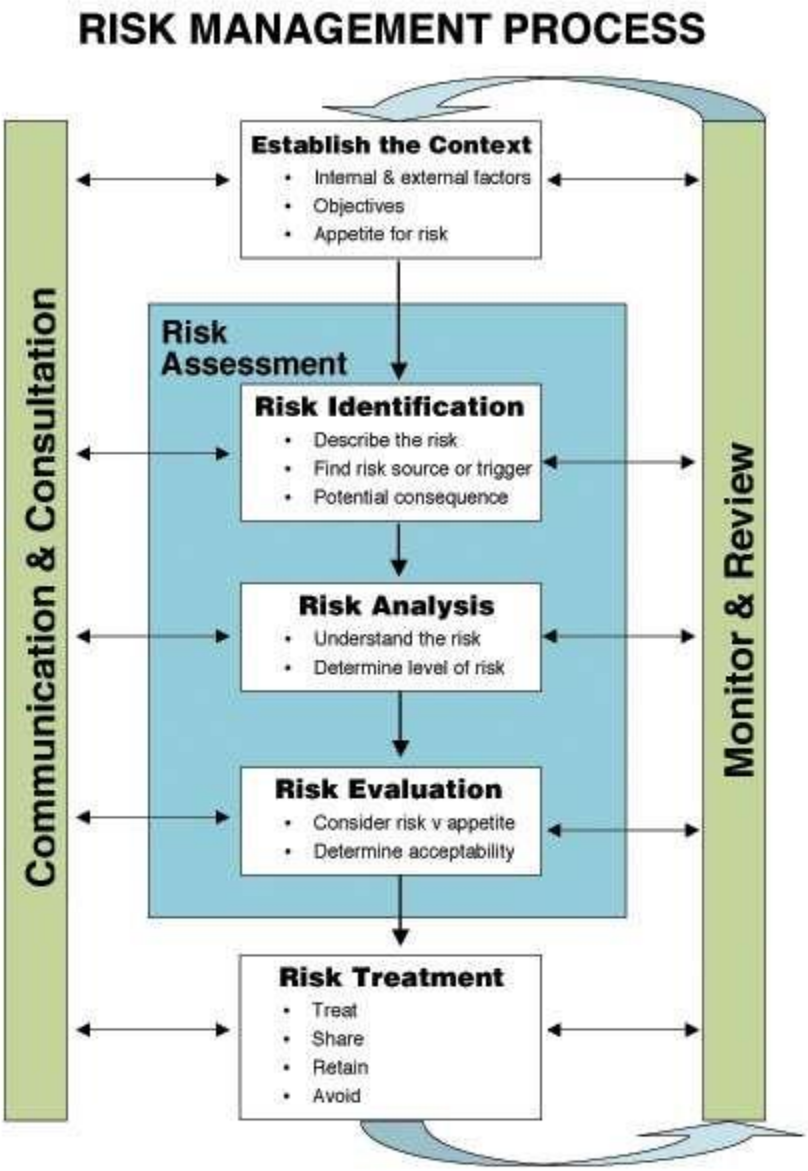
- Natural disasters e.g. cyclones and flooding
- Manmade hazards/disasters e.g. fires
- Lack of environmental awareness practices (Reduce, reuse, recycle)

Technology, Equipment & Systems

- Inadequate ICT equipment
- Poorly resourced ICT systems support
- Centralised network failure

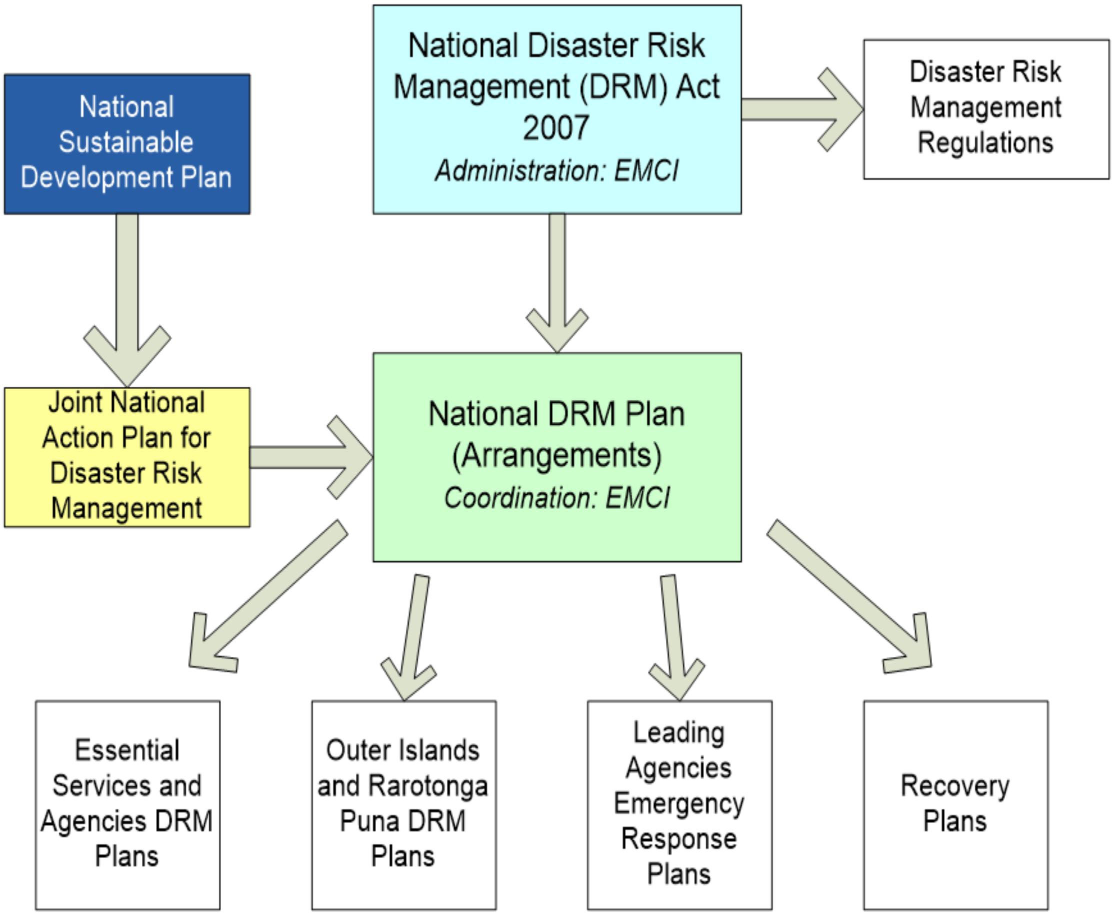
Annex 02: Risk Management Process

A risk management committee (RMC) must be established to develop and oversee implementation of the agency risk management plan. The RMC should comprise senior managers/employees who have a strong understanding of the agency operations and processes.



Source: http://www.education.vic.gov.au/school/principals/spag/governance/pages/risk.aspx

Annex 03: Disaster Risk Management Framework


National Sustainable Development Plan
National Disaster Risk Management (DRM) Act 2007
Administration: EMCI
Disaster Risk Management Regulations
Joint National Action Plan for Disaster Risk Management
National DRM Plan (Arrangements)
Coordination: EMCI
Essential Services and Agencies DRM Plans
Outer Islands and Rarotonga Puna DRM Plans
Leading Agencies Emergency Response Plans
Recovery Plans