

---

# RISK MANAGEMENT FRAMEWORK

---

REGISTRAR GENERAL'S DEPARTMENT



JANUARY 22, 2024

# Contents

Topics	Page No.
Preface	2
Interpretation	3
Introduction	5
Risk Management	8
The Approach to Managing Risks	8
Accountability, Roles and Responsibilities	9
Risk Management Process- Overview	13
Risk Management Process- Methodology	14
Evaluation of Risk Management Effectiveness	19
Review of the Framework	20
Appendices:	
1.0 Risk Management Policy	21
2.0 Risk Management Plan	23
3.0 Risk Identification Process	24
4.0 Risk Analysis and Evaluation Process	31
5.0 Risk Response	34
6.0 Risk Assessment Table	35
7.0 Risk Register	37

## Preface

This Framework has been developed in response to the requirements for the establishment of formal risks management structures.

Risk management is a fundamental element of corporate governance. Risk is associated with possible events which, should they occur, could prevent the **Registrar General's Department** from fulfilling its mission, meeting its commitments and achieving its objectives. Risks may adversely affect the **Department's** strategy, people, assets, environment or reputation.

A structured and systematic approach to managing risks and opportunities is more effective and efficient as it:

- defines a process for systematically managing the risk of all activities and units in the **Registrar General's Department**;
- encourages a high standard of accountability at all levels;
- supports effective governance systems and reporting mechanisms;
- encourages a high standard of efficient and effective service delivery by taking advantage of opportunities for improvement; and
- allows the **Department** to better meet its stakeholders needs and demands.

It is everyone's responsibility to be involved in the identification, evaluation and treatment of risks and opportunities that could impact or influence outcomes for the **Department**.

## Interpretation

In this Framework,

**“Audit Committee”** is an integral element of public accountability and governance and plays a key role in assisting Ministries/Departments in their legal and fiduciary responsibilities, especially with respect to the integrity of the Government’s financial information and the adequacy and effectiveness of the internal control system.

**“Likelihood”** is the chances of something happening.

**“Impact”** is the outcome of an event affecting objectives. .

**“Operational Risk”** is risk of loss or gain resulting from inadequate or failed internal processes, people and systems or from external events.

**“Inherent Risk”** is the exposure arising from risk factors in the absence of deliberate management intervention(s) to exercise control over such factors.

**“Residual Risk”** is the remaining risk after Management has put in place measures to control the inherent risk.

**“Risk”** means an unwanted outcome, actual or potential, to the institution’s service delivery and other performance objectives, caused by the presence of risk factor(s). Some risk factor(s) also present upside potential, which Management must be aware of and be prepared to exploit. This definition of “risk” also encompasses such opportunities.

**“Risk Appetite”** is the amount of residual risk that the Min/Dept. is willing to accept.

**“Risk Factor”** is any threat or event which create, or has the potential to create risk.

**“Risk Owner”** is a person with the accountability and authority to manage the risk.

**“Risk Register”** is a record of information about identified risk.

**“Risk Assessment”** is the overall process of risk identification, risk analysis and risk evaluation.

**“Internal Auditing”** is to objectively and systematically evaluate the effectiveness of risk management, control and governance processes, provide assurance on the efficient use and management of resources within the Ministry/Department. This function is carried out by the Internal Control Cadre

**“Project Risk”** is risk relating to delivery of a service or change or product, usually within the constraints of Time Cost and Quality.

**“Strategic risk”** is risk concerned with where the Ministry/ Department wants to go, how it plans to get there and how it can ensure survival.

## Abbreviations

**AO- Accounting Officer**

**P.S- Permanent Secretary**

**SCE- Senior Chief Executive**

**OIC- Officer in Charge.**

**AC- Audit Committee**

**RMC- Risk Management Committee**

# The Risk Management Framework

Registrar General's Department			
Approved by	Approval Date	Effective date	Next Review
Registrar General	22 January 2024	24 January 2024	22 January 2025
<b>Purpose</b>	The Risk Management Framework provides the foundation and organizational arrangement for designing, implementing, monitoring, reviewing and continually improving risk management throughout the Department.		
<b>Scope</b>	The Framework applies to the Department, including all its Units/Sections/Functions.		
*AO: Director, Commissioner, or officers in other grades who are Accounting Officers.			

## 1.0 Introduction

This Risk Management Framework provides the policies, procedures, organizational arrangements and the tools that will embed risk management throughout the **Registrar General's Department**. at all levels. The Framework;

- outlines the *Department's* risk management plan (**Appendix 2.0**);
- defines the roles and responsibilities for risk management within the **Department**;
- provides guidance on the risk management process; and
- explains the risk management recording and reporting requirements within the **Department**.

The risk management framework has been developed in line with the;

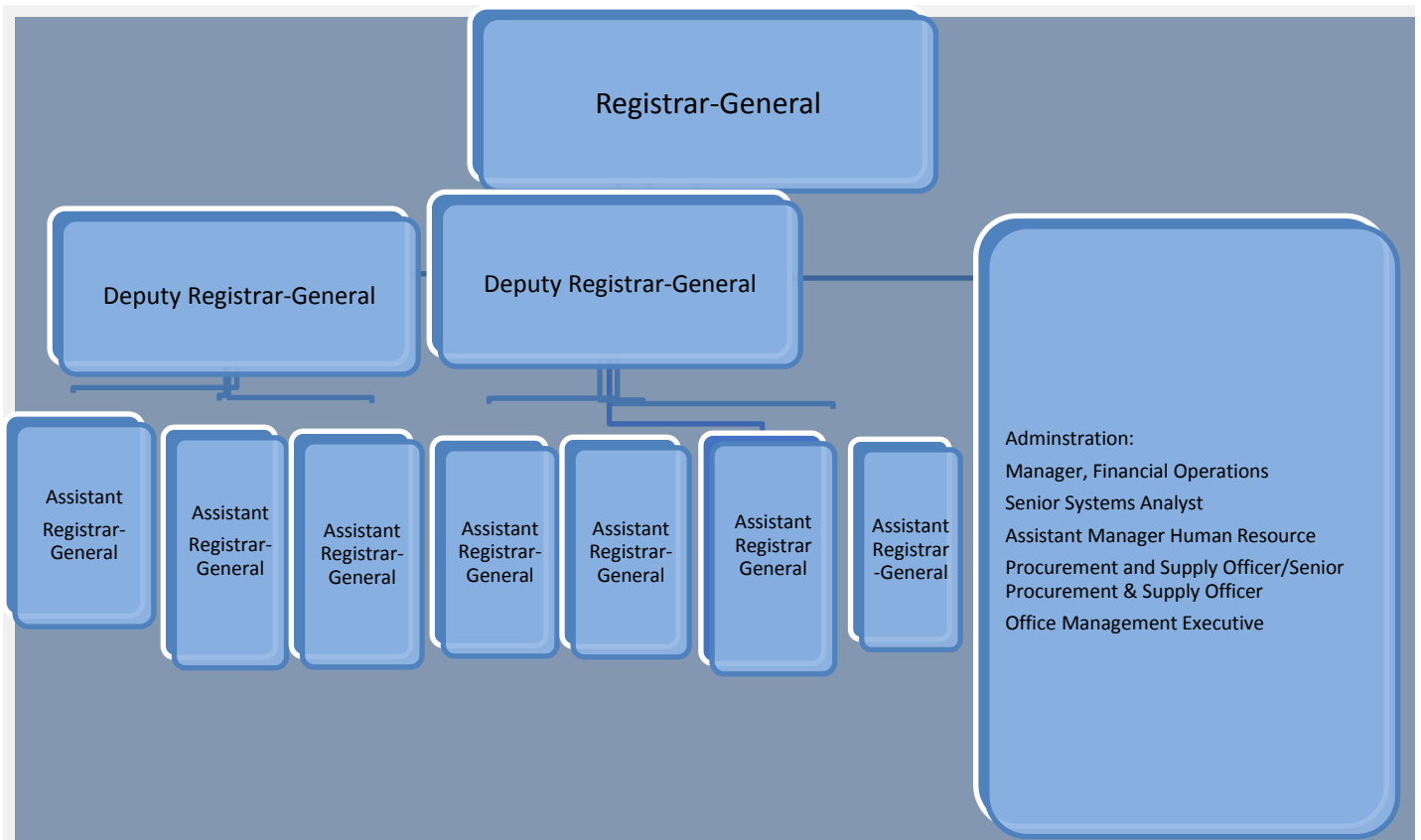
- I. **Circular No 8 of 2021 – Guidelines for the establishment of Risk Management in the Public Sector** which is based on the essence of the '*ISO 31000- Risk Management*' and best international practices; and
- II. **The *Department's* Risk Management Policy**

The Risk Management Policy confirms the **Department's** commitment to identify, assess and manage risks which may prevent the achievement of strategic goals and objectives. The policy directs that the **Department** will integrate risk management into its culture, decision-making processes,

programs, practices, business planning and performance reporting activities. The Department's Risk Management Policy is at **Appendix 1.0**. The Risk Management Policy is applicable to the whole Department as per Organizational Structure.

## ORGANISATIONAL STRUCTURE

### SENIOR MANAGEMENT TEAM



**Figure 1: Top Management at RGD**

## *Organisational Structure of the department*

<b>Ministry</b>	<b>Department</b>	<b>Sections</b>	<b>Units</b>	<b>Address</b>
Finance, Economic Planning and Development	Registrar-General's Department	Management	Management	6 <sup>th</sup> Floor, Emmanuel Anquetil Building,  Port Louis
			RG Secretariat	
		Taxing Professional	Taxing	
			Confirmation Unit	
			Help Desk/ Submission	
		Taxing Public	Taxing	
		Mortgage	Data Capture/ Verification	
			Erasure	
		Valuation	Reassessment	
			Objection Unit	
		Certified Copy Section		
		Finance	Revenue & Expenditure	
			Cashier's Office	
		HR Section		
		Procurement & Supply		
Office Accommodation & Transport				
IT Section				
Registry				
	Quality Assurance Unit			

**Figure 2: Sections and Units at RGD**



## 2.0 Risk Management

Risk Management is a process made up of activities and actions taken to ensure that an organisation is conscious of risk it faces, make coordinated and informed decisions in managing those risk and identifies potential opportunities. Risk management is about managing threats and opportunities.

Risk Management essentially means answering six basics questions

1. What are we trying to achieve?
2. What might affect us in what we are trying to achieve?
3. Which of those things which have been identified might affect us are the most important?
4. What should we do?
5. Did it work?
6. What changed?

## 3.0 The approach to Managing Risks

In order to ensure an effective Risk Management that will create and protect value, the **Department** will:

- Integrate Risk Management at Strategic, Operation and Project levels;
- Customise the Risk Management to suit its requirement;
- Use the best available information to conduct the Risk Management;
- Consider Cultural and Human factors when developing and implementing risk management; .
- Adopt a Structured, and omprehensive approach to risk management to ensure consistency and comparability of results;
- Be Inclusive, that is, will involve in a timely manner revelant stakeholders and will consider their knowledge, views and perceptions;
- Ensure a Dynamic that will respond, in a timely manner, to the changing environment; and
- Continually improve the process through learning and experience.

## 4.0 Accountability, Roles and Responsibilities

Risk Management is the responsibility of everyone at the **Department**. Accountability refers to the ultimate responsibility for actions, decisions, and management pertaining to the nominated activity. The roles and responsibilities of each stakeholders in managing risks are defined in the table below.

### SCE/PS/AO of Departments

**The Registrar General of the Department is accountable for the overall governance of risk. His roles and responsibilities include inter-alia:**

- (a) *setting an environment for effective management of risk;*
- (b) *allocation of appropriate resources for risk management, including capacity building;*
- (c) *ensuring that risk management is integrated in day-to-day activities;*
- (d) *responsible for setting up of the appropriate internal structure and processes for risk management;*
- (e) *designating relevant officials with the responsibility for developing and reviewing the Risk Management Framework;*
- (f) *holding internal structures accountable for performance in terms of their responsibilities for risk management;*
- (g) *approving the risk management policy, framework and implementation strategy plan;*
- (h) *approving the **Department's** risk appetite and risk tolerance; and*
- (i) *Reporting/Disclose on matters on risk management in the Annual Report of the **Min/Dept.***

### Risk Management Committee

(Committee set by the Accounting Officer for implementing & Monitoring of Risk Management)

**A Risk Management Committee has been set up at the Department level for the implementation and monitoring of Risk Management. The Committee comprises of the following officers:**

	<b>Name</b>	<b>Grade</b>	<b>Roles</b>
1	HURRYNAG Deoyani (Mrs)	Registrar General	Chairperson
2	GUKHOOL Sadmadevi (Mrs)	Deputy Registrar-General	Member
3	SEEWOO Tookraj	Deputy Registrar-General	Member
4.	RAMRECHA Lutchmeenarain,	Assistant Registrar-General	Member
5.	SOODHOO Aruna Devi (Mrs)	Assistant Registrar-General	Member
6.	BENNY Janéswaree (Mrs) ,	Assistant Registrar-General	Member
7.	FAKUN Yogeeta (Mrs)	Assistant Registrar-General	Member
8.	GHOOLET Rakesh	Assistant Registrar-General	Member
9.	BHUNJUN Parmanand	Assistant Registrar-General	Member
10.	NARAN Jayalakshmi (Mrs)	Senior Systems Analyst	Member

11.	KHODABUX Bibi Oummeh Salmah Mahmoud (Mrs)	Manager, Financial Operations	Member
12.	LANGUR Bhanoodutt	Assistant Manager, Internal Control	Member
13.	RAMSAHA Sharmila (Miss)	Assistant Manager, Human Resources	Member
14.	BHOYROO Beekash	Procurement and Supply Officer/Senior Procurement and Supply Officer	Member
15.	POOMUN Sowkatally	Office Management Executive	Member
16.	MUNBOD Goroodev,	Office Management Executive	Member
17.	VENDEN Backtee (Mrs)	Inscription and Check Clerk	Member
18.	BEEHARRY Mukesh	Office Management Assistant	Secretary

In addition to the above, any other officer may form part of the team as may be decided by the [Registrar General](#). The roles and responsibilities of the Risk Committee include:

- (a) To prepare a risk management Implementation Strategy & Plan.
- (b) To prepare and circularise the Policy Statement and the Risk Management Framework in line with **Circular No. 8 of 2021 (MOFEPD)** and review same as per time frame set.
- (c) Identify capacity building needs and arrange for same.
- (d) To provide the necessary brainstorming session with Risk Owners.
- (e) To consolidate the Central Risk Register for the **Department**..
- (f) To report to Audit Committee and the SCE/PS/AO the outcome of the consolidation and any matter on Risk Management.
- (g) To coordinate, monitor and review the risk management process on a regular basis.
- (h) Provide risk-related advice and review and challenge risk information / decisions.

## **Risk Owners**

**Officers, identified as Risk Owners as per paragraph 4.1, will have the following roles and responsibilities:**

- (a) Brainstorm with all staff on Risk Management.
- (b) Identify the risk controls and ratings as part of the risk assessment process.
- (c) Document all risks, risk assessment, control in place, risk rating and prepare a Risk Register as per pro-format provided.
- (d) Record and monitor implementation of related actions to manage risks in alignment with the requirements of the Framework.
- (e) Communicate and escalate risks to relevant stakeholders.
- (f) Review all risks on a yearly basis.

**Hand-over updated risk register to incoming responsible official.**

## Other Staff

**Staff posted in the different Units/Sections or Departments will have the following responsibilities:**

- (a) *To participate in brainstorming exercise on Risk Management.*
- (b) *To provide support to Risk Owners in managing risk and engage in constructive risk mitigations.*
- (c) *To inform Risk Owners if coming across new or emerging risks during the year.*

## Audit Committee

**The Audit Committee will be responsible to, inter-alia:**

- (a) *To review and recommend for the approval of the Accounting Officer on the Risk Management Framework.*
- (b) *To review and recommend disclosures on matters of risk in the annual financial statements and risk management in the annual report.*
- (c) *To provide regular feedback to the Accounting Officer on the adequacy and effectiveness of risk management in the **Department**, including recommendations for improvement;*
- (d) *To ensure that the internal audit plans are aligned to the risk profile of the Min/Dept./Department to address the following areas:*
  - (i) *financial reporting risks, including the risk of fraud;*
  - (ii) *internal financial controls; and*
  - (iii) *IT risks as they relate to financial reporting.*

## Internal Audit

**The roles of the Internal Audit in risk management are:**

- (a) *To provide an independent, objective assurance on the effectiveness of the Department's system of risk management.*
- (b) *To evaluate the effectiveness of the entire system of risk management and provide recommendations for improvement where necessary.*
- (c) *To develop its internal audit plan on the basis of the key risk areas of the Department.*
- (d) *To ascertain that the risk management processes put in place in the Department cover the following:*
  - *The Department's objectives and mission are aligned;*
  - *significant risks are identified and assessed;*
  - *risk responses are appropriate to limit risk to an acceptable level; and*
  - *relevant risk information is captured and communicated in a timely manner to enable Accounting Officers to carry out their responsibilities.*

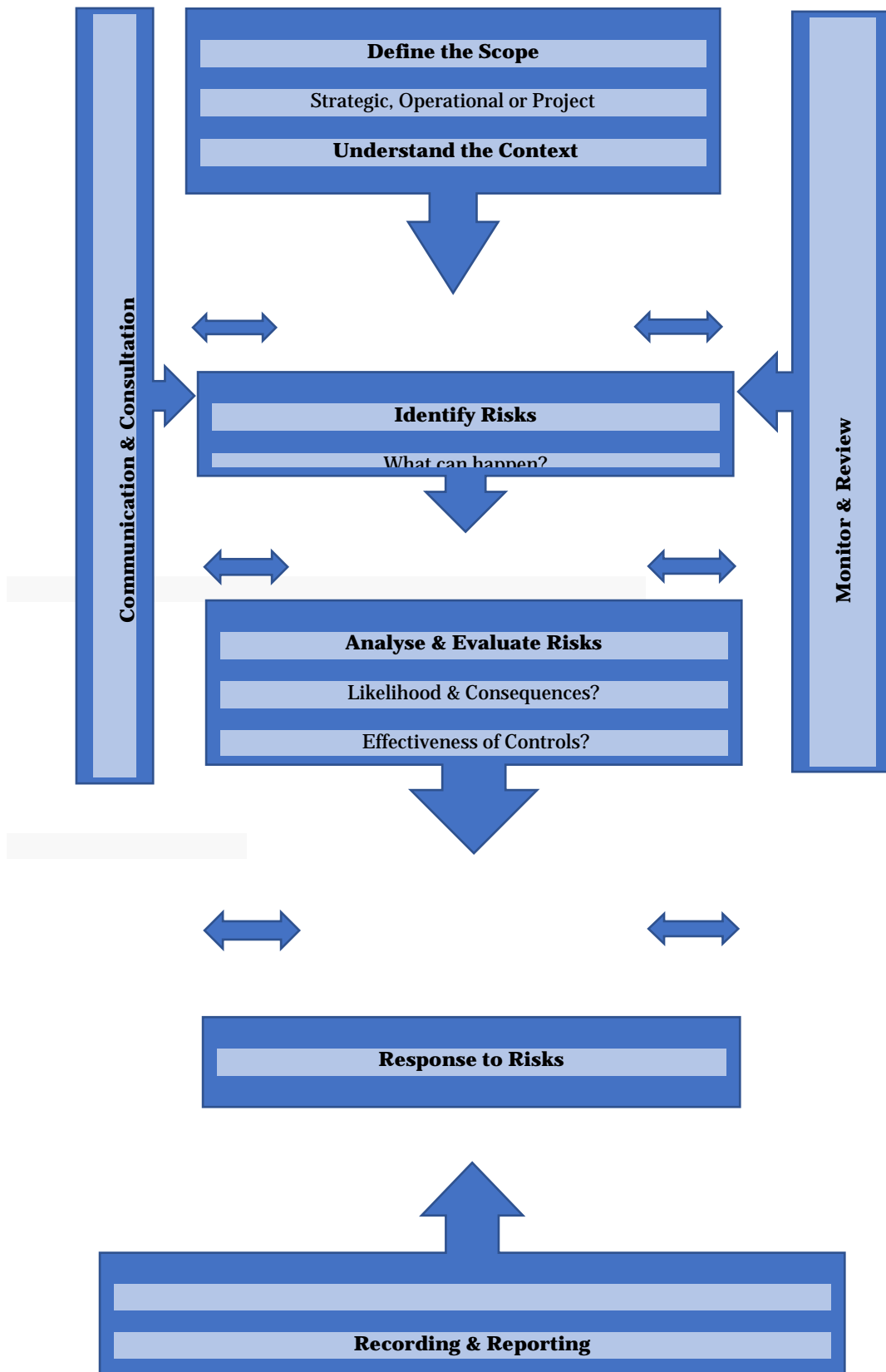
#### 4.1 Risk Owners

The following officers have been identified as Risk Owners:

SN	Divisions/ Units/ Sections/ Functions	Risk Owners
1	Management	HURRYNAG Deoyani (Mrs), Registrar General
2	Taxing Professional	SEEWOO Tookraj, Deputy Registrar-General GHOOLET Rakesh , Assistant Registrar-General
3	Taxing Public	GUKHOOOL Sadmadevi (Mrs), Deputy Registrar-General BENNY Janéswaree (Mrs) ,Assistant Registrar-General
4	Mortgage	SEEWOO Tookraj , Deputy Registrar-General BHUNJUN Parmanand , Assistant Registrar-General
5	Valuation	GUKHOOOL Sadmadevi (Mrs), Deputy Registrar-General FAKUN Yogeeta (Mrs), Assistant Registrar-General
6	Erasure	RAMRECHA Lutchmeenarain, Assistant Registrar-General
7	Quality Assurance Unit	SOODHOO Aruna Devi (Mrs) , Assistant Registrar-General LANGUR Bhanoodutt, Assistant Manager, Internal Control
8	Certified Copy Section	VENDEN Backtee (Mrs), Inscription and Check Clerk
9	Finance	KHODABUX Bibi Oummeh Salmah Mahmoud (Mrs) Manager, Financial Operations
10	HR Section	RAMSAHA Sharmila (Miss), Assistant Manager, Human Resources
11	Procurement & Supply	BHOYROO Beekash, Procurement and Supply Officer/Senior Procurement and Supply Officer
12	Office Accommodation & Transport	POOMUN Sowkataly, Office Management Executive
13	IT Section	NARAN Jayalakshmi (Mrs), Senior Systems Analyst
14	Registry	MUNBOD Gooroodev, Office Management Executive

## 5.0 Risk Management Process – Overview

The risk management process involves the elements as illustrated in the **Fig 1.0**



**Fig 1.0**

## 5.1 Risk Management Process- Methodology

The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the scope, context and criteria, assessing, treating, monitoring, reviewing, recording and reporting of risk (**Fig 1.0**).

The procedures as set out below should be followed when the different activities of the risk management process are conducted.

### 5.1.1 Communication and consultation

Communication and consultation should take place within and throughout the risk management process as outline in **Fig 1.0**, with relevant external and internal stakeholders to have a better understanding of risk which ultimately will provide:

- *the basis on which decisions will be made; and*
- *the reasons why particular actions will be required.*

For each step of the risk management process consideration should be given to bring different areas of expertise together.

### 5.1.2 Scope, context and criteria

The **scope** of the risk management activities comprises of the followings:-

- *Strategic;*
- *Operational (other activities); and*
- *Project (programme).*

The relevant objectives that have been considered need to be aligned with the Department objectives.

Only key risks which will have significant/material impact on the Department strategic/operational/project objectives, categorised as medium or high will be recorded in the Risk Register.

The **context**, external and internal environment, in which the Department operate and seek to achieve its objectives need to be thoroughly examined, understood and defined.

When establishing the context of the risk management process considering may be given to the following factors (not limited to):

External	Internal
<ul style="list-style-type: none"> <li>➤ the social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, whether international, regional national or local;</li> <li>➤ key drivers and trends affecting the objectives of the organization;</li> <li>➤ external stakeholders' relationships, perceptions, values, needs and expectations;</li> <li>➤ contractual relationships and commitments;</li> <li>➤ the complexity of networks and dependencies.</li> </ul>	<ul style="list-style-type: none"> <li>➤ vision, mission and values;</li> <li>➤ governance, organizational structure, roles and accountabilities;</li> <li>➤ strategy, objectives and policies;</li> <li>➤ the organization's culture;</li> <li>➤ standards, guidelines and models adopted by the organization;</li> <li>➤ capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, intellectual property, processes, systems and technologies);</li> <li>➤ data, information systems and information flows;</li> <li>➤ with internal stakeholders, taking into account their perceptions and values;</li> <li>➤ contractual relationships and commitments;</li> <li>➤ interdependencies and interconnections.</li> </ul>

**Risk criteria** is the amount and type of risk that the **Department** may or may not take relative to objectives and is used to evaluate the significance of risk and to support decision-making processes.

Risk criteria, for each area of risk assessment, will have to be determined and defined in relation to its objective. The risk criteria will have to be based on different Acts, regulations, Financial Circulars & Instructions, HR Manual and any other relevant procedures Manual governing the specific activity, area or operation. The criteria should continually be reviewed and amended, if necessary.

### 5.1.3 Risk Assessment

The risk assessment is the overall process of risk identification, risk analysis and risk evaluation. This needs to be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. This should be done using the best available information, supplemented by further enquiry.



### 5.1.3.1 Identify Risks

This step is the first in the risk assessment. The risk identification activity is performed to develop a list of potential things that could stop the **Department**. from achieving its goals/objectives. This list should always be wide-ranging as unidentified risks can cause major losses through missed opportunities or adverse events occurring.

‘Brainstorming’ will always produce a broad range of ideas and all things should be considered as potential risks. Relevant stakeholders with specific expertise are to be considered for this activity.

When identifying risks, consideration will be given to the following:

- What can happen?
- Why can it happen?
- What shall be the consequences?

Risks can also be identified through other business operations including policy and procedure development, internal and external audits, customer complaints, incidents and systems analysis.

When identify risk it is important that risks are correctly described to ensure they are fully understood and appropriate actions identified. The risk description will have to include the potential causes and consequences.

To ensure comprehensiveness of risk identification, the **Department** will identify risk factors through considering both internal and external factors, through appropriate processes of:

(a) **Strategic risk identification** to identify risks concerned with the Ministry/Department’s strategic decisions:

- (i) strategic risk identification will precede the finalisation of strategic choices to ensure that potential risk issues are factored into the decision making process for selecting the strategic options;
- (ii) risks inherent to the selected strategic options will be documented, assessed and managed through the normal functioning of the system of risk management; and
- (iii) strategic risks will be formally reviewed concurrently with changes in strategy, or at least once a year to consider new and emerging risks.

(b) **Operational risk identification** to identify risks concerned with the Department’s operations:

- (i) Operational risk identification will seek to establish vulnerabilities introduced by employees, internal processes and systems, contractors, regulatory authorities and external events;
- (ii) Operational risk identification will be an embedded continuous process to identify new and emerging risks and consider shifts in known risks through mechanisms such as management and committee meetings, environmental scanning, process reviews and the like; and

(iii) Subject to significant environmental and institutional changes, operational risk identification will be repeated when changes occur, or at least once year, to identify new and emerging risk.

(c) **Project risk identification** to identify risks inherent to particular projects:

(i) Project risks will be identified for all major projects, covering the whole lifecycle; and

(ii) For long term projects, the projects risk register will be reviewed at least once a year to identify new and emerging risks.

The Risk Identification Process is outlined at **Appendix 3.0**.

Examples of Risk Categories are given at **Appendix 3.1**.

### *5.1.3.2 Analyse and Evaluate Risks*

The risk analysis is performed to comprehend the nature of the risk and its characteristics including where appropriate the level of risk. On the other hand, the risk evaluation activity is conducted once the analysis is completed to decide whether risk is acceptable in its current state or whether further actions may be required to mitigate the risk.

The risk analysis is done for;

- determining the causes and consequences;
- determining the likelihood of the event; and
- identifying any existing controls. The existing controls are things that are already in place such as policies, procedures, training programs etc. These controls will require rating as either **effective**, **requires improvement** or **ineffective**.

The risk analysis provides insight and input for risk evaluation. This activity involves comparing the results of the risk analysis with the established risk criteria to determine actions in terms of whether:

- to do nothing further;
- to consider risk response options;
- to undertake further analysis to better understand the risk;
- to maintain existing controls;
- to reconsider objectives.

The outcome of risk evaluation will be recorded, communicated and validated/approved at appropriate levels of the [Department](#).

## **Risk Escalation**

Any risk that have a **high or extreme** controlled level or have controls rated as less than effective will require treatment plans. If the treatment plan does not reduce the level of risk or increase control effectiveness, the risk is required to be escalated to management for further attention or authority to issue additional action. Management determines if the risk should be escalated further.

**The Risk Analysis and Evaluation process is outlined at Appendix 4.0.**

### *5.1.4 Risk Response*

Risk responses are concerned with developing strategies to reduce or eliminate the threats and events that create risks.

Management will develop response strategies for all material risks which are within the direct control of the **Department**, prioritising the risks exceeding or nearing the risk appetite level.

The response strategies will consider the following:

- (a) **avoiding** the risk by, for example, choosing a different strategy or terminating the activity that produces the risk;
- (b) **treating** the risk by, for example, implementing or improving the internal control system;
- (c) **transferring** the risk to another party more competent to manage it by, for example, contracting out services and establishing strategic partnerships;
- (d) **accepting** the risk where cost and strategy considerations rule out alternative strategies; and
- (e) **exploiting** the risk factors by implementing strategies to take advantage of the opportunities presented by such risk factors.

Further details are given at **Appendix 5.0**.

When selecting the most appropriate risk treatment option(s) consideration should be given for balancing the potential benefits derived in relation to the achievement of the objectives against costs, effort or disadvantages of implementation.

Response strategies will be documented and the responsibilities and timeline attached thereto should be communicated to the relevant persons.

All risks identified by Risk Owners will be recorded in the Risk Assessment Table (**Appendix 6**) together with results of Risk analysis/evaluation and the risk response.

### 5.1.5 Monitoring and Review

The results of monitoring and review will be incorporated throughout the organization's performance management, measurement and reporting activities.

Monitoring will be effected through ongoing activities or separate revaluations to ascertain whether risk management is effectively practised at all levels and across the **Department**. in accordance with the risk management strategy, policy and framework.

Monitoring activities will focus on evaluating whether:

- (a) allocated responsibilities are being executed effectively; and
- (b) response strategies are producing the desired result of mitigating risks or exploiting opportunities.

### 5.1.6 Recording and reporting

The risk management process and its outcomes will be documented and reported through appropriate mechanisms. All key risks having significant/material impact on the **Department's** strategic/operational/project objectives, categorised as medium or high as identified in the Risk Assessment Table will be recorded in the Risk Register.

Risk Owner will report on a half yearly basis to the Risk Management Committee on the updated Risk Register.

The Risk Management Committee will consolidate the individual Risk Registers and will report accordingly to the SCE/PS/AO and the Audit Committee.

The Risks that will be reported to the Risk Management Committee is as per Risk Register Template at **Appendix 7.0**.

## 6.0 Evaluation of Risk Management Effectiveness

The **Department** will incrementally and sustainably achieve a mature risk management regime and periodically evaluate the value add of risk management by measuring outcomes against pre-set key performance indicators aligned to the overall goals and objectives.

### 6.1 Performance Indicators


Everyone in the **Department** has a part to play in achieving and sustaining a vibrant system of risk management and to that extent must function within a framework of responsibilities and performance indicators..The SCE/PS/AO will evaluate the performance in leading the risk management process in the **Department** through, *inter-alia*, the following:

- (a) the **Department's** performance against key indicators, including comparison of year-on-year performance; and
- (b) progress in securing improved audit outcomes in regularity and performance audits.

## 7.0 Review of the Framework

The Department will measure the effectiveness of the Risk Management in addressing the value creation principles and its ability to support the Department in identifying and consistently analysing risks and opportunities inherent in all our activities and operations.

All reviews of the Framework will be done as per Time Frame set out at **Appendix 2.0**.

Signature	
D. Hurrynag	
Registrar General	
Date	22/01/2024

## Risk Management Policy

Registrar General's Department			
Approved by	Approval Date	Effective date	Next Review
Registrar General	07 November 2023	07 November 2023	November 2025
<b>Purpose</b>	The Risk Management Policy demonstrate the commitment of Registrar General to Risk Management.		
<b>Scope</b>	The policy applies to all activities of the Registrar General's Department, including those of its Divisions/Units/Sections/ Functions.		

The Registrar General undertakes to put in place a process of risk management that is aligned to the principles of good governance.

Risk management is recognised as an integral part of responsible management and the Registrar General's Department therefore adopts a comprehensive approach to the management of risk. The features of this process are outlined in the Risk Management Framework. It is expected that all Units/Sections of the Registrar General's Department will be subject to the Risk Management Framework. It is the intention that these Units will work together in a consistent and integrated manner, with the overall objective of reducing risk, as far as reasonably practicable.

Effective risk management is imperative to the Registrar General's Department to fulfil its mandate, the service delivery expectations of the different stakeholders and the performance expectations within the Registrar General's Department. The realisation of our strategic plan depends on us being able to take calculated risks in a way that does not jeopardise the direct interests of stakeholders. Sound management of risk will enable us to anticipate and respond to changes in our service delivery environment, as well as make informed decisions under conditions of uncertainty.

We subscribe to the fundamental principles that all resources will be applied efficiently, effectively and economically to ensure:

- The highest standards of service delivery;
- A management system containing the appropriate elements aimed at minimising risks and costs in the interest of all stakeholders;
- Education and training of all our staff to ensure continuous improvement in knowledge, skills and capabilities which facilitate consistent conformance to the stakeholder's expectations; and
- Maintaining an environment, which promotes the right attitude and sensitivity towards internal and external stakeholder satisfaction.

An entity-wide approach to risk management will be adopted by the Registrar General's Department which means that every key risk in each part of the Registrar General's Department will be included in a structured and systematic process of risk management. It is expected that the risk management processes will become embedded into the Registrar General's Department systems and processes, ensuring that our responses to risk remain current and dynamic. All risk management efforts will be focused on supporting the Registrar General's Department objectives. Equally, ensuring compliance with relevant legislation, and fulfil the expectations of staff and other stakeholders in terms of corporate governance.

The Registrar General's Department will address all risks categorised as medium and high.

The risk policy statement shall be reviewed annually to reflect the current stance on risk management.

Every staff has a part to play in this important endeavour and we look forward to working with you in achieving these aims.

Signed on 07 November 2023 by Mrs Deoyani HURRYNAG, Registrar General

## Risk Management Plan

Element	Description	When	Who
Risk Management Policy	Policy review is once year	Annually	Risk Management Committee (RMC)
Risk Management Framework	A review every two years	Bi-annually	RMC
Risk Management Process	Formal risk management process meetings are to be undertaken as part of the annual business plan cycle, new initiatives, budget bids, cabinet submissions etc.	Annually	All Divisions/ Units/Sections
Roles and responsibilities	Roles and responsibilities are reviewed annually	Annually	All Divisions/ Units/Sections
Training and education	Risk Awareness and Meetings	As & When required	RMC
Risk Management Reporting Process	Risk Owners need to establish the risk registers and review the risk registers on a half yearly basis. Risk Committee is then provided with reports outlining the results. The <b>Registrar General</b> is then provided with a memo outlining the results of the half yearly reporting process. The AC will also have to provide an opinion on the results of the half yearly reporting process	Half Yearly	All Divisions/ Units/Sections
Escalation process	Any risks that have a high or extreme controlled level of risk OR have controls rated as less than effective will require treatment plans. If the treatment plan does not reduce the level of risk or increase control effectiveness, the risk is required to be escalated to management for further attention or authority to issue additional action. Management determines if the risk should be escalated further.	As required	All Divisions/ Units/Sections
Communication	Communication and consultation occurs on a regular basis to ensure key stakeholders (both internal and external) are consulted, engaged and actively involved throughout the risk management process.	Continually	All Divisions/ Units/Sections
	This allows for lessons learned to be identified and applied to continuously improve upon the risk management framework, processes and associated practices.	Half Yearly	All Units



## Risk Identification Process

Systematically and continuously identify risks faced in meeting objectives. For each business objective, it is necessary to identify the key risks that might impede the achievement of the respective business objectives. Risk identification will be performed as part of all major decision making processes.

### Step 1: Set out the objectives and activities of the Division/Unit/Section

#### Objectives and Activities

OBJECTIVES OF THE UNIT What we are trying to achieve in our business?	Activities (What are our activities?)
<b>1.</b>	<b>1.</b>
<b>2.</b>	<b>2.</b>
<b>3.</b>	<b>3.</b>
<b>4.</b>	<b>4.</b>
<b>5.</b>	<b>5.</b>

**Step 2: Identify all risks for each objective/ activity.**

(What can happen and why? What will be the cosequences?)

**Risk Decription**

SN	Risk Type	Risk Category	Risk Description		
			<i>Risks Identified</i>	<i>Cause</i>	<i>Consequences</i>
R001					
R002					
R003					
R004					
R005					

--	--	--	--	--	--

Note:

**Risk Type:** *Internal or External*

**Risk Category:** *see Appendix 3.1 below.*

**Each risk identified will be Coded as shown above; Examble R001. R002 etc.**

**Risk Categories**

Risk type	Risk category	Examples
<b>Internal</b>	Human resources	<p>Risks that relate to human resources of an institution. These risks can have an effect on the Min/Dept.'s human capital with regard to:</p> <ul style="list-style-type: none"> <li>• Integrity and honesty;</li> <li>• Recruitment;</li> <li>• Skills and competence;</li> <li>• Employee wellness;</li> <li>• Employee relations; and</li> <li>• Occupational health and safety.</li> </ul>

Risk type	Risk category	Examples
	Knowledge and Information management	<p>Risks relating to the Min/Dept.'s management of knowledge and information. In identifying the risks consider the following aspects related to knowledge management:</p> <ul style="list-style-type: none"> <li>• Availability of information;</li> <li>• Stability of the information;</li> <li>• Integrity of information data;</li> <li>• Relevance of the information; and</li> <li>• Retention and Safeguarding.</li> </ul>
	Litigation	<p>Risks that the Min/Dept. might suffer damages due to litigation and lawsuits against it which may emanate from different stakeholders including staff.</p>
	Loss \ theft of assets	<p>Risks that the Min/Dept. might suffer losses due to either theft or loss of an asset.</p>
	Service delivery	<p>The risk will arise if the appropriate quality of service is not delivered to the stakeholders.</p>
	Information Technology	<p>Possible considerations could include the following when identifying applicable risks:</p> <ul style="list-style-type: none"> <li>• Security concerns;</li> <li>• Technology availability (uptime);</li> </ul>

Risk type	Risk category	Examples
		<ul style="list-style-type: none"> <li>• Integration / interface of the systems;</li> <li>• Effectiveness of technology; and</li> <li>• Obsolescence of technology.</li> </ul>
	Health & Safety	Risks from occupational health and safety issues e.g. injury on duty, health hazards or outbreak of disease (epidemic/pandemic).
	Disaster recovery / business continuity	<p>Risks related to an Min/Dept.'s preparedness or absence thereto to disasters that could impact the normal functioning of the institution e.g. natural disasters, act of terrorism etc. This would lead to the disruption of processes and service delivery and could include the possible disruption of operations at the onset of a crisis to the resumption of critical activities. Factors to consider include:</p> <ul style="list-style-type: none"> <li>• Disaster management procedures; and</li> <li>• Contingency planning.</li> </ul>
	Compliance / Regulatory	<p>Risks related to the compliance requirements that the Min/Dept. has to meet. Aspects to consider in this regard are:</p> <ul style="list-style-type: none"> <li>• Failure to monitor or enforce compliance; and</li> <li>• Consequences of non-compliance.</li> </ul>
	Fraud and corruption	These risks relate to illegal or improper acts by staff resulting in a loss of the Min/Dept.'s assets or resources.

Risk type	Risk category	Examples
	Cultural	<p>Risks relating to the Min/Dept.'s overall culture and control environment. The various factors related to organisational culture include:</p> <ul style="list-style-type: none"> <li>• Communication channels and the effectiveness;</li> <li>• Cultural integration;</li> <li>• Entrenchment of ethics and values;</li> <li>• Goal alignment; and</li> <li>• Management style.</li> </ul>
	Reputation	Factors that could result in the tarnishing of the Min/Dept.'s reputation, stakeholder's perception and image.
<b>External</b>	Technological environment	Risks emanating from the effects of advancements and changes in technology.
	Legislative environment	<p>Risks related to the Min/Dept.'s legislative environment.</p> <p>E.g. changes in legislation, conflicting legislation.</p>


**Risk Analysis and Evaluation Process**

The main purpose of the Risk Analysis is to prioritise the most important risk of the **Department**. This will be done on the basis of the Likelihood of occurrence and its Impact.

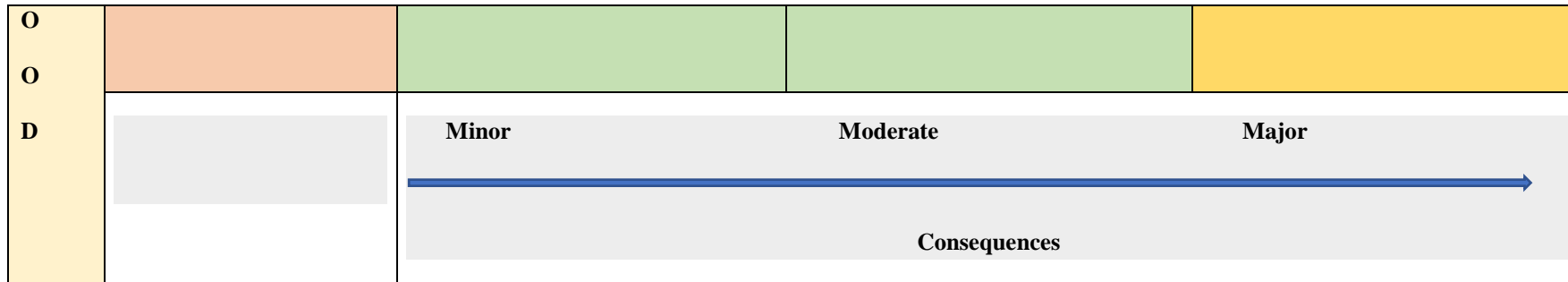
**Step 1: Analyse each risk in terms of Likelihood of occurrence and its Impact if it occurs**

The Heat Map as shown below will be used.

**Risk Analysis: Criteria and Scores**

<b>L I K E L I H</b> 	<b>Probable</b> (above 70%)	Medium	High	High (Critical)
	<b>Likely</b> (30 to 70 %)	Low	Medium	High
	<b>Remote</b> (Less than 30 %)	Low	Low	Medium





## Appendix 4.0 Cont'd

**High (Critical):-** Issues that require immediate attention of senior management.

**High:** - Issues that need constant monitoring by senior management.

**Medium:** - Issues for frequent review

**Low:** - Issues that need to be reviewed from time to time

### Step 2: Work out the Existing Control in place

- What are the controls in place?
- Are they governed by any Act, Regulations, Procedures Manual, FMM, HRMM etc..?

### Step 3: Assess the effectiveness of the Controls in place.

Are the controls:

- Effective?

- Ineffective?
- Need Improvements?

**Step 4: Assess whether further action required**

If the Control is not effective, or if need improvement, then consideration will be given whether further action is required. This can lead to a decision:

- Do nothing further.
- **Consider Risk Response options.**

**Appendix 4.0 Cont,d**

- Undertake further analysis to better understand the risks.
- Maintain existing controls.
- Reconsider objectives.

**Step 5: Outcome of the Evaluation**

The outcome of risk evaluation will be recorded, communicated and validated/approved at appropriate levels of the [Department](#).

**Template to be used as per Appendix 6.0**

**Risk Response**

Risks can be dealt with in various ways. The risk response options encompass all possible management response to risk, whether viewed as opportunities, uncertainties or hazards. The risk response options and examples of activities under each option are outlined below:

<p style="text-align: center;"><b>TREAT</b></p> <p>Steps taken to reduce either the likelihood of an occurrence or impact.</p> <ul style="list-style-type: none"> <li>-Improve or implement new controls.</li> <li>-Ensuring adequate skill sets.</li> <li>-Improving staff morale.</li> <li>-Implementing Business Continuity Programme.</li> </ul>	<p><b>Risk Response Options</b></p>	<p style="text-align: center;"><b>AVOID</b></p> <p>Steps taken to prevent the occurrence of hazards, such as:</p> <ul style="list-style-type: none"> <li>- Ceasing activity, Divestment of operations, Changing objective, scale of operations or scope of coverage.</li> </ul>
<p style="text-align: center;"><b>TRANSFER</b></p> <p>Steps taken to shift the loss or liability to third parties, such as:</p> <ul style="list-style-type: none"> <li>-Insuring , Outsourcing, Diversifying of investments, Hedging</li> </ul>		<p style="text-align: center;"><b>EXPLOIT</b></p> <p>Steps taken to leverage opportunities, such as:</p> <ul style="list-style-type: none"> <li>-Expanding business portfolios, Influencing regulators, public perception.</li> <li>-Renegotiating contracts - Reorganising and restructuring.</li> <li>-Creating innovative products</li> </ul>

All Risk Response will be documented in the Risk Assessment Table.

## Appendix 6.0

### Risk Assessment Table

Section/Unit:.....

SN	Risk analysis & Evaluation								
	Risks Identified	Likelihood <i>-Probable</i> <i>-Likely</i> <i>-Remote</i>	Impact <i>-Major</i> <i>-Moderate</i> <i>-Minor</i>	risk Ratings H,M or L	Existing control	Is existing controls Effective? Yes/No  Need Improvement?	Further action required/  Yes/No	Risk Response	Risk monitoring
R001									
R002									
R003									
R004									

R005									

***Risk Owner***

***Name:.....***

***Signature:.....***

***Date:.....***

**Risk Register**

*Unit/Section*.....

SN	Risk Type	Risk Category	Risk Identified	Risk Rating Medium/ High	Risk Response	Risk Monitoring Status
R001						
R002						
R003						
R004						
R005						

**Risk Owner**

**Name:**.....

**Signature:**.....

**Date:**.....

