



WASAARADDA TAMARTA IYO

KHEEYRAAD KA BIYAHA GALAMUDUG

MINISTRY OF ENERGY AND WATERT

RESOURCES

GALMUDUG-STATE SOMALIA

**RISK MANAGEMENT/REGISTER MATRIX
POLICY AND PROCEDURE**

FEBRUARY, 2022

Contents

RISK MANAGEMENT/REGISTER MATRIX POLICY AND PROCEDURE	1
1.0 Introduction	3
1.1. Purpose of the Policy	3
2.0 Understanding Risk Management	3
2.1. Definitions	4
3.0 Responsibility	5
3.1 Director General.....	5
3.2 Policy & Planning Director	5
3.3 Risk Owner	6
3.4 General responsibilities	6
4.0 Risk Management Procedure.....	6
4.1: Summary of procedure	6
4.2. Risk Management Process	7
5.0 Risk Management Methodology	8
Appendix A – Risk Assessment Matrix and Risk Register	9
Risk Assessment Matrix	10
RISK REGISTER	11
6. ASSOCIATED PROCEDURES & GUIDELINES	12
7. REVIEW OF THIS POLICY	12

1.0 Introduction

The Ministry top management will have a systematic approach to the management of risk in all of its functions and services. As part of this approach, the Minister and DG expects employees to give greater priority to managing and reducing risks associated with the safety of people, the experience of people who receive care, and the delivery of effective care.

There is a comprehensive risk management system in place to identify, assess, manage and monitor risk at all levels of the Ministry.

There is appropriate ownership of risk in the Ministry, and that there is an effective culture of risk management. Whatever you may be trying to achieve there will always be some risk. Risk creates uncertainty, and if we do not actively manage risk, could lead to us not achieving our goals and objectives, such as safe and effective care. To increase our chances of success, we should:

- Be very clear what we are trying to achieve, and purposely set out the objectives.
- Identify the risks to those objectives. Risks should always be related to objectives, as this allows us to properly assess them and consider how important they are in terms of their threat to success.
- Put in place measures and take appropriate action to manage the risks. This Risk Management Policy has been produced to embed a consistent approach to risk management across the Ministry of Energy and Water Resources Galmudug.

1.1. Purpose of the Policy

All activities undertaken by Ministry of Energy and Water Resources Galmudug (MoEWR) carry an element of risk. The exposure to these risks is managed through the practice of Risk Management. In managing risk, it is the Ministry's practice to take advantage of potential opportunities while managing potential adverse effects. Managing risk is the responsibility of everyone in the Ministry. This policy outlines the Ministry's risk management process and sets out the responsibilities of the staff, the Audit and Risk Committee, the Managing Director, senior management and others within the Ministry in relation to risk management.

2.0 Understanding Risk Management

Risks have been described in terms of combination of the consequences of an event occurring and its likelihood of occurring. Risk is the chance of something happening that will have an impact on objectives and risk management can be described as the culture, processes and structures that are directed towards realizing potential opportunities whilst managing an adverse effect.

MoEWR's risk management system is designed to identify the risks it faces and has measures in place to keep those risks to an acceptable minimum. The existence of risk presents both threats and opportunities to Ministry.

Risk owners have been assigned responsibility for the identified risks in the Risk Register. Ministry's risk assessment matrix is used as the benchmark in planning and implementing the risk management measures. It takes into consideration the nature, scale and complexity of the business. The risk management process consists of the following main elements:

Identify: identify a risk (threats or opportunities) and document the risks captured by the risk register owner.

Assess: the primary goal is to document the net effect of all identified threats and opportunities, by assessing:

- Likelihood of threats and opportunities (risks);
 - Impact of each risk;
 - Proximity of threats; and
 - Prioritization based on scales.

Plan: preparation of management responses to mitigate threats and maximize opportunities.

Implement: risk responses are actioned.

Monitor and review: monitor and review the performance of the risk management system and changes to business initiatives.

Communicate: provide regular reports to management team / Audit and Risk Committee at agreed times

Risks are effectively managed by ministry through the effective implementation of various controls, which include:

- Approved risk management framework;
- Documented policies and procedures;
- Maintenance of registers;
- Implementation of risk based systems and processes;
- Ongoing monitoring of regulatory obligations;
- Checklists to guide activities and project plans to record actions; and
- Internal and external reporting.

2.1. Definitions

Risk is uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. It is the combination of the likelihood and impact of the risk materializing.

Risk should always be related to some objective or purpose. A statement of risk should always contain:

1. The cause of the impact on the objective, AND
2. The impact on the objective (i.e. the consequence of the risk)

Risk Management is a process which helps the whole Ministry to identify areas that require attention and remedial action. It can be defined as the processes involved in managing those risks, including:

- Identifying
- assessing and judging risks
- assigning ownership for the management of the risk
- taking actions to mitigate or anticipate them
- monitoring and review progress

The risk register is a record of the risks identified, the assessment of them, the controls in place to manage them and any additional actions planned to improve controls to manage them. There should be risk registers at all levels of the Ministry.

An internal control is measure put in place with the aim to mitigate risk. Internal controls will constrain risks but are unlikely to eliminate them entirely and every control will come at some type of cost.

Inherent risk can be defined as the exposure arising from a specific risk before any action is taken to manage it i.e. there are no controls in place

Residual risk - the exposure arising from a specific risk after action has been taken to manage it and making the assumption that the action is effective i.e. controls are in place and are operated as intended

Risk escalation is the process of communicating a risk across up, down or across the Ministry to ensure that is managed effectively

Risk tolerance – the boundaries of risks judged to be justifiable and which the Ministry is prepared to accept or be exposed to at any point in time. This will typically be expressed in quantifiable measures that will be monitored.

3.0 Responsibility

3.1 Director General

The Dg of the Ministry, has responsibility under its Charter to review and report to the Ministry that:

- The Dg is the Accountable person for Ministry, and as such is legally responsible for ensuring that risks are identified, that their significance is assessed and that systems appropriate to the risks are in place in all relevant areas to manage them.
- The Dg has, at least annually, reviewed the MoEWR's risk management framework to satisfy itself that it continues to be sound and that MoEWR is operating with due regard to the risk appetite set by the Ministry, and effectively identifies all areas of potential risk;
- Adequate policies and processes have been designed and implemented to manage identified risks;
- A regular program of audits is undertaken to test the adequacy of and compliance with prescribed policies; and
- Proper remedial action is undertaken to redress areas of weakness.

3.2 Policy & Planning Director

The Policy & Planning Director of ministry has responsibility under this policy for:

- Monitoring compliance with this policy;
- Reporting to the Minister, and DG on compliance with this policy;
- Developing, implementing and monitoring systems, management of policies and procedures relevant to the business, including facilitating review by the executive on a regular basis; and
- Maintaining the risk register.

3.3 Risk Owner

The risk owner (as noted in the Risk Register) is responsible for ensuring on a daily basis that the relevant operational procedures and controls implemented to treat each risk area are adequate and effective. If a control or procedure is not adequate and effective in treating the risk, the risk owner should report this, with a recommendation for an alternative risk treatment, to the Financial director for escalation to the Director general and ultimately approval by the minister.

3.4 General responsibilities

Every Ministry staff members is responsible for effective management of risk including the identification of potential risks. Management is responsible for the development of risk mitigation plans and the implementation of risk reduction strategies. Risk management processes should be integrated with other planning processes and management activities.

Where there is legislation in place for the management of specific risks (such as Occupational Health and Safety) this Risk Management policy does not relieve ministry of its responsibility to comply with that legislation.

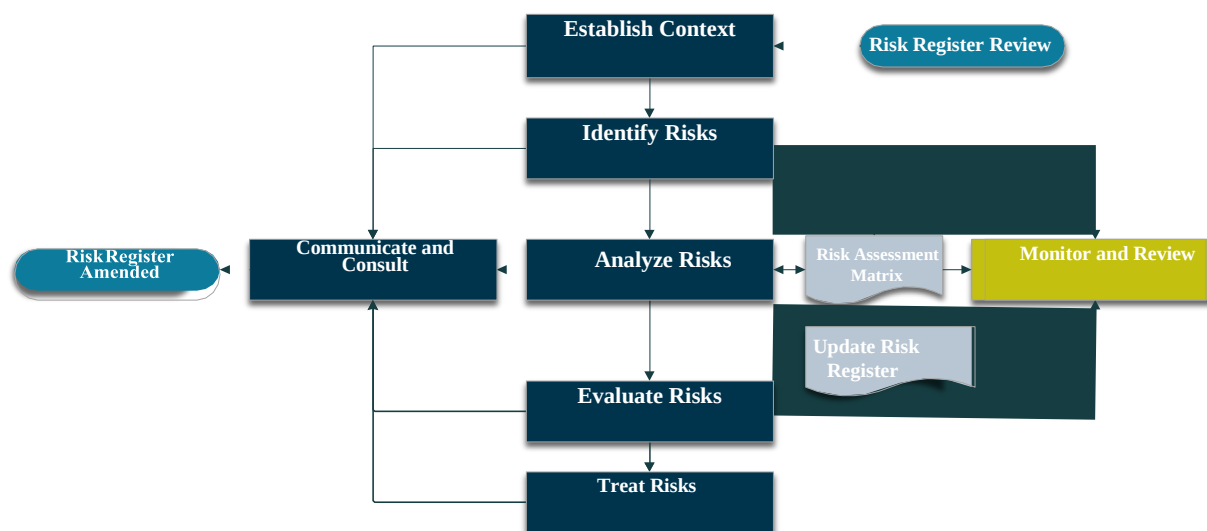
Top officials including first and deputy ministers are accountable for strategic risk management within areas under their control, including the promotion and training of the risk management process to staff.

All staff are responsible for:

- continually considering the potential risks
- identifying risks
- taking quick and appropriate action to escalate any risk they have identified

4.0 Risk Management Procedure

4.1: Summary of procedure



4.2. Risk Management Process

The risk management system is dynamic and is designed to adapt to MINISTRY 's developments and any changes in the risk profile over time. Compliance measures are used as a tool to address identified risks.

The risk management system is based on a structured and systemic process which takes into account ministry 's internal and external risks.

The main elements of the risk management process are as follows:

- **Communicate and consult** – communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole.
- **Establish the context** – establish the external, internal and risk management context in which the rest of the process will take place – the criteria against which risk will be evaluated should be established and the structure of the analysis defined.
- **Identify risks** – identify where, when, why and how events could prevent, degrade, delay or enhance the achievement of ministry 's objectives.
- **Record risks** – document the risks that have been identified in the risk register.
- **Analyze risks** – identify and evaluate existing controls. Determine consequences and likelihood and hence the level of risk by analyzing the range of potential consequences and how these could occur.
- **Evaluate risks** – compare estimated levels of risk against the pre-established criteria and consider the balance between potential benefits and adverse outcomes. This enables decisions to be made about the extent and nature of treatments required and about priorities.
- **Treat risks** – develop and implement specific cost-effective strategies and action plans for increasing potential benefits and reducing potential costs.
- **Monitor and review** – it is necessary to monitor the effectiveness of all steps of the risk management process. This is important for continuous improvement. Risks and effectiveness of treatment measures need to be monitored so that changing circumstances do not alter priorities.

MoEWR's risks may come from any internal or external event which, if it occurs, may affect the ability to efficiently and effectively operate:

- **Internal risks** – those risks that specifically relate to MINISTRY 's business itself and as such as generally within its control. They include risks such as employee related risks, including conduct related risks, strategic risks, and financial risks.
- **External risks** – those risks that are outside the control of ministry. They include risks

such as market conditions, digital disruption, cyber-security, privacy and data breaches, sustainability, climate change and legislative change.

5.0 Risk Management Methodology

The methodology adopted by Ministry for managing and treating its risks can be defined as follows:

1. Document a risk management framework (ie the context)
2. Identify the general activities involved in running the business (ie risk categories)
3. Identify the risks involved in undertaking the specific activity by asking the questions:
 - a) What could happen
 - b) How and why could it happen?
4. Rate the likelihood of the business activity not being properly performed. Likelihood is assessed to the assumption that there are no existing risk management and compliance processes in place. It is assessed as either **Almost Certain, Likely, Possible, Unlikely** and **Rare**.
5. Rate the consequence of not properly performing the business activity - damage can be quantified in terms of financial loss to investors and/or Ministry itself. It is assessed as **Catastrophic, Major, Severe, Serious** and **Minor**.
6. Assign the inherent risk rating based on a combination of the risk rating. Low and medium risks may be considered acceptable and therefore minimal further work on these risks may be required. The rating may be assessed as **Critical, High, Significant, Medium** and **Low**.
7. Decide whether a control (e.g policy, procedure, checklist, reporting mechanism or account reconciliation) is necessary given the level of risk, based on likelihood and consequences and if so, identify control.
8. Assess whether the existing controls are adequate and allocate the responsibility of monitoring the control to treat the risk. This will integrate risk management and compliance to daily activities and facilitate appropriate control of operational risk.
9. Raise awareness about managing risks across the Ministry through communicating the policy and responsibilities.
10. Routinely monitor and review ongoing risks so can risk can be effectively managed

The Risk Assessment Matrix and Risk Register format are shown in Appendix A.

Appendix A – Risk Assessment Matrix and Risk Register

Risk Consequence Severity

Consequence Type	Minor	Serious	Severe	Major	Catastrophic
Financial Loss	< \$1m	\$1m-5m	\$5m-\$10m	>\$10m	Threatens viability of Ministry
Reputation Loss					

Likelihood Probability & Frequency

Likelihood Rating	Description	Probability
Almost Certain	Known to happen often	> 95%
Likely	Could easily happen	50% - 95%
Possible	Could happen & has occurred before	15% - 50%
Unlikely	Hasn't happened yet but could	5% - 15%
Rare	Conceivable, but only in extreme circumstances	> 5%

Control Effectiveness

Control Effectiveness	Description
Effective	The control design meets the control objective and the control is operating the majority of the time
Partially Effective	The control design mostly meets the control objective and/or the control is normally operational but occasionally is not applied when it should be, or not as intended
Ineffective	The control design does not meet the control objective and/or the control is not applied or is applied

Risk Assessment Matrix

LIKELIHOOD	Likelihood Rating	Minor	Serious	Severe	Major	Catastrophic
	5. Almost Certain	Medium	High	Critical	Critical	Critical
	4. Likely	Medium	Significant	High	Critical	Critical
	3. Possible	Medium	Medium	Significant	High	Critical
	2. Unlikely	Low	Low	Medium	Significant	Critical
	1. Rare	Low	Low	Medium	Medium	High
	CONSEQUENCE					
Critical	Extreme risk - detailed research and management planning required at senior levels					
High	High risk- immediate senior management attention needed					
Significant	Significant risk - Senior management attention needed					
Medium	Moderate risk - Management responsibility must be specified					
Low	Low risk - Manage by routine procedures					

RISK REGISTER

No	Risk	Owner	Consequence	Likelihood	Inherent Risk Level	Controls	Control Effectiveness
	Risk Area						
1.	Risk name and description						
2.							
3.							
4.							

6. Associated Procedures & Guidelines

Implementation of this policy is predominantly achieved by recording the risk management information in the Ministry risk register. Following MoEWR policies, procedures, guidance and systems on all matters is in itself a 'key' to controlling risk. All Galmudug Ministry policies, procedures, guidance and systems are designed to achieve the aims and objectives of the subject matter. This Risk Management Policy and its associated procedures should assist in managing the risks that arise from these activities. Details of the processes are set out in the Risk Management procedure and supporting guidance documents.

7. Review of This Policy

The policy and planning director and risk matrix committee will continually keep this policy under review with a formal review every 4 years.