

**Disclaimer : Ministry of Finance and Planning repository shall be regarded as a publisher and bears no liability for any damage upon using contents of the repository.**

---

Manuals & Guidelines

Risk Management Guidelines

---

2023

# Guidelines for Developing and Implementing Institutional Risk Management Framework in Public Sector Entities

Tanzania, The United Republic

---

<https://repository.mof.go.tz/handle/123456789/843>

*Downloaded from Ministry of Finance and Planning Repository*

**THE UNITED REPUBLIC OF TANZANIA**  
**MINISTRY OF FINANCE**



**GUIDELINES FOR DEVELOPING AND IMPLEMENTING INSTITUTIONAL RISK  
MANAGEMENT FRAMEWORK IN PUBLIC SECTOR ENTITIES**

REVISED  
**JULY 2023**

## TABELE OF CONTENTS

STATEMENT OF THE PERMANENT SECRETARY .....	v
STATEMENT OF THE INTERNAL AUDITOR GENERAL.....	vi
LIST OF TABLES.....	vii
LIST OF FIGURES.....	viii
LIST OF ABBREVIATIONS.....	ix
<b>SECTION I</b> .....	<b>1</b>
1 INTRODUCTION .....	1
1.1 Background.....	1
1.2 Risk .....	1
1.3 Risk Management .....	2
1.4 Risk Management Framework .....	2
1.5 Benefits of Managing Risks.....	3
1.6 Purpose of the Guidelines.....	3
1.7 Scope of the Guidelines.....	4
1.8 Review of the Guidelines .....	4
<b>SECTION II</b> .....	<b>5</b>
2 GOVERNMENT’S RISK MANAGEMENT POLICY STATEMENT .....	5
2.1 Introduction .....	5
2.2 Risk Management Policy Statement .....	5
2.3 Adoption of Risk Management Standards.....	6
2.4 Implementation Requirements to PSEs .....	6
2.5 Implementation Roles and Responsibilities.....	6
<b>SECTION III</b> .....	<b>17</b>
3 DESIGNING THE RISK MANAGEMENT FRAMEWORK.....	17
3.1 Introduction .....	17
3.2 Principles of Risk Management.....	17
3.3 Develop and Document a Risk Management Framework .....	21

<b>SECTION IV</b> .....	32
<b>4 IMPLEMENTING THE RISK MANAGEMENT PROCESS</b> .....	32
4.1 Introduction .....	32
4.2 Prepare Annual Plan for Risk Management Activities .....	32
4.3 Align the Timing of Risk Assessment Process to PSE Planning Process .....	33
4.4 Implement the Risk Management Process .....	34
<b>SECTION V</b> .....	57
<b>5 MONITORING AND REVIEW OF RISK MANAGEMENT FRAMEWORK</b> .....	57
5.1 Introduction .....	57
5.2 Monitoring the Risk Management Process .....	57
5.3 Reviewing the Risk Management Framework .....	62
<b>5.4 Assessing Maturity of the Risk Management Framework</b> .....	67
<b>SECTION VI</b> .....	69
<b>6. TEMPLATES</b> .....	69
Template 1: Example of Risk Management Policy Statement .....	69
Template 2: Examples of Risk Categories, Appetite Statement and Ratings for Risk Categories .....	71
Template 3: Indicative Risk Management Governance Structure in Ministries .....	74
Template 4: Indicative Risk Management Governance Structure for LGAs .....	75
Template 5: Indicative Risk Management Governance Structure for Departments/ Parastatals .....	76
Template 6: Sample Outline of a Risk Management Framework .....	77
Template 7: Sample of Outline of an Annual Risk Management Plan .....	78
Template 8: List of Common Examples of Risks .....	83
Template 9: Guide to Wording of Risks .....	86
Template 10: Risk Assessment Sheet .....	87
Template 11: Extract of a Risk Register .....	90
Template 12: Extract of Risk Treatment Action Plan .....	91

Template 13: Risk Management Quarterly Implementation Report .....	92
Appendix 14: Risk Management Performance Monitoring Plan .....	94
Appendix 15: Risk Management Evaluation Matrix .....	95
Template 16: Risk Maturity Assessment Questionnaire .....	108
Glossary of Terms .....	113

---

APPROVED

## STATEMENT OF THE PERMANENT SECRETARY

---

In the year 2010, the Government of the United Republic of Tanzania amended the Public Finance Act, CAP 348 by establishing the Internal Auditor General's Division (IAGD). One of the key responsibilities of the IAGD is to undertake continuous audit of risk management. Further, Section 6 (2) of the Public Finance Act, CAP 348 gives mandate to the Permanent Secretary-Treasury to issue directions and/or instructions, from time to time, to ensure safety and efficient use of public resources. This has placed greater need for the Public Sector Entities (PSEs) to develop and implement their own risk management frameworks as part of their governance processes.

In 2012, the Ministry of Finance and Planning released Guidelines for Developing and Implementing Institutional Risk Management Framework in Public Sector followed by implementing circular No. 12 of May 2013. The purpose of the guidelines was to provide practical guidance to PSEs in developing, implementing and enhancing risk management frameworks, hence, improve performance by proactively anticipate and manage risk, set and achieve strategic objectives, improve decision-making and help to allocate and utilize resources effectively. There has been good progress in the implementation of the guidelines where 331 PSEs have in place the Risk Management Frameworks and basic Risk Registers.

In compliance with the five level Organisation of Economic Cooperation and Development (OECD) Risk Maturity model, the achievement of implementation of risk management has shown that most PSEs are between second and third level of maturity. In order to reach the fourth and fifth optimal maturity level, a need to align the Guidelines with updated international standards and incorporation of lessons learned from monitoring and evaluation activities is imperative.

From the foregoing, the Ministry has reviewed the Guidelines in developing and implementing customized risk management frameworks. The Guidelines are also expected to instil a changed culture within PSEs, where risk awareness will be embedded in every aspect of governance and at every level of management. It is expected that all PSEs will have robust risk management policies, structures and procedures that will facilitate an effective assessment of risks against their objectives and be able to put in place appropriate controls to mitigate these risks. This, at the end, will provide assurance on the achievement of their objectives in providing service to the public.

In reviewing these Guidelines, there were many collaborative efforts. The Guidelines have been reviewed in close consultation with the staff within the Office of the Internal Auditor General, Mzumbe University and other key stakeholders, from both public and private sector. I wish to express my appreciation to all of them for their time and efforts in the successful completion of this document.

These guidelines apply to all PSEs and their employees at both levels of the government. Each PSE should develop an implementation plan to comply with these guidelines, clearly providing timelines for the development of risk management policy, governance structure; risk registers and continuously improve its risk maturity.

All PSE should fully adopt these guidelines and report to the Ministry of Finance and Planning through the IAGD on adherence of these guidelines on quarterly basis.

*Nwamba*

DR. NATU E. MWAMBA  
PERMANENT SECRETARY – TREASURY

## STATEMENT OF THE INTERNAL AUDITOR GENERAL

---

The preparation of these guidelines forms an important milestone in the process of helping Public Sector Entities (PSEs) to achieve their intended objectives more efficiently and effectively. It is on this premise that even the amendment of the Public Finance Act, CAP 348 includes a section that charge the Internal Auditor General to undertake continuous audit of risk management.

The reviewed Guidelines are composed of four main areas:

- i. Introduction, Purpose, and Scope;
- ii. Government's Policy Statement and Implementation Requirements;
- iii. Risk Management Guidelines to PSEs; and
- iv. Toolkit.

These sections provide practical guidance (steps and procedures) to PSEs when developing and implementing their own customized risk management frameworks. The Guidelines should be considered as a live document. It is subject to periodic review/updates as and when changes in laws, regulations, standards occur and/or any other experience learned during implementation that need to be captured in the document.

I further stress on the important aspect that while developing and implementing the risk management frameworks, PSEs should consider and align the frameworks with their current/existing structures. Risk management should not be seen as an "external" or "new" component but rather a complement and improvement in the decision-making process. It should be integrated with strategic planning process and embedded within the business processes adopted by the PSE. These guidelines complement Guidelines for Developing and Implementing Fraud Risk Management Frameworks in Public Sector and Guidelines for Enhancing Internal Control Frameworks in the Public Sector.

I also wish to record my acknowledgement to all individuals and organs that were involved in the process of preparation and finalization of these guidelines, for their dedication and commitment into the whole process. I, furthermore, recognize the invaluable assistance, encouragement, and support to the whole process by the Permanent Secretary - Treasury.



BENJAMIN M. MAGAI

**INTERNAL AUDITOR GENERAL**

## LIST OF TABLES

---

Table 1: Indicative List of Workshops to Provide on Risk Management .....	30
Table 2: Illustrative 5-point Scale for Assessing Impact of a Risk (COSO, 2012) .....	39
Table 3: Illustrative 5-point Scale Likelihood of Risk (COSO, 2012) .....	40
Table 4: Risk Ratings and Colour Status to Guide Risk Tolerance Levels .....	41
Table 5: Effectiveness of Controls, Colour Coding and Meaning .....	48
Table 6: Example of Risk Heat Map with Risks Plotted in the Three (3) Regions of Risk Tolerance .....	50
Table 7: Extract of Risk Maturity Assessment Questionnaire .....	68

## LIST OF FIGURES

---

Figure 1: Principles of Risk Management (ISO 3100: 2018) .....	17
Figure 2: Key Considerations for Developing Risk Management Framework (ISO 31000:2018) .....	22
Figure 3: Risk Management Process (ISO 31000:2018): .....	35

APPROVED

## LIST OF ABBREVIATIONS

---

<b>AIAG</b>	Assistant Internal Auditor General
<b>ASEC</b>	Asset, Source, Event and Consequence
<b>CAP</b>	Chapter
<b>COSO</b>	Committee of Sponsoring Organizations of the Treadway Commission
<b>CRSA</b>	Control Risk Self-Assessment
<b>ERM</b>	Enterprise Risk Management
<b>FERMA</b>	Federation of European Risk Management Associations
<b>IAG</b>	Internal Auditor General
<b>IIA</b>	The Institute of Internal Auditors
<b>IRM</b>	Institute of Risk Management
<b>IRMF</b>	Institutional Risk Management Framework
<b>IT</b>	Information Technology
<b>ISO</b>	The International Organization for Standardization
<b>OECD</b>	Organisation of Economic Cooperation Development
<b>IAGD</b>	Internal Auditor General Division
<b>KCI</b>	Key Control Indicator
<b>KRI</b>	Key Risk Indicator
<b>LGAs</b>	Local Government Authorities
<b>MDAs</b>	Ministries, Departments and Agencies
<b>PSE</b>	Public Sector Entities
<b>RIMS</b>	Risk Management Society
<b>RSs</b>	Regional Secretariats
<b>SWOT</b>	Strength, Weakness, Opportunities and Threat
<b>ToR</b>	Terms of Reference

## SECTION I

---

### 1 INTRODUCTION

#### 1.1 Background

Since the year 2012, when the first edition of Risk Management Guidelines was issued, risk management remains to be a crucial aspect of public sector governance. The 10 years journey towards integrating risk management in PSEs and the proven success in its role in creating and preserving value have heightened the need to achieve maturity levels of capability.

As with the first edition, this document is written to give a step-to-step guidance to PSEs on how to develop and implement risk management. The language and structure of the guidelines are generic, simplified and designed for application by all types and sizes of PSEs, namely: Ministries, Independent Departments, Authorities, Agencies, Regional Secretariats Local Government Authorities, Public Corporations, Judiciary, Parliament, and all other offices in the public service.

The need for updating came as a response to several factors including the changed public sector governance terrain, updates in global risk management body of knowledge and respective international standards; and as pointed out earlier, to accommodate lessons learnt during the 10 years' implementation of the first edition of the guidelines.

Specifically, changes in ISO 31000 *Risk Management – principles and guidelines* (from 2009 to 2018) and stakeholders' inputs have called for the revision that will not only align the Guidelines to the public sector context, but also to globally accepted definition of risk and updated risk management principles, framework and process.

#### 1.2 Risk

In this guide, risk is defined as the *effect of uncertainty on objectives*<sup>1</sup>.

Other definitions of risk are considered appropriate, when accommodates the following aspects of risk:

- i. Risk as an uncertain event, situation, condition, or a deviation from the expected that, if it occurs, will affect the achievement of a given objective.

---

<sup>1</sup> ISO 31000:2018

- ii. Risk can be positive, negative or both, and may create or result in opportunities and/or threats.
- iii. Risk is differentiated from a problem, challenge, and issue mainly by uncertainty to its occurrence. The characteristics of risk distinguishing it from challenge and a problem include; a future event with likelihood/impact, can be a threat or opportunity and a degree of uncertainty.

### 1.3 Risk Management

In this guide risk management is:

*“Coordinated activities to direct and control an organization with regard to risk”.* (Source: ISO 31000:2018)

The following features give more elaborations to the above definition of risk management:

- i. It includes management policies and procedures for identifying, analysing, evaluating, treating, and monitoring various risks that might affect an PSE’s ability to achieve its objectives.
- ii. It encompasses the culture, capabilities, and practices, integrated with strategy setting and its performance, that PSE rely on to manage risk in creating, preserving, and realizing value<sup>2</sup>.
- iii. It is application of management policies and procedures and practices to task of identifying, analysing, evaluating, treating, and monitoring various risks that might prevent PSE from achieving its objectives.

### 1.4 Risk Management Framework

A risk management framework as defined by the ISO 31000: 2018 is:

*“Set of components that provide the foundations and organizational arrangements for integrating, designing, implementing, evaluating and improving risk management across the entity”.*

The purpose of a risk management framework is to assist a PSE to manage its risks effectively through the application of risk management process at varying levels and within specific contexts of the PSE.

---

<sup>2</sup> Definition of Enterprise Risk Management by COSO (2017).

## 1.5 Benefits of Managing Risks

The following are the potential benefits for managing risks in PSEs:

- i. Establishment of a reliable basis for decision making and planning (strategic and operational planning);
- ii. Assurance on the achievement of PSE's objectives and performance targets through the awareness and management of potential events/and situations that work against the objectives;
- iii. Enhanced communication across all levels of management within the PSE;
- iv. Effective use of resources; minimize operational surprises and shocks and other costly and time-consuming litigation and/or unexpected losses;
- v. Management will grasp new opportunities in a timely manner;
- vi. Facilitate compliance with relevant legal and regulatory requirements and international norms;
- vii. Enhance health and safety performance, as well as environmental protection;
- viii. Improve stakeholders' confidence and trust (i.e., reassure stakeholders that the PSE is managing its risks efficiently and effectively);
- ix. Support strategic and business planning processes leading to few shocks and unwelcome surprises; and
- x. Support effective use of resources and promotes continual improvement.

## 1.6 Purpose of the Guidelines

The key purpose of the Guidelines is to provide practical guidance to PSEs in developing and implementing risk management framework and process.

The Guidelines are developed such that they can be applied by PSE with varying levels of risk management maturity, while recognizing that risk management is a continuous journey of improvement.

Specifically, the guidelines serve the following purposes:

- i. To disseminate the Government's commitment and intentions towards the adoption, implementation and enhancement of enterprise risk management practices across the public sector;
- ii. To develop common understanding of Risk Management policies, issues and procedures across the PSEs;
- iii. To sensitize Accounting Officers, senior and all other staff of the PSE on the risk management concept and its importance on the achievement of strategic and operational objectives;
- iv. To provide insights on steps to be followed when developing and implementing customized risk management frameworks;
- v. To provide a benchmarking criterion of evaluating internal and/or external capacity to develop an Institutional Risk Management Framework;
- vi. To assist PSEs to embed risk management culture and practices amongst all staff as well as put in place effective accountability strategies and mechanisms; and
- vii. To assist internal auditors in providing an independent assurance to the management, councils, boards, oversight bodies and key stakeholders of PSE on the effectiveness of the risk management frameworks.

### 1.7 Scope of the Guidelines

These guidelines apply to all PSEs, including Ministries, Independent Departments, Authorities, Agencies, Regional Secretariats Local Government Authorities, Public Corporations, Judiciary, Parliament, and all other offices in the public service.

Public Sector Entities, in addition to these guidelines, should comply with risk management guidelines issued by their respective industry regulators.

### 1.8 Review of the Guidelines

These guidelines shall be reviewed after every five (5) years or as may be necessitated by changes in applicable laws, regulations in the United Republic of Tanzania or significant changes in the International Standards relating to risk management.

Suggestion for amendments, additions and improvements to the guidelines should be directed to the Ministry of Finance and Planning through the Internal Auditor General Division (IAGD).

## SECTION II

---

### 2 GOVERNMENT'S RISK MANAGEMENT POLICY STATEMENT

#### 2.1 Introduction

The policy statement on risk management is given in this document to communicate the government's mission, commitment and adopted standards towards managing risks in the public sector. It is also aimed at charging PSE officials with duties for effective risk management in their areas of responsibilities.

Section 6 (2) of the Public Finance Act, CAP 348 gives mandate to the Permanent Secretary-Treasury to issue directions and/or instructions, from time to time, to ensure safety and efficient use of public resources. Therefore, the adoption of risk management, and any other best practice, is a responsibility that public sector Officials are charged with ensuring safety and efficient use of public resources.

In addition, risk management becomes an important aspect in public sector governance when responding to the current requirements of Section 32 of Public Finance Act, CAP 348, which gives the Internal Auditor General (IAG) the responsibilities to assure the effectiveness of risk management in PSEs.

#### 2.2 Risk Management Policy Statement

The Government recognizes that risk is inherent in each objective and operations of all PSEs. The Government considers the management of risks as an integral part of sound public sector governance because it provides assurance to the achievement of government's objectives across different sectors, which in turn leads to the effectiveness and efficiency in government performance towards providing services to the citizens and increased stakeholders' confidence. The Government is committed to ensuring that risk management is adopted, implemented, and enhanced across the public sector.

The Government, through the Ministry of Finance and Planning, takes an active role in providing and setting broad guidance and support on the development, implementation, and enhancement of risk management practices across the public sector. With the same commitment, Accounting Officers of all PSEs are required to adopt and implement effective risk management practices in their respective entities.

## 2.3 Adoption of Risk Management Standards

It is acknowledged that there are several best practices and standards for managing PSEs risks. The Guidelines are written in line with the ISO 31000:2018 Risk management — Principles and Guidelines.

Regardless of maturity levels, all PSEs are required to comply with minimum requirements of the guidelines. Public entities should in addition, comply with risk management standards and/ or any other standards issued by their respective industry regulators.

## 2.4 Implementation Requirements to PSEs

All PSEs are required to develop, implement, and enhance a risk management framework and process, which ensures that:

- i. There is a risk policy, culture and structure that facilitates how the entity will identify, record, and monitor risks, including procedures for reporting risk information to the Accounting Officers and other oversight organs within and outside the PSEs;
- ii. Procedures for the risk management are in line with ISO 31000:2018 risk management process and/or other risk management standards issued by their industry regulators;
- iii. The risk management process is integrated to be part of the strategic, budgeting and operational business planning activities of the PSE;
- iv. There is a risk register, which is used to record, rate, profile, monitor and report the identified risks;
- v. There is an established process for monitoring, reviewing, reporting, and enhancing risk management and governance systems; and
- vi. There is established procedures for incident management.

## 2.5 Implementation Roles and Responsibilities

The following are the implementation responsibilities for various executive authorities, oversight organs and officials in PSE.

At an institutional level, all PSEs are required to customize the specific roles and responsibilities so that they align to their entity's organizational structure and context.

### 2.5.1 Permanent Secretary-Treasury

The Permanent Secretary - Treasury (Paymaster General) shall have the overall responsibility of ensuring effective application of risk management processes, procedures, and practices in all PSEs. In discharging this responsibility; he/she will be assisted by the Internal Auditor General.

### 2.5.2 Internal Auditor General

The Internal Auditor General (IAG), working under the Permanent Secretary – Treasury, is responsible for

- i. Ensure all internal auditors performs Risk Based Internal Auditing and are forefront in championing the adoption, implementation, and enhancement of risk management practices across the public sector.
- ii. Issuing guidelines and directives on issues regarding public sector risk management.
- iii. Providing support (in form of capacity building), guidance and disseminating best practices on risk management to PSEs.
- iv. Conducting reviews and assessments on the quality and effectiveness of risk management in PSEs.
- v. Receiving risk management quarterly implementation report and Risk Management Assurance Report from all PSEs.
- vi. Coordinate National risk management effort including development of National Risk Register.
- vii. Conduct annual risk management maturity assessment across public sector entities.

### 2.5.3 Governing/Oversight Bodies

Where applicable, Governing Body (Board of Directors and Councils) should provide direction and oversight of risk management across the PSE. This is also applicable to PSE without oversight bodies such as Regional Administrative Secretary and Permanent Secretary.

The Governing Body's key risk management responsibilities should include:

- i. Approving the PSE's risk management documentation (risk management policy, structure, procedures, and risk registers).
- ii. Setting the standards and expectations of the PSE with respect to conduct and behaviour and ensuring the effective risk management is enforced through an effective performance management system.
- iii. Monitoring the management of high and significant risks, and the effectiveness of associated controls through the review and discussion of quarterly risk management reports from PSE management.
- iv. Satisfying itself that risks with lower ratings are effectively managed, with appropriate controls in place and effective reporting structures.
- v. Approving major decisions affecting the PSE's risk profile or exposure.

#### 2.5.4 Accounting Officers

Accounting Officers are accountable for the overall governance of the risk management practice in the PSE. They will oversee the development and implementation of risk management frameworks that align to their PSE's operations, structure, and context.

Specifically, the Accounting Officers has the responsibility to:

- i. Effectively and efficiently manage risks in all PSE operations.
- ii. Setting an appropriate tone by supporting the adoption and implementation of effective risk management.
- iii. The design, implementation, and enhancement of risk management framework and process.
- iv. Delegate responsibilities for risk management to risk management and internal formations so that it aligns to the existing PSE structure, processes, culture and context.
- v. Ensuring appropriate action in respect of the recommendations of audit committee, risk committees, internal audit, and external audit with regard to issues of risk management.
- vi. Providing assurance to the Governing Body and other stakeholders that key risks are properly identified, assessed, and treated; and
- vii. Ensuring the risk coordinating function is supported in carrying out its role.

- viii. Ensuring quarterly risk management reports are submitted to the Ministry of Finance and Planning (Internal Auditor General) for assurance purposes.

### 2.5.5 Entity Management Team/Risk Committee

The Management Team shall also be known as the *Risk Management Committee*, which shall be composed of members of the Management Team and chaired by the Accounting Officer. The team should bear the following responsibilities that are related to risk management:

- i. Have a standing agenda item on risk in all its meetings for enhancement of Risk Management practices throughout the PSE
- ii. Having a standing agenda on risk in their quarterly meeting to discuss risk management implementation report submitted by Risk Management Coordinator who will be an invited person for the purpose, depending on the organization structure;
- iii. On annual meeting to receive the feedback from Internal Auditor on the effectiveness of the implementation of the Risk Management Framework and Process;
- iv. Monitors performance of management in implementing risk management responses and internal control rectification activities and ensure that there are appropriate systems for identifying and monitoring risks and that are operating as intended;
- v. Shall be responsible for the overall mitigation of the risk management processes within the PSEs;
- vi. In a quarterly basis, shall review significant risks affecting the PSE and take proper actions to ensure that the risks are reduced to the acceptable risk level in line with the PSE's risk appetite;
- vii. Shall effectively implement risk management policies and internal control system complemented by Guidelines for Enhancing Internal Control Framework in the Public Sector; and
- viii. Re-asses the appropriateness of the risk appetite decision periodically.

### 2.5.6 Audit Committee/Other Related Committee

Depending on the reporting structure, some PSEs have a risk management committee in place, while others have not. It is here advised that if there is no special committee for risk management, there is no need to form one at the early stages of adopting risk management. Instead, the audit committee/other related committee should be given the responsibilities for this aspect by including issues of risk management in its existing charter.

Also depending on the nature of the PSE, where some have Audit Committee/or a risk management committee as committees of the governing board/or council, hence is more of an oversight than advisory. It is advised that the roles and responsibilities should be designed to fit this structure. However, as in most PSEs, the Audit Committee has an advisory role and reports to the Accounting Officer.

In relation to risk management, the Audit Committee or risk management oversight committee, as appropriate should therefore:

- i. Familiarize itself with risk management process and approach of the PSE.
- ii. Make risk management as one of its standing agendas in all its meetings.
- iii. Catalyse risk management by enquiring from management risk assessments and treatment reports.
- iv. Ask to see the departmental/institutional level risk registers periodically.
- v. Review all matters related to risk and risk management, through risk management reports, on the manner they are being managed.
- vi. Ensure appropriate internal audit work is undertaken concerning risks, by ensuring that internal audit plans are risk-based and focus on the most significant risk areas.
- vii. Provide regular feedback to the Accounting Officer/the governing body/Council on the adequacy and effectiveness of risk management in the PSE, including recommendations to improvement.

### 2.5.7 Risk Management Coordinator/Risk Management Coordination Unit

It is advisable that the PSE establishes the Risk Management Coordination Unit as part of structure improvement. In case the Unit is not in place, the Risk Management Coordinator shall be appointed among senior officers to coordinate issues of risk

management in the PSE. The principles and responsibilities of Risk Management Coordinator, amongst many, shall include:

- i. The appointed person should be able to attend regular management meetings and debrief on the status of risk management mitigation strategies.
- ii. For PSEs with mature risk management practices, the senior officer is also named as the Risk Manager/Chief Risk Officer.
- iii. The risk management coordinator works to assisting the Accounting Officer and is therefore responsible for coordinating efforts in designing the PSE's risk management framework and for the day-to-day activities associated with coordinating, maintaining, and embedding the framework in the PSE.
- iv. For the PSEs without specific unit for coordination of risk management, the department responsible for planning should coordinate the development and implementation of risk management practices.
- v. The risk management function should be assigned to a senior member of staff with appropriate knowledge, experience, skills and professional qualifications in risk management.
- vi. If the appointed Risk Management Coordinator has no knowledge, experience, skills, the PSE should arrange training of risk management for the appointed risk coordinator.
- vii. The risk management coordinator has the responsibility to:
  - a) Coordinate efforts for developing and enhancing appropriate risk management policies, procedures, and systems;
  - b) Coordinate and monitor the implementation of risk management initiatives within the PSE;
  - c) Work with risk owners to ensure that the risk management processes are implemented in accordance with agreed risk management policy and strategy;
  - d) Collate and review all risk registers for consistency and completeness;
  - e) Provide advice and tools to staff, management, the Executive and Board on risk management issues within the organization, including facilitating workshops in risk identification;

- f) Promote understanding of and support for risk management including delivery of risk management training;
- g) Oversee and update PSE-wide risk profiles, with input from risk owners;
- h) Ensure that relevant risk information is reported and escalated or cascaded, as the case may be, in a timely manner that supports PSE requirements;
- i) Issue a report on implementation of risk management to PSEs Management, risk committee (where applicable) and Audit Committee meetings on quarterly basis;
- j) Monitoring the adequacy and effectiveness of risk treatment plans, and accuracy and completeness of reporting; and
- k) Attendance at audit committees meetings where risk management issues are discussed.

#### 2.5.8 Directors, Heads of Divisions, Heads of Units and Sections (Risk Owners)

Heads of Division, Sections and Units have ownership, responsibility, and accountability for assessing, controlling and mitigating risks together with maintaining effective internal controls. As “risk owners”, they play a more hands-on-role in executing, day-to-day, risk and control procedures and are responsible for maintaining effective internal controls on a day-to-day basis. The specific responsibilities for heads of departments and divisions in relationship to risk management include:

- i. Identifying and managing risks as part of their everyday business, escalating them promptly as and when necessary;
- ii. Facilitate development of risk tolerance thresholds for processes;
- iii. Maintenance of risk register and other documents/reports relating to risk management within their respective departments or directorates in a systematic manner;
- iv. Embedding risk management practices within the business processes;
- v. Monitoring risk management against risk criteria;
- vi. Provide information about the risk when it is requested. This includes giving cooperation to auditors (both internal and external) during audit of risk management activities within their departments or directorates;

- vii. Periodic review of their risk registers and related controls; and
- viii. Preparation of quarterly risk management implementation reports of risk treatment action plans and to submit them to the Risk Management Coordinator.

### 2.5.9 Risk Champions

It is advised that several existing staff be appointed as risk champions. Risk champions are people who promote risk management across the entity, or specifically within a particular function, division, section, unit, or project. They can help embed risk management into the entity other systems and processes. Champions can also help ensure that functional and project areas are using the organizations risk management processes consistently.

A risk champion may hold any position within the entity but is generally a person who:

- i. Has the skills, knowledge and leadership qualities required to support and drive a particular aspect of risk management.
- ii. Has sufficient capacity to intervene in instances where risk management efforts are being hampered by a lack of cooperation or through lack of risk management capability or maturity.
- iii. Is able to add value to the risk management process by providing guidance and support in managing difficult risk or risks spread across functional areas.
- iv. If the appointed Risk Champion has no knowledge, experience, skills, the PSE should arrange training of risk management for the appointed risk champion.

The risk management champions have the responsibility within the Division, Section or Unit:

- a) Coordinate efforts for developing and enhancing appropriate risk management policies, procedures, and systems;
- b) Coordinate and monitor the implementation of risk management initiatives within the Division, Section or Unit;
- c) Work with risk owners to ensure that the risk management processes are implemented in accordance with agreed risk management policy and strategy;
- d) Collate and review all risk registers for consistency and completeness;

- e) Provide advice and tools to staff, management, the Executive and Board on risk management issues within the organization, including facilitating workshops in risk identification;
- f) Promote understanding of and support for risk management including delivery of risk management training;
- g) Oversee and update Division, Section or Unit-wide risk profiles, with input from risk owners;
- h) Ensure that relevant risk information is reported and escalated or cascaded, as the case may be, in a timely manner that supports Division, Section or Unit requirements;
- i) Prepare a report on implementation of risk management and submit to Risk Owner and Risk Management Coordinator on quarterly basis;
- j) Monitoring the adequacy and effectiveness of risk treatment plans, and accuracy and completeness of reporting; and
- k) Attendance at Division, Section or Unit meetings where risk management issues are discussed.

#### 2.5.10 Internal Audit

- i. Internal auditors' primary responsibility is to provide independent and objective assurance on the effectiveness of the PSE's risk management arrangements including reviewing risk management processes, reviewing the management of key risks; evaluating the reporting of key risks and giving assurance that risks are correctly evaluated;
- ii. Internal audit should use the results of the entity risk assessment in preparing a risk-based audit plan;
- iii. Internal audit can provide risk management consulting roles such as facilitating identification and evaluation of risks, coaching management in responding to risks, coordinating risk management activities, consolidating reporting on risks, maintaining, and developing risk management framework, championing establishment of risk management frameworks and developing risk management strategy. When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility as required by IPPF;

- iv. Internal auditors should pay particular attention on the professional limitation of their role regarding risk management activities. This should be made in reference to IIA position statement (i.e., on core roles, legitimate roles, and roles not to undertake); and
- v. Internal Auditors should champion establishment of risk management processes in their respective PSEs wherever there is a gap of expertise and understanding.

#### 2.5.11 All Staff

Every individual staff shall have the following roles and responsibilities:

- i. Understand responsibilities in implementing the risk management framework including the risk management strategy adopted by the Governing Authority;
- ii. Implement the recommendations and directives of their supervisors as far as risk management is concerned;
- iii. Comply with the risk management guidelines and procedures;
- iv. Identify risk and use appropriate documentation procedures to record them; and
- v. Promptly report on any risk incident to the respective risk owner and respective Risk Management Champion.

#### 2.5.12 Service Providers and Contractors

PSE's Service Providers are third Party entities that are contracted to provide operational activities on regular basis such as Security Guards, Cleaners and Contractors. The Responsibilities of Service Providers and Contractors includes but not limited to:

- i. Ensure their staff are aware of PSE's Risk Management Policy;
- ii. Report any risk to respective PSEs Head of Division/Section/Unit/Zones;
- iii. Ensure their staff are aware of key risks in their areas of operations and are well managed; and
- iv. Promptly report on any risk incident to the respective risk owner and respective Risk Management Champion.

### 2.5.13 The Controller and Auditor General (CAG)

The Control and Auditor General (CAG) by his powers and responsibilities stipulated in the Public Audit Act, CAP 418 plays a role of an external auditor. The CAG will consider issues of risk management when conducting audits of PSEs and provide observations and/or recommendations for improving the effectiveness of risk management.

APPROVED

## SECTION III

### 3 DESIGNING THE RISK MANAGEMENT FRAMEWORK

#### 3.1 Introduction

This section provides a procedural guide in developing and implementing risk management framework and conducting risk management process. As a preliminary to the procedural instructions, the section is preceded by principles and key considerations for developing a risk management framework (as given by the ISO 31000: 2018) on how to formulate the basic components of a risk management framework, namely risk management policy, risk appetite statements, risk governance structure, and procedures.

#### 3.2 Principles of Risk Management

Risk management principles are general rules and/or characteristics that form as a foundation for efficient and effective risk management.

The principles should be considered when establishing the PSE's risk management framework and processes. Figure 1 summarizes the eight (8) principles given by the ISO 31000:2018:

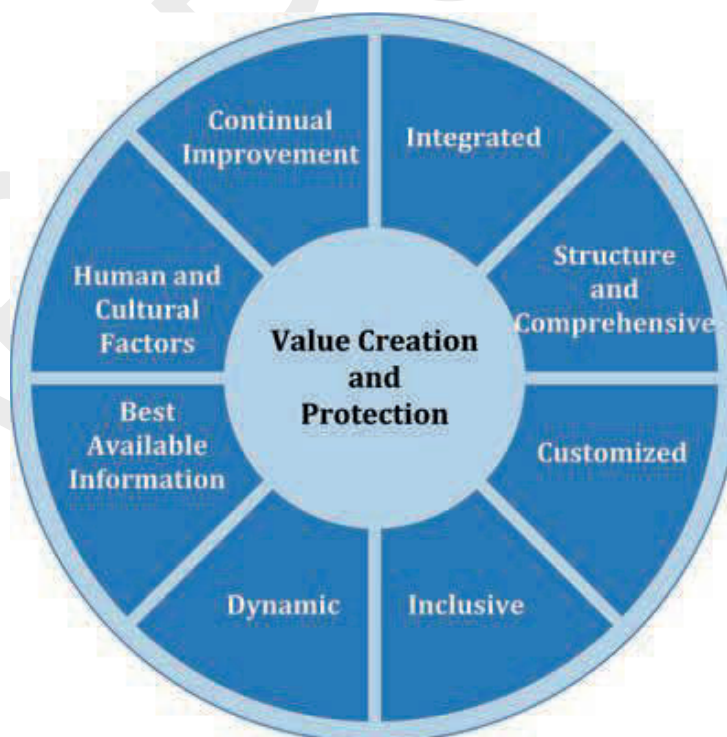


Figure 1: Principles of Risk Management (ISO 3100: 2018)

For simplicity, in this document the principles are sub-divided into two groups, namely:

- i. Principles for designing and planning risk management initiatives, and
- ii. Principles for implementing risk management initiatives.

### 3.2.1 Principles for Designing and Planning Risk Management Initiatives

When designing and planning risk management initiatives, including the development of risk management framework, PSEs must make sure that such initiatives are:

#### *i. Integrated to Existing Governance Structure, Culture, and other Management Systems*

PSEs should make sure that risk management activities are integrated (or embedded) in all aspects of the organization.

Integrated includes making sure that:

- a) Risk management should not be a stand-alone activity;
- b) Risk management should be part of the responsibilities of oversight bodies, management and an integral part of all organizational processes, including strategic planning and all project and change management processes (see [Section 4.3](#));
- c) Risk management processes and reports are aligned with PSE's reporting cycle, the board/audit committee meetings, management meetings, and organs outside the PSE; and
- d) Risks should be considered when making strategic decisions, in approving plans, budgets, investments, disposals, product or service design, organization structures, system development, contracting and appointments, among others.

#### *ii. Apply a Structured and Comprehensive Approach*

PSE's risk management activities should be structured and comprehensive:

- a) Having a structured and comprehensive approach will help to have risk management initiatives that achieves consistent and comparable results;
- b) PSEs should have risk management roles within a common unifying structure that is consistent with its organization structure;

- c) There should be a clear and consistent approach that identifies, assesses, treats and monitors risks.

### *iii. Customized to Fit the PSEs' Internal and External Context*

In formulating their risk management frameworks, PSEs should:

- a) Customize their risk policies, governance structures and procedures to align to their entities industry/sector, organizational structure, compliance and reporting requirements, and internal and external contexts; and
- b) Choice of risk management methodologies in conducting risk assessments should be tailored to match the risk management maturity level and available skills among staff.

### *iv. Inclusive of Inputs of Internal and External Stakeholders*

PSEs should ensure that risk management initiatives are appropriate and consider inputs/ issues from their internal and external stakeholders.

- a) Appropriate and timely involvement of PSE's internal and external stakeholders enables their knowledge, views and perceptions to be considered;
- b) This results into improved awareness and informed risk management and reduces subjectivity and resistance; and
- c) PSE should facilitate stakeholder's participation through transparent disclosure of information, consultation, communication, feedback, recording and reporting.

### *v. Dynamic to Adopt to Changes*

Risk management framework and related activities must be dynamic and responsive to emerging and changing risks.

- a) PSEs risk policies, procedures and registers should be able to capture risks that emerge due to changes in the PSEs internal and external context; and
- b) The updated information should be maintained through monitoring and review activities and the risk management framework evolved and improved to ensure it remains valid.

### 3.2.2 Principles for Implementing the Risk Management Initiatives

When implementing risk management initiatives, especially throughout the risk management process, PSEs must make sure that it follows the following principles:

#### *i. Use the Best Available Information*

Risk management activities should use the best available information and consider any limitations of available information.

- a) Base inputs to risk management from historical and current information, as well as on future expectations;
- b) Consider any limitations and uncertainties associated with such information and expectations;
- c) Information used for risk management activities should be timely, clear, and available to relevant stakeholders;
- d) There should be constant collection, analysing, reviewing, updating, and reporting of the information on risk and risk management systems to facilitate continuous improvement; and
- e) Decision makers should consider, any limitations of the data or assumptions used or the possibility of divergence among experts.

#### *ii. Takes into Account Human and Cultural Factors*

Human behaviour and culture significantly influence all aspects of risk management at each level and stage.

- a) Risk management activities in PSEs should recognize the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organization's objectives;
- b) PSEs should strive to create a risk-supportive culture that recognizes uncertainty, supports considered risk-taking and embeds risk management into day-to-day activities;
- c) PSE should support open sharing of risk information and discussion among staff without fear of retribution, and provide learning opportunities to internal stakeholders; and

- d) Risk seekers and risk-takers should be challenged to create and protect PSE value through risk management.

### iii. *Continually Improved*

PSEs should make sure that:

- a) Risk management initiatives are continually improved through learning and experience.
- b) Each PSE develop and implement strategies to improve their risk management maturity through review of their framework and application of results of monitoring, external reviews, and learning.
- c) Monitoring activities such as assurance, routine data collection, incident investigation, and root cause analysis and performance reviews should be put in place to identify areas of improvement and to develop an annual risk management plan.

## 3.3 Develop and Document a Risk Management Framework

The development of a risk management framework involves the following key aspects:

- i. Understanding the key components of a risk management framework;
- ii. Key considerations by ISO 31000:2018 for developing a risk management framework; and
- iii. Specific procedures from designing and documenting key components of a risk management framework.

Each of these aspects are given detailed explanations in the following sub-sections:

### 3.3.1 Key Considerations for Integrating Risk Management Framework

The framework part of the ISO 31000 provides the “how part” of integrating risk management in an organization. As shown in Figure 2, the framework includes six (6) components:



Figure 2: Key Considerations for Developing Risk Management Framework (ISO 31000:2018)

Each of the components is given more explanation in the next sub-sections, including guidance on how PSEs can put them into practice.

*i. Leadership and Commitment*

Success of risk management is highly dependent on the support and tone set at the top of the PSE.

Top management and oversight bodies, where applicable, should ensure that risk management is integrated into all PSE activities.

Top management and oversight bodies should demonstrate leadership and commitment by:

- a) Customizing and implementing all the components of the framework.
- b) Formulating and issuing a risk management policy<sup>3</sup> that formally communicates the PSEs commitment to managing risks, and that charges official and other staff with the responsibility to manage risks areas of their responsibilities.
- c) Ensuring necessary resources (financial, human, tools etc.) are allocated for risk management coordination and proposed risk mitigations.

<sup>3</sup> See Section 3.3.2 on how to formulate of risk management policy.

- d) Assigning risk management authority, responsibility, and accountability at appropriate levels within the PSE.

## *ii. Integration*

Risk management should be a part of, and not separate from, the organizational purpose, governance, leadership and commitment, strategy, objectives, and operations.

The following are key areas that PSEs should do to have an integrated risk management:

- a) Risk management roles and responsibilities should be assigned to all levels of the PSE, including top management, oversight bodies, and all other staff involved in risk management<sup>4</sup>;
- b) The assigned roles and responsibilities must be aligned with the existing organizational structure to avoid conflicting roles and responsibilities across the PSE and within different levels;
- c) Develop the necessary procedures/guidelines for carrying out risk management activities in the PSE;
- d) Align risk management plans and activities with PSE cycle of events, including planning, budgeting, reporting, and meeting calendars;
- e) Identify and evaluate all risks against PSE objective and prepare risk registers, risk mitigation actions plan, reports; and
- f) Monitor the implementation of risk management process and continually review the outcomes for improvement.

## *iii. Designing*

In designing the framework for managing risk, the PSE should examine and understand its external and internal context.

Further, management and oversight bodies, where applicable, should:

---

<sup>4</sup> See Section II for indicative risk management roles and responsibilities of different organs in PSEs.

- a) Demonstrate and articulate their continual commitment to risk management through a risk management policy ([see sub-section 3.3.2](#)) that clearly conveys PSE's objectives and commitment to risk management;
- b) Ensure that the authorities, responsibilities and accountabilities for relevant roles with respect to risk management are assigned and communicated at all levels of the PSE;
- c) Ensure allocation of appropriate resources for risk management, which can include but not limited to people, skills, experience and competence and tools to be used for managing risks; and
- d) The PSE should establish an approved approach to communication and consultation to support the framework and facilitate effective application of risk management.

#### *iv. Implementation*

The PSE should implement the risk management framework by developing appropriate risk management plans, including:

- a. Time and resources for implementation of risk management plan and specific mitigations.
- b. Identifying where, when, and how different types of decisions are made across the organization and by whom.
- c. Modifying the applicable decision-making processes where necessary.
- d. Ensure that the PSE's arrangements for managing risk are clearly understood and practiced.

#### *v. Evaluation*

PSEs must make decisions on how the risk management framework performance will be monitored, measured, analysed, and evaluated. The following can be considered:

- a. Internal audit unit must include the audit of the risk management framework in their audit plans to provide assurance that the risk management activities conform to the requirements of the organization and is successfully implemented and maintained.
- b. Management to conduct periodical review to measure risk management framework performance against its purpose, implementation plans, indicators and expected behaviour.

- c. PSE should periodically conduct a self-assessment to measure the maturity of their risk management initiatives. It is recommended that PSEs should use a validated checklist for measuring their risk management maturity<sup>5</sup>.

#### vi. *Improvement*

The PSE should continually monitor and adapt the risk management framework to address the external and internal changes that will improve its value.

The PSE should continually improve the suitability, adequacy and effectiveness of the risk management framework and the way risk management process is integrated.

The PSE should monitor and review risk performance indicators to measure the contribution of risk management; report risk performance in line with obligations and monitor improvement.

As relevant gaps or improvement opportunities are identified, the PSE should develop plans and tasks and assign them to those accountable for implementation. Once implemented, these improvements should contribute to the enhancement of risk management.

Every PSE should provide regular training to its staff on risk management to ensure adequate risk management competence is achieved and maintained. Refer to [Section V – is dedicated for monitoring the effectiveness of risk management framework](#).

### 3.3.2 Formulate Key Components of the Risk Management Framework

According to ISO (2018), the risk management framework includes the context, policies, resources, process, organizational structure, and techniques necessary to implement risk management. The above-mentioned components must be documented; especially those, which set the risk management policy, risk appetite or tolerance levels, roles and responsibilities, and procedures.

Sub-sections below give guides and template for the formulation of the following components:

- i. Risk management policy;
- ii. Risk management roles and responsibilities; and

---

<sup>5</sup> For example the OECD Risk management capability maturity model available at <https://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/analytics-maturity-model.pdf>

- iii. Risk management procedures.

### 3.3.2.1 Risk Management Policy

A risk management policy sets out the PSE's risk strategy and communicate issues like the PSE's overall commitment, attitudes, intentions, and direction related to risk management.

PSE must formulate and document a risk management policy, which should clearly articulate the organization's objectives for and commitment to its risk management initiatives.

The policy typically should specify three important aspects of risk management:

- i. *The purpose*: for adopting risk management.
- ii. *Policy statement*, which will highlight the PSE's acknowledgement of risk being inherent in their activities and commitment towards risk management.
- iii. *Risk management principles, which the PSE adopts*, the principles should be in line with those provided by the ISO 31000:2018 and added with specific principles that align with the PSE context.

[Template 1](#) illustrates a sample of risk policy statement.

- iv. *Risk Appetite Statements*

Risk appetite is defined as the level of acceptable risk or risks the organization is willing to take in pursuit of its strategic goals and objectives. The PSE's appetite for and tolerance of risk, when outlined in the Risk Appetite Statement, form the basis of the PSE's approach to managing risk in its day-to-day activities.

The following considerations should be observed when formulating the risk appetite statements:

- a) Risk appetite is set by those charged with governance of the PSEs i.e., the Board (where applicable) or the Accounting Officer;
- b) Individual risk appetite statements are usually structured to reflect the main sources or categories of risks that the PSE faces (e.g., strategic, marketplace, compliance, reputational, environmental, and technical/ IT, financial etc.);

- c) Given the different levels of appetite on each source/ category of risk, it is again required that a PSE indicate the exact appetite level for each category of risk that it is willing to accept ([see Template 2](#)); and
- d) After formulating the appetite statement, the PSE should communicate the draft risk appetite statement(s) to key stakeholders, especially the Governing authority and Audit Committee (where applicable) for validation and approval before implementation.

### 3.3.2.2 Risk Management Roles and Responsibilities

Risk management structure (also termed as risk governance structure or risk architecture) outlines the different roles, responsibilities, communication, and reporting structure within the PSE. It is important for everyone in the PSE to be aware of individuals and collective risk management responsibilities.

As earlier given in [Section 2](#), depending on the structure of the PSE, design a risk governance structure that defines appropriate risk management roles and responsibilities of officials and all staff including, but not limited to

- a) The Board/Council (where applicable);
- b) Accounting Officer;
- c) Audit Committee/Risk Oversight Committee;
- d) Risk Management Coordinator;
- e) Executive Management (Top management);
- f) Risk owners; and
- g) Other staff, contractors, and stakeholders.

The risk architecture can be represented diagrammatically as a means of identifying the committees and officials with risk management responsibilities and the reporting relationships between them. See the following templates for sample:

- a) [Template 3](#) - Risk management governance structure in Ministries;
- b) [Template 4](#) – Risk management governance structure for LGAs; and
- c) [Template 5](#) - Risk management governance structure for Independent Departments, Agencies, and Parastatals.

It is understood that PSEs have different structures; hence, each should customize the diagrams according to PSEs structure.

### 3.3.2.3 Risk Management Procedures

Risk management procedures provides guidelines, rules, methodologies, and tools that should be used when implementing risk management activities in the PSE.

A PSE should write down specific procedures that should be followed in carrying out risk management activities.

In developing the risk management procedures, a starting point should be a risk management process by ISO 31000:2018 as explained [Section IV](#) of this document.

The procedure document should at least, include the following:

- i. *Risk management definitions/language* – a common risk language will produce consistent understanding of risk management concepts and provide clarity of communication and action.
- ii. *Relationship and integration with other initiatives* – risk management is not a stand-alone discipline. In order to maximize risk management benefits and opportunities, it needs to be integrated with existing business processes (e.g., strategic planning, budgeting and reporting).
- iii. *Description of how each step of the risk management process will be applied within the organization* – a PSE’s risk management framework and processes must meet the minimum key principles of the ISO 31000:2018.
- iv. *Overview of the PSE’s risk reporting framework* – content, format, frequency and recipients of risk reports.
- v. *Risk assessment criteria* – agreed criteria for assessment of risk likelihood, consequence, and overall risk rating.

## 3.4 Compile the Risk Management Component into a Risk Framework Document

All the above steps should result into documented risk management policy, risk governance structure, and risk management procedures.

These components should be combined into a single document termed as “The Risk Management Framework Document” of the PSE. In its complete state, the document will have the following minimum chapters/sections:

- i. *Section 1*: Introduction (background, purpose, legal issues, scope, and document structure);
- ii. *Section 2*: The Risk Management Policy (risk policy statement, risk appetite statements, and risk management principles);
- iii. *Section 3*: Risk Management Governance Structure (roles and responsibilities in risk management of various organs and officials);
- iv. *Section 4*: Risk Management Procedures (rules, methods, and approach in conducting risk assessment, treatment and reporting); and
- v. *Annex*: Risk Management Templates (samples of key documents/forms/and sheets).

[Template 6](#) illustrates a typical outline of a Risk Management Framework document.

#### 3.4.1 Get Approval of the Document from Top Levels of the PSE

Given its importance and strategic nature, risk management requires strong and sustained commitment by the PSE's board, audit/risk committee, and the Accounting Officer.

Depending on structure of the PSE, the approval process should follow the same pattern and should go along the same lines of approving new policies and frameworks.

It is recommended that before initiating the approval process, the key stakeholders (e.g., Top Management, Council, and Board, whichever is applicable) should be given a brief awareness about risk management and the position of the document they are to approve.

The approval process should result into the official signing of the Risk Management Framework by the approving/authenticating authority or official.

#### 3.4.2 Create Awareness and/ or Build Capacity of Key Stakeholders

PSE should provide training so that to create awareness, sensitize and build basic capacity for risk management.

Training needs to be provided to board/council members, audit committee, director, managers, staff and other stakeholders.

Managers and staff need to be encouraged to comment on risk management procedures that the organization is adopting, so that they may be improved further as part of the learning culture within the organization.

The following could be the indicative training that may be provided to different stakeholders:

*Table 1: Indicative List of Workshops to Provide on Risk Management*

<b>Workshop Type</b>	<b>Target Group</b>	<b>Purpose</b>	<b>Comments</b>
Orientation on risk management and Risk Management Framework	Board/Council Members (depending on the type of PSE)	To create awareness on risk management  To obtain Board - level sponsorship  To review/approve the Risk Management Framework.	While the purposes could be combined (i.e., orientation, review and approval), the best option could be to have a separate session for:  Board/Council sensitization and review of Risk Management Framework  Approval of Framework could be done in normal Top Management/ Board meetings.
Top-Level Awareness on Risk Management and Review of Risk Management Framework	Audit Committee/Risk Oversight Committee  Top Management	To create awareness on risk management  To obtain top-level sponsorship and ownership of the Framework  To review and approve the Risk Management Framework.  To appoint Risk Management Committee	Top Management and Audit Committee need to review and make improvement on Framework and Risk register and appoint risk committee.  This is to prepare the Framework for Board/Council approval.

Workshop Type	Target Group	Purpose	Comments
Middle-level and operating staff awareness on Risk Management and Practical Risk Assessment	Top management Middle level Management Audit/Risk Committee Key Staff/Stakeholders	To provide orientation of risk management,  To review and refine the Risk Management Frameworks  Provide basic skills in risk management.  To conduct a Risk Assessment for developing a Risk Register.	This is the most important group because it will be involved in the practical development of the risk management framework and risk register.

## SECTION IV

---

### 4 IMPLEMENTING THE RISK MANAGEMENT PROCESS

#### 4.1 Introduction

Implementing the risk management process means carrying out all the procedural components of the risk management framework, especially by conducting the risk assessment exercise for preparation of the Risk Register and related mitigation action plans.

The section therefore gives guidance on the following areas:

- i. Preparation of a risk management annual plan;
- ii. Aligning the risk management process with the PSE's planning and budgeting process;
- iii. Conducting the risk management process (as per the ISO 31000: 2018); and
- iv. Reporting the implementation of risk mitigations and progress.

#### 4.2 Prepare Annual Plan for Risk Management Activities

A risk management plan details the steps necessary to establish, implement or improve a PSE's risk management capabilities. At the annual level, the plan will ensure that activities occur in a coherent order, and it provides a means of recording progress and tracking improvement.

- a) The risk management plan should set out on how to implement risk management framework and policy;
- b) The focus of the plan should be to integrate risk management into PSE's management systems;
- c) The plan should be simple, but should clearly outline the activities associated with pursuing the risk management strategy;
- d) It should include topics like:
  - i. The scope and objectives of the plan;

- ii. A description of how risk management activities support the pursuit of the organization's objectives;
  - iii. An outline of roles and responsibilities of relevant oversight committees, governing bodies and key stakeholders and the expectations and responsibilities for each of these groups;
  - iv. Timeframes for risk management activities;
  - v. Resourcing requirements (e.g., finances, people, IT, and physical assets);
  - vi. Capacity building and risk management training and other support activities that will be necessary to integrate risk management;
  - vii. Performance measures; and
  - viii. The review processes.
- e) Engaging a broad group of stakeholders, with diverse responsibilities in developing the plan, can provide a more comprehensive view of the desired outcomes and encourage better adoption;
- f) The plan should be tabled in Risk Committee of the Management and approved by the Audit Committees, as appropriate;
- g) PSE should regularly monitor progress against the plan. The top management or governing body, as appropriate must approve any changes to PSE's risk management plan;
- h) [Template 7](#) provides a sample outline of an Annual Risk management Plan. PSEs are encouraged to develop their own format so that it fits with planning formats adopted.

#### 4.3 Align the Timing of Risk Assessment Process to PSE Planning Process

Since the purpose of risk management is to deal with the uncertainty associated with the achievement of objectives, there is an intrinsic link between planning, budgeting and risk management.

- a) In this case, the risk assessment process must be embedded into strategy development and planning process.
- b) Depending on the size and complexity of PSE, such plans may include:
- i. PSE's strategic plan.
  - ii. Functional plans, such as those for human resource management, asset management, financial management.

- iii. Activity plans, such as those for procurement, communications, information management, work health and safety, etc.
  - iv. Divisional business plans, such as service delivery plans.
  - v. Project plans, and
  - vi. Individual work plans.
- c) The extent of such linkage depends on the level chosen to conduct the risk management process in the PSE (e.g., at strategic, functional, project or operation levels).
- d) If a PSE develops an integrated hierarchy of plans and risk assessments, it can optimize the benefits of both planning and risk management, which can help ensure risks are managed at the appropriate level in PSE.
- e) The best way to do it is to conduct both the strategic planning process with the risk assessment process as a parallel exercise, such that when strategic objectives and their implementing strategies and activities are formulated, the respective risks to those objectives are also identified, assessed and treatment/mitigation activities are planned along with strategy implementation activities.
- f) For annual planning, the same approach should be to have a risk assessment exercise conducted alongside the Annual Action Plan or MTEF, such that risk mitigations are budgeted along other operational activities.
- g) The result is that the PSE budget should include fund allocation for all the risk mitigations reflected in the Risk Mitigation Action Plan (See [Section 4.5](#)).

#### 4.4 Implement the Risk Management Process

The risk management process is conducted by carrying out procedures as stipulated in procedure section of PSE's Risk Management Framework, which are also in line with the ISO 31000:2018 risk management process. The focus of risk management process is ensuring that controls for each of the identified risks are appropriate, work effectively, and provide assurance that the risks are kept within the tolerable levels.

As indicated in Figure 3, the risk management process includes the following key aspects:

- i. Communication and consultation with stakeholders;
- ii. Definition of scope, context, and criteria of risk assessment;
- iii. Conducting the risk assessment exercise;

- iv. Planning and implementing risk treatments/ mitigations;
- v. Recording and reporting; and
- vi. Monitoring and review the performance of risk management.

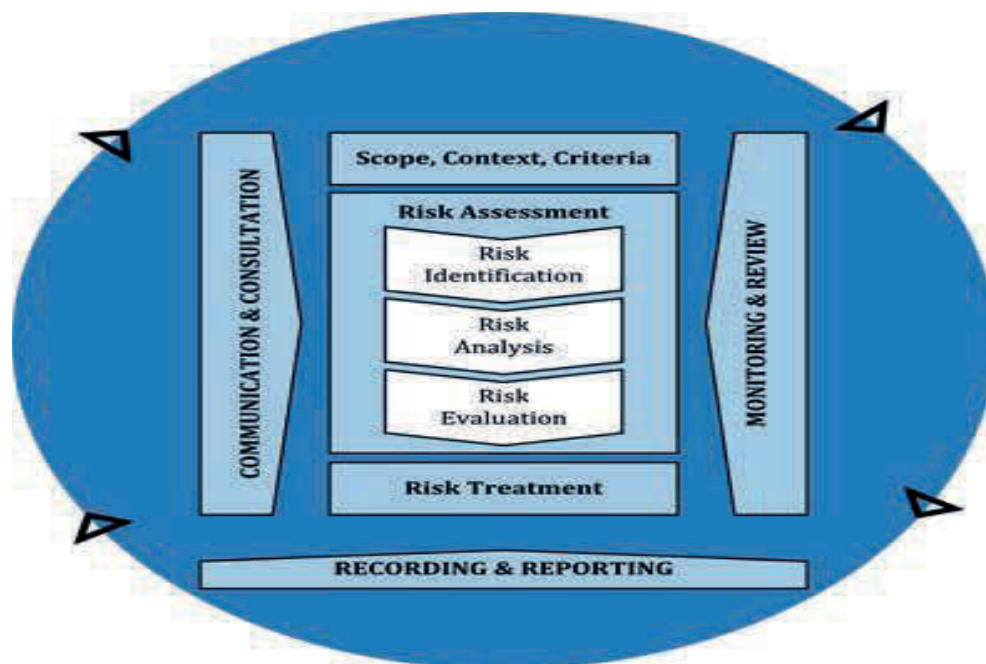


Figure 3: Risk Management Process (ISO 31000:2018):

#### 4.4.1 Communicate and Consult with Stakeholders

PSE should take an inclusive approach to risk management by communicating and consulting internal and external stakeholders in identifying risks and gaining acceptance and active support for decisions about the significance and treatment of risks.

When considering communication issues, the following can be potential objectives:

- a) Building awareness and understanding about a particular issue;
- b) Learning from stakeholders;
- c) Influencing the targeted audience;
- d) Obtaining a better understanding of the context, the risk criteria, the risk, or the effect of risk treatments;
- e) Achieving an attitudinal or behavioural shift in relation to a particular matter; or
- f) Any combination of the above.

In communicating and consultation with stakeholders, PSEs should consider the following:

- a) Internal and external stakeholders are to be identified, and plans made on how to communicate and consult with them. This occurs at the start of the process and at appropriate points throughout;
- b) Communication and consultation with internal and external stakeholders should take place at each step of the risk management process, as far as necessary;
- c) Since the views of stakeholders can have a significant impact on the decisions made, it is important that their perceptions of risk be identified, recorded, and integrated into the decision-making process;
- d) The following questions can assist in determining effective and efficient stakeholder consultation<sup>6</sup>:
  - i. Were appropriate internal and external stakeholders identified before the risk management process began?
  - ii. Were the right stakeholders appropriately engaged at each stage of the process?
  - iii. Were any additional stakeholders identified throughout the risk management process?
  - iv. Which stakeholders were consulted throughout risk assessment and treatment?
  - v. Was there communication with appropriate stakeholders throughout?
  - vi. Were the outcomes of the decision or risk management process appropriately communicated? and
  - vii. Were the outcomes required by the stakeholders considered?
- e) During the risk identification process, and depending on the type of the PSE, the main types of stakeholders may include:
  - i. Risk owners (directors, heads of departments and units);
  - ii. Risk champions;
  - iii. Key staff from across the entity;

---

<sup>6</sup> ISO 31000:2018 | Risk management – a practical guide.

- iv. External stakeholders (where necessary) who are considered crucial to risk mitigation, especially from entities linked activities of the PSE.

It should be decided in advance, on how the outputs and outcomes of risk assessment are to be reliably, accurately and transparently communicated to relevant stakeholders, especially those external to the PSE.

#### 4.4.2 Define Scope and Context of Risk Assessment

The aim of this step is to provide a comprehensive appreciation of all the factors that may have an influence on the ability of PSE to achieve its intended outcomes, and to ensure better utilization of time, effort, and resources when conducting the risk management process.

- a) Scope of risk management activities, which can be strategic, Operational, program, project or other activities. The scope should be clear, thus, relevant to objectives and alignment of the PSE objectives;
- b) Context of risk management involves understanding the background of the PSE and its risks, then scoping the risk management activities being undertaken, and developing a structure for the risk management tasks to follow. It may also include defining the stakeholders, community involved, and the types of events addressed; and
- c) Sources of information for defining the scope and context of risks assessment include interview/discussion with members of the PSE management, and review of documents, including PSE's strategic plan, budget, directives, internal and external auditor's report, and the respective institutional legal framework;
- d) The outcome is a concise statement that summarizes the following about the PSE:
  - i. Brief information about the entity e.g., sector, mission, vision, core values, and legal context;
  - ii. List of strategic objectives and their specific key performance indicators (criteria for success);
  - iii. The objectives and scope for risk management (and legal/ compliance requirements for risk management);
  - iv. A list of key stakeholders who would need to be involved in risk management assessment process and risk communications; and
  - v. Definition of risk categories or main sources of risks (see [Template 8](#)); criteria for risk rating (See [Sub-section 4.4.3](#)); and risk tolerance levels ([Section 4.4.4](#)) to be used when assessing and prioritizing risks.

### 4.4.3 Define Risk Assessment Criteria

Risk criteria are rules to enable a consistent decision-making on risks, especially in determining the scale to measuring the two dimensions of risk, namely: impact and likelihood.

- a) Assessment scales for impact and likelihood enable the rankings, prioritization, and comparison of risk across the PSE and benchmark them to the risk tolerance levels;
- b) The risk criteria should be established at the beginning of the risk management process and used to evaluate the significance of different types of risks to support decision-making processes; and
- c) A PSE may choose to use either a three-point scale or a five-point scale band. However, a five-point scale has been widely judged to yield better dimensions than three-point scales<sup>7</sup>.

#### 4.4.3.1 Impact

Impact (or consequence) refers to the extent to which a risk event might affect the PSE.

- a) Impact assessment criteria may include financial, reputational, regulatory, health, safety, security, environmental, employee, customer, and operational impacts;
- b) PSEs should define impact using a combination of these types of impact considerations (as illustrated on Table 2), given that certain risks may affect the enterprise financially while other risks may have a greater impact to reputation or health and safety; and
- c) PSEs are to develop either their own ratings criteria or modify the provided illustration. This is true, especially for financial related ratings, which differ from one PSE to another.

Table 2 provides an illustrative scales and criteria for judging the impact of a risk for a 5-point scale.

---

<sup>7</sup> COSO (2012) Risk assessment in practice.

Table 2: Illustrative 5-point Scale for Assessing Impact of a Risk (COSO, 2012)

Rating	Descriptor/ color	Definition
5	Extreme (Very High)	<ul style="list-style-type: none"> <li>Financial loss of TZS X million or more<sup>8</sup>.</li> <li>International long-term negative media coverage; game-changing loss of market share</li> <li>Significant prosecution and fines, litigation including class actions, incarceration of leadership.</li> <li>Significant injuries or fatalities to employees or third parties, such as customers or vendors</li> <li>Multiple senior leaders leave.</li> </ul>
4	Major (High)	<ul style="list-style-type: none"> <li>Financial loss of TZS X million up to TZS X million</li> <li>National long-term negative media coverage; significant loss of market share</li> <li>Report to regulator requiring major project for corrective action.</li> <li>Limited in-patient care required for employees or third parties, such as customers or vendors.</li> <li>Some senior managers leave, high turnover of experienced staff, not perceived as employer of choice</li> </ul>
3	Moderate	<ul style="list-style-type: none"> <li>Financial loss of TZS X million up to TZS X million</li> <li>National short-term negative media coverage</li> <li>Report of breach to regulator with immediate correction to be implemented.</li> <li>Out-patient medical treatment required for employees or third parties, such as customers or vendors.</li> <li>Widespread staff morale problems and high turnover</li> </ul>

<sup>8</sup> Financial impact is typically measured in terms of loss or gain, profitability or earnings, or capital. This measure varies from PSE to PSE depending on their financial materiality.

Rating	Descriptor/ color	Definition
2	Minor (Low)	<ul style="list-style-type: none"> <li>Financial loss of TZS X million up to TZS X million</li> <li>Local reputational damage</li> <li>Reportable incident to regulator, no follow up</li> <li>No or minor injuries to employees or third parties, such as customers or vendors.</li> <li>General staff morale problems and increase in turnover</li> </ul>
1	Incidental (Very Low)	<ul style="list-style-type: none"> <li>Financial loss up to TZS X million</li> <li>Local media attention quickly remedied.</li> <li>Not reportable to regulator</li> <li>No injuries to employees or third parties, such as customers or vendors</li> <li>Isolated staff dissatisfaction.</li> </ul>

#### 4.4.3.2 Likelihood

Likelihood represents the possibility that a given event will occur. The likelihood of a risk may be assessed using two scenarios, either:

- Basing on the annual *frequency* of happening; or
- Basing on judgement of *possibility* of happening.

Table 3 provides an illustration for the scales and criteria for assessing the likelihood of a risk happening. PSEs may develop either their own ratings criteria for likelihood or modify the provided illustration to fit with their internal context.

Table 3: Illustrative 5-point Scale Likelihood of Risk (COSO, 2012)

Rating	Annual Frequency		Probability	
	Descriptor	Definition	Descriptor	Definition
5	Frequent (Very High)	Up to once in 2 years or more.	Almost certain (Very High)	90% or greater chance of occurrence over life of asset or project.

Rating	Annual Frequency		Probability	
	Descriptor	Definition	Descriptor	Definition
4	Likely (High)	Once in 2 years up to once in 25 years.	Likely (High)	65% up to 90% chance of occurrence over life of asset or project.
3	Possible (Moderate)	Once in 25 years up to once in 50 years.	Possible (Moderate)	35% up to 65% chance of occurrence over life of asset or project.
2	Unlikely (Low)	Once in 50 years up to once in 100 years.	Unlikely (Low)	10% up to 35% chance of occurrence over life of asset or project.
1	Rare (Very Low)	Once in 100 years or more.	Rare (Very Low)	<10% chance of occurrence over life of asset or project.

#### 4.4.3.2 Set Risk Tolerance Levels

Risk tolerance levels determine the amount (and type) of risk that a PSE may or may not take relative to its objectives.

To tolerate a risk does not mean that the PSE regard the risk as negligible, rather as something that need to be kept under review and/or seek possibilities to reduce the risk further, where possible.

In setting risk tolerance levels, PSEs can use either one of both of the following:

- i. Risk rate obtained by multiplying impact and likelihood of the risk (see Table 4); or
- ii. Risk appetite for a given risk category (see [Template 2](#)).

When risk rate is used for setting the risk tolerance level, a PSE may use guidance given in Table 4 to determine levels of risk tolerance.

*Table 4: Risk Ratings and Colour Status to Guide Risk Tolerance Levels*

Risk Rate/ Status (Impact x Likelihood)	Description of Tolerance Criteria	Risk Tolerance

Increasing Risk ↑	<b>15-25</b>	Not willing to accept risks, threats, opportunities under any circumstances. All reasonably practicable measures to eliminate the risk must be taken.	<b>No Tolerance/Extreme (Unacceptable)</b>
	<b>10-14</b>	Safe approaches should be taken, but the cost of controls / mitigation should be carefully evaluated to ensure they achieve a reasonable outcome. A strong preference for strategies and plans that present minimal risk.	<b>Cautious/High</b> <i>“OK to proceed, but only if the likelihood and consequence of the risk can be managed at reasonable cost”.</i>
	<b>5-9</b>	Can accept a degree of uncertainty to achieve an intended outcome providing that effective measures be in place to monitor the risk and limit adverse outcomes.	<b>Tolerable / Conservative/Moderate</b> <i>“OK to proceed, providing that losses can be minimized”.</i>
	<b>1-4</b>	Comfortable for risks to be taken even if there is a high degree of uncertainty to gain highly valued reward/s.	<b>Acceptable/Negligible</b> <i>“OK to proceed, even if ability to minimize potential losses is limited”.</i>

The following details explains each of the groups in the above table:

- a) **Red region** (15 to 25) = Unacceptable/ Intolerable risks, where the PSE will use all reasonably practicable measures to eliminate the risks;
- b) **Light brown region** (10 to 14) = Cautiously taken risks, where the safe approaches should be taken but cost of mitigation be used to reduce to be *As Low As Reasonable Possible (ALARP)*;
- c) **Yellow region** (5 to 9) = Tolerable risks, where the PSE can accept a degree of uncertainty to achieve and intended objective, effective measures are in place against the risks; and

- d) **Green region** (1 to 4) = Acceptable risks, where existing mitigations are considered effective, and the PSE will proceed with activities.

As a point of reminder, most of the risk criteria for measuring risks (i.e., rates for impact and likelihood) and tolerance levels should also be stipulated in the procedure section of the PSE's risk management framework (see [Section 3.3.2.4](#)).

#### 4.4.3.3 Conduct Risk Assessment

Risk assessment involves three stages namely: risk identification, risk analysis, and risk evaluation.

The remaining section gives detailed explanations of the three stages of risk assessment process. The explanations are arranged into the following aspects:

- i. Timing for risk assessment;
- ii. Choice of approach for conducting the risk assessment exercise;
- iii. Risk identification exercise;
- iv. Analysing risks; and
- v. Evaluating risks.

It should be noted that, the first two sets of activities are not indicated in the risk management ISO 31000:2018 risk management process, they are however considered crucial for guiding the actual implementation of the risk assessment exercise.

#### 4.4.3.4 Align Timing of Risk Assessment with the Planning Process

It is prudent, before embarking on the risk assessment exercise, to decide on overall approach on which to conduct the exercise. Key aspects that must be considered include when to conduct the risk assessment; which stakeholders to engage; and risk assessment methods and tools to use.

Risk management, as it has typically been practiced, has helped many organizations identify, assess, and manage risks to the strategy<sup>9</sup>.

- a) It is therefore crucial that, at PSE level there is alignment of timing between strategy, objective-setting, risk management and budgeting;

---

<sup>9</sup> COSO (2017) Enterprise Risk Management – Integrating with Strategy with Performance: Executive Summary.

- b) The proper timing there is to conduct the risk assessment exercise just after setting objectives but before preparation of the PSE Annual Action Plan and Budget. This is to provide an opportunity for risk mitigations to be accommodated in the Annual Action Plan and Budget; and
- c) In addition, if the risk assessment process is done for projects or strategic decisions should as well be timed such that risks are considered before a decision is reached.

#### **4.4.3.5 Choose Appropriate Risk Assessment Method**

The specific approach to be used will depend on the nature of the activities under review, and types of risks:

- a) Team-based brainstorming in a form of a facilitated workshop is a preferred approach as it encourages commitment, considers different perspectives, and incorporates differing experiences;
- b) For less clearly defined situations, such as the identification of strategic risks, processes with a more general structure, such as 'what-if' and scenario analysis could be used; and
- c) It is critically important during this step to understand the cause-effect relationships between a risk, its causes, and the potential consequences should the risk occur.

A PSE may consider the use of an external facilitator to assist in the risk assessment process and the development of resultant risk register and mitigation action plans. However, the use of a facilitator should be opted where internal capacity is limited or there is a need to have an independent person to oversee the exercise.

#### **4.4.3.5 Identify Risks against Objectives**

The objective of risk identification is to generate a comprehensive list of risks based on those events and circumstances that might affect (i.e., enhance, prevent, degrade or delay) the achievement of a given objective.

It is therefore important to follow the following pattern of events, namely:

- a) Agreement on a working definition of risk;
- b) Agreement on a set of objectives on which to base the risk identification; and
- c) Generate a comprehensive list of risks on each of the objective.

#### **4.4.3.5 Agree on the Definition of Risk to Use**

Since risk, to many people, mean differently it is advised that before starting the identification of risks an agreement should be reached among the participants/stakeholders on definition of risk to be used.

- a) Risk assessment workshops or process should provide a clear meaning of *what is risk*;
- b) If the PSE is to adopt a definition by ISO 31000:2018, which define risk as “the *effect of uncertainty on objectives*”, more explanations should be given to clarify the definition. The focus for clarification should be on linking risk, uncertainties, and impact to objectives; and
- c) A comparison can be made of two or more definitions from internationally recognized models (e.g., COSO, ISO and IRM) and make the participants to agree on one as a working definition.

#### 4.4.3.6 Agree on a Set of Objectives on which to Identify Risks

While business objectives put strategy into practice, the same objectives serve as a basis for identifying, assessing, and responding to risk<sup>10</sup>.

- a) For the purpose of risk identification, the said objectives could be those linked to either the strategic plan, project, or a major strategic decision to be made;
- b) In this case, before the identification of risks, it is important to obtain a list/set of objectives that will be used in identifying the risks; and
- c) Again, a decision must also be made on level/ hierarchy of risk identification, i.e., whether risks will be identified on strategic objectives, or lower level at targets, or even division level.

The members of staff from a unit responsible for planning can be very useful in orienting the risk identification team on how the objectives are structured in the strategic plan.

#### 4.4.3.6 Generate a List of Risks for Each Objective

Risks should be identified for each of the objectives listed. A good starting point is to base the risk identification on asking a set of questions aimed at ascertaining potential uncertainties facing the achievement of a given objective.

*What is the event that, if it happened, could affect your objectives?*

More questions:

- a) What events, conditions, or situations might affect the achievement of the objective?
- b) What uncertainty exists and what its effects might be? or
- c) What has happened in the past and how this might reasonably relate to the future?

---

<sup>10</sup> COSO (2017) Enterprise Risk Management – Integrating with Strategy with Performance: Executive Summary

The team may use historical information about PSE and then discussions with a wide range of stakeholders about historical, current and evolving issues.

The risk identification process should include all risks, whether or not PSE has control over them or not.

The output from risk identification can be recorded as a list of risks against each objective.

[Template 8](#) gives a sample of risks. Further, [Template 9](#) provides a guiding factor to consider in wording for identified risk.

#### **4.4.4 Analyse the Risks**

The objective for the risk analysis stage is to establish the nature and characteristics of risk, including the level of risk, consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur.

This stage provides inputs to decisions on whether risks need to be treated or not and the most appropriate and cost-effective risk treatment strategies.

The following key consideration must be taken when analysing risks:

- a) Categorizing the identified risks;
- b) Determining causes and consequences of the risks;
- c) Rating the impact and likelihood of the inherent risk;
- d) Documenting existing mitigation/controls and their weaknesses; and
- e) Rating the impact and likelihood of the residual risk.

##### *(a) Categorize the Identified Risks*

The analysis of risks should also include a proper categorization of risks into groupings that align to the categories indicated in the risk appetite statement ([See Template 2](#)).

Categorization of risks helps with understanding the nature of risk and comparing the risk with PSE's risk appetite for a given category of risk, which will trigger specific decision for mitigation in line with risk appetite.

##### *(b) Establish Risk Causes and Consequences*

A cause indicates a factor that is associated with a given outcome. The cause to the risk makes the uncertain event happen and affect the objective. Understanding the cause to the risk helps the design of mitigations.

Sources of risk can include events, decisions, actions, and processes, both favourable and unfavourable, as well as situations that are known to exist but where outcomes are uncertain.

It is crucial that causes and sources of risk are identified because they can be used to:

- a) Estimate the likelihood of an event or consequence;
- b) Identify treatments that will modify risk;
- c) Determine early warning indicators and their detection thresholds; and
- d) Determine common causes, which can help, develop priorities for treating risk.

Depending on the type of risk, a risk can be associated with a number of different types of consequences (e.g., injury, environmental, reputation, loss of a given value, etc.).

When making a risk assessment all the possible consequences must be listed, or explained on how they affect the given objectives, or the PSE in general.

#### *(c) Assign Scores on Impact and Likelihood of Inherent Risks*

An inherent risk is the level of risk before control actions are taken to alter the risk's impact or likelihood.

- a) Rating the impact and likelihood of inherent risks should be based on ratings established in the risk assessment criteria discussed in [Section 4.4.3](#);
- b) PSE should therefore use the established rating criteria stipulated in the risk management framework, or agreed during risk assessment exercise;
- c) Rating of impact and likelihood of risks is usually a matter of experience and consultation;
- d) Where no reliable or relevant past data is available, subjective estimates may be made which reflect an individual's or group's degree of belief that a particular event or outcome will occur; and
- e) When determining, the overall risk rating you will need to use the predetermined rates for impact and likelihood (for example in Table 2 and Table 3) [in Section 4.4.3](#).

### (d) Identify and Evaluate Effectiveness of Existing Controls

A control is something an organization is currently doing to “modify” a risk<sup>11</sup>. It is what is *currently in place* to reduce risk within an organization and/or an industry.

Control effectiveness is the term used to describe how well a control is reducing or managing the risk it is meant to modify.

The purpose of a control is to reduce one or both likelihood and impact of the risk.

Controls take many forms, including policies, procedures, practices, processes, technology, techniques, methods or devices that reduce a risk.

As given in Table 5, when evaluating the effectiveness of your controls, it is helpful to use an agreed rating scale for all control testing to ensure consistency and common understanding.

*Table 5: Effectiveness of Controls, Colour Coding and Meaning*

Effectiveness	Colour code	Definition	Judgement %
Effective	Green	Controls eliminate or remove the source/root cause of the risk	=>80%
Partially-Effective	Yellow	Controls are in place but with minor weaknesses that need improvement to address the root cause/source	>40%
Ineffective	Red	Controls are ineffective or not in place to address the root cause/source of risk	=<40%

When judging the effectiveness of control against a risk the following should be considered:

- Whether the controls are in place, are capable of operating as intended, and are achieving the expected results;
- Whether there are shortcomings in the design of controls or the way they are applied;
- Whether there are gaps in controls;
- Whether there are factors, conditions, vulnerabilities, or circumstances that can reduce or eliminate control effectiveness including common cause failures;
- Whether controls themselves introduce additional risks; and

<sup>11</sup> VMIA (2021) Control effectiveness guide.

- f) A distinction should be made between controls that change likelihood, consequences or both, and controls that change how the burden of risk is shared between stakeholders.

The rating for each existing control/ mitigation should be done in the Risk Assessment Sheet (See [Template 9](#)).

#### *(e) Assign Scores on Impact and Likelihood of Residual Risks*

A residual risk is the rate of risk that remains when controls and other mitigating factors have been put in place.

- a) The idea for putting control is to eliminate or reduce some of the inherent risks compared to before any such control measures were implemented;
- b) The term *impact of risk control* is alternatively used to depict the effectiveness of control/ mitigation on reducing the inherent risk. Hence a mathematical formula: *Residual risk = Inherent risk – Impact of risk controls*;
- c) The targeted level of residual risk is a risk that is as low as reasonably practical;
- d) In assigning scores of the residual risk, consideration should be made of the effectiveness of existing control and mitigation action against the risk; and
- e) This implies that more residual risk will be remaining when existing controls are assessed as ineffective.

The rating for impact and likelihood of residual risk should be done in the Risk Assessment Sheet (See [Template 9](#)).

#### **4.4.5 Evaluate the Risks**

Risk evaluation involves comparing the residual risk's overall rate (i.e., impact x likelihood) against PSE's established risk tolerance criteria (see Table 4 of [Section 4.4.4](#)).

The main idea for this comparison of residual risk rate to the risk tolerance criteria is to determine the significance of the risk and whether additional action is required to reduce the risk.

The results of the risk assessment process must be well documented in the Risk Assessment Sheet ([See Template 10](#)).

##### **4.4.5.1 Prepare Risk Register**

The risk register is the main repository of all risks across the PSE. It enables to profile risks, monitor controls, and prioritize treatment actions. The risk register also facilitates standardized reporting of risks.

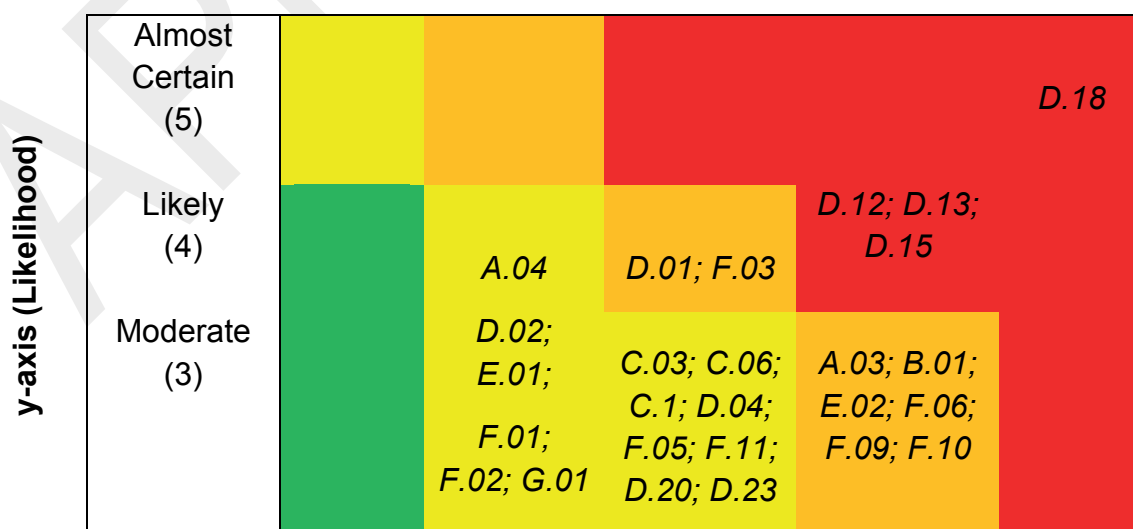
- a) A risk register is prepared by summarizing all risks from Risk Assessment Sheet (See [Template 10](#)) into a single spreadsheet (see [Template 11](#));
- b) In the spread sheet only ratings for residual risk are used and risks may be arranged by objectives, or departmental-wide; and
- c) Each risk should be given a unique ID, which may be formulated such that one can identify the risk against the objective, target or department it affects (e.g., risk D.03 for risk number 3 affecting objective D).

*(a) Plot Risks in the Risk Heat Map*

From the summary spread sheet it is possible to plot all the risks in a graph/matrix called the Risk Heat map, where ratings for impact are in the x-axis and those from likelihood are in the y-axis.

- a) The risk heat map can be included in one of the sections of the risk register as an added section to give an overall profile of risks across the PSE;
- b) The risk ID should be plotted in where the coordinates for impact and likelihood meet. This will automatically place the risk in the appropriate region in the Heat map; and
- c) In Table 6, for example, risk A.03 is having rates for impact x likelihood of 4 and 3, respectively. The risk falls in the high-risk region, hence requires further mitigations to lower the risk as low as reasonably practical.

*Table 6: Example of Risk Heat Map with Risks Plotted in the Three (3) Regions of Risk Tolerance*



Unlikely (2)	C.07; C.08; C.09; D.14; G.02	A.01; A.02; B.02; C.02; D.05; D.06; D.07			
Rare (1)					
	Low (1)	Minor (2)	Moderate (3)	Major (4)	Catastr ophic (5)
	<b>x-axis (Impact/ Consequences)</b>				

The following details explains each of the groups in Table 6:

- i. **Red region** (15 to 25) = Extreme risks. Unacceptable/Intolerable risks, where the PSE will use all reasonably practicable measures to eliminate the risks; However, considerations should be made to whether an entity intends to pursue the strategic objective or not since elimination may lead to relegation of pursuit of the respective objective;
- ii. **Light brown region** (10 to 14) = Significant risks. Cautiously taken risks, where the safe approaches should be taken but cost of mitigate be used to reduce to be *As Low As Reasonable Possible (ALARP)*;
- iii. **Yellow region** (5 to 9) = Moderate risks. Tolerable risks, where the PSE can accept a degree of uncertainty to achieve and intended objective, effective measures are in place against the risks; and
- iv. **Green region** (1 to 4) = Low risks. Acceptable risks, where existing mitigations are considered effective, and the PSE will proceed with activities.

#### *(b) Conduct Sanity Check of the Risks*

Once the initial risk profile has been developed, through the Risk Heat map, there is a need to conduct a “sanity check” i.e., to consider how each risk ranks in relation to the other risks.

- a) This step also allows to check if placed on the heat map have been rated correctly when compared to each other; and
- b) Possible outcomes of this step include:

- i. Re-assessment of the rating of some of the risks if it is felt that the overall spread of the risks relative to each other is not a true reflection of reality.
- ii. A recognition that some risks are similar to the other risks or are contributing factors to other risks. Hence, they may be incorporated into the risk description of other risks within the risk register.
- iii. A consideration of the interdependencies between the risks and consideration of the consequence to PSE if more than one risk occurred at the same time. This may result in changes to the overall risk ratings.

#### *(c) Develop Priority List of Risks*

The primary objective of evaluation is to prioritize risks. This helps to inform the allocation of resources to manage risks, both non-financial and financial considerations.

- a) The priority list can be categorized by a number of different criteria dependent on what is most relevant for PSE e.g., risk rating, functional area or by type of impact (i.e., strategic or operational). This will further refine the focus for risk treatment;
- b) From the priority list, it should be possible to create Top Risk List for PSE operational units and the entire entity; and
- c) The Priority list also makes it possible for the development of several important Risk reports for example, the Risk Profile, the Risk Treatment Action Plan, The Risk Management Annual Activity Schedule and the Detailed Risk Registers.

#### **4.4.6 Develop Risk Treatment Options and Mitigation Action Plans**

Risk treatment involves examining possible treatment options to determine the most appropriate action for managing a risk.

- a) The purpose of risk treatment is to select and implement options for addressing risk. A PSE should select, design and implement the most appropriate risk treatment options that support achievement of intended outcomes and manage risks to an acceptable level;
- b) Treatment actions are required where the current controls are not managing the risk within defined tolerance levels; and
- c) Treatment options could involve improving existing controls and implementing additional controls.

*a. Design Risk Mitigations based on Risk Causes and Weakness in Current Control*

The formulation of risk mitigation should focus on addressing the root causes of the risks and to correct identified weaknesses in current controls.

- a) A PSE should develop a range of options for mitigating risk, assess those options, and then preparing and implementing action plans; and
- b) The highest rated risks should be addressed as a matter of urgency.

*b. Choose Several Treatment Options to Modify the Risk*

Depending on the type and the nature of the risk, the PSE should choose one or several treatment options that modify the risk by:

- a) **Accepting (Tolerate/Retain):** No action is taken to change the severity of the risk. The risk treatment option appropriate when the risk to strategy and business objectives is ready within the risk criteria. Risk that is outside the PSEs risk criteria and that management seeks to accept will generally require approval from the governing body;
- b) **Avoiding (Terminate/Eliminate):** Action is taken to remove the risk, which may mean terminating the project, avoiding to expand the service to a new geographical region, abandoning a project/program, or privatising the entity. Choosing avoidance suggest that the entity was not able to identify a response that would reduce the risk to an acceptable level of severity;
- c) **Exploiting (Pursue):** Action taken that accepts increased risk to achieve improved performance. This may involve adopting more aggressive growth strategies, expanding operations, or developing new products and services. When choosing to pursue risk, management should understand the nature and extent of any changes required to achieve desired performance while not exceeding the boundaries of acceptable tolerance;
- d) **Mitigating (Reduce):** Action is to reduce severity of the risk. This involves any of myriad everyday business decision that reduces risk to an amount of severity aligned with the target residual risk profile and risk criteria;
- e) **Sharing (Transfer):** Action is taken to reduce the severity of the risk by transferring or otherwise sharing a portion of the risk. Common techniques include outsourcing to specialty service provider, purchasing insurance products and engaging in hedging transaction. As with reduce risk treatment, sharing risk lower residual risk in alignment with the risk criteria;

- f) Change the likelihood – undertake actions aimed at reducing the cause of the risk;
- g) Change the consequence – undertake actions aimed at reducing the impact of the risk; and
- h) When determining the preferred treatment option, consideration should be given to the cost of the treatment as compared to the likely risk reduction that will result (cost benefit analysis).

#### *c. Prepare Risk Treatment Action Plan*

On selecting the preferred treatment option, the following should occur:

- a) The cost of any actions should be incorporated into the relevant budget planning process;
- b) A responsible person should be identified for delivery of the action, with this expectation being communicated to them;
- c) A realistic due date should be set; and performance measures should be determined through Key Risk Indicator (KRI) and Key Control Indicator (KCI); and
- d) The Risk Treatment Action Plan in [Template 12](#) shall be used to guide the preparation of treatment plans. It shall be filled by each activity risk owner and then submitted to the Risk Management Office/Department for further processes.

### **4.4.7 Record and Report Risks**

#### **4.4.7.1 Record Risks**

Risk recording and reporting provide a benchmark to management and assurance to the stakeholders that there is documented and structured process of identifying and treating risks affecting PSE. The risk management process and its outcomes should be documented and reported through appropriate mechanisms.

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

##### **4.4.7.1.1 Record Risks in Risk Register and Risk Treatment Action Plans**

There should be a main repository to record all risks across the PSE, e.g., a risk register (see [Template 11](#)), Risk Treatment Action Plan (See [Template 12](#)) through paper-based spreadsheets or any Information System application designed for such purpose.

- a) The Risk Register eases to profile risks and the dissemination through the PSE and enables transparency regarding management of proposed treatments;
- b) As explained in the Risk Assessment (see [Section 4.4.5.5](#)), risk register should be developed for each objective or areas assessed and the following information included in the risk register supported by risk assessment as a minimum:
  - i. Objectives;
  - ii. Risk title and Risk ID;
  - iii. The description of the risk;
  - iv. Risk Category;
  - v. The causes and implication of the risk;
  - vi. The assigned risk owner;
  - vii. Details of the existing controls in place to manage the risk;
  - viii. The inherent risk rating determined from the assessment of the potential consequences and likelihood for the risk;
  - ix. Details of any proposed controls, including a due date for implementation;
  - x. The residual risk rating after consideration of the controls in place; and
  - xi. Regulated entities should include the register reporting requirements set out by the sector regulator.
- c) A Risk Treatment Action Plan helps to plan when to implement individual mitigations by showing implementation responsibilities, timelines for implementation, and Key Control Indicators (KCI).

#### **4.4.7.2 Report the Implementation of Risk Mitigations**

Risk management reporting is a key element of the 'Monitor and Review' phase of the risk management process and needs to occur at each step of the process.

- a) Risk management reporting process supports a formalized, structured and comprehensive approach by PSE to the monitoring and review of its risks, thereby enhancing its risk management process;
- b) Risk Management Reporting is done using [Template 13](#), which is supposed to be completed in a quarterly basis by each Risk Owner assisted by Risk Champion);

- c) The forms from each Risk Owner should be submitted to the Risk Management Coordinator, who will compile them and prepare an institutional Risk Management Report; and
- d) The reporting process must align with the PSE's reporting cycle and meeting schedules to allow relevant organs (e.g., Management, Audit Committee, and the Board, where applicable) to have the report among their meeting agenda items.

#### **4.4.8 Monitor and Review**

Monitoring and review are key aspects of risk management framework. The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes of both the framework and process.

Monitoring and review are two terms which are differentiated as follows:

- a) *Monitoring* – Deals with the risk management process. To monitor, on the daily basis, the inputs, activities and outputs of risk management process; and
- b) *Review (or evaluation)* – Deals with the overall risk management framework. Focus is on the outcome, impact and/ or maturity of the overall or part of the risk management framework in the entity.

There is no one single standard method for assessing the effectiveness of risk management programs in organizations. Whatever process or method is chosen, it needs to be adaptable to changes in the organization.

Section 5 illustrates some of the key considerations and approach to conducting monitoring and evaluation of risk management process and overall framework.

## SECTION V

---

### 5 MONITORING AND REVIEW OF RISK MANAGEMENT FRAMEWORK

#### 5.1 Introduction

In risk management, monitoring and evaluation, is most of the times termed as “monitoring” or “monitoring and review” in COSO and ISO 31000, respectively. The terms review and evaluation will be used interchangeably.

As indicated in the previous section, monitoring is for assessing the risk management process, and evaluation is for checking the effectiveness and maturity of the overall risk management framework.

The following is the focus of each:

- i. *Monitoring* – on the daily inputs, activities, and outputs of risk management process in the PSE;
- ii. *Review/Evaluation* - on the outcome and impact of the overall or part of the risk management framework in the PSE; and
- iii. *Risk Maturity Assessment* - Understanding the capability and maturity of the PSE’s risk management framework and its ambitions for growth.

#### 5.2 Monitoring the Risk Management Process

Monitoring is defined as ongoing process focused providing real-time analysis of implementation of the risk management process against planned activities and mitigations, providing a continuous flow of information, and thereby enabling positive decision-making about risk management process.

##### 5.2.1 Set the Tone at the Top

The effectiveness of monitoring activities is dependent on the commitment and sponsorship from the highest level of governance. This includes, where applicable: the board, the Accounting Officer, and top management.

This will influence the seriousness of managers and other employees (as implementers) on monitoring activities.

##### 5.2.2 Arrange the Reporting Structure

A monitoring structure should be developed and should be consistent with the risk management governance structure which appears in the PSE’s Risk Management Framework.

- i. *Board (if applicable)* – have an oversight role by understanding and inquiring how the management has assured the effectiveness of monitoring activities in risk management;

- ii. *Audit committee* – (whether of the board or of the Accounting Officer) plays and oversight or advisory role in relation to effectiveness of risk management and related monitoring activities. Receives and reviews monitoring reports and advise the board/Accounting Officer accordingly;
- iii. *Management* – has the primary responsibility for the effectiveness of risk management and related monitoring and evaluation activities. They establish and implement the monitoring activities to ensure that risk management process continue to operate effectively;
- iv. *Risk management coordinator* – or in some places is known as Chief Risk Officer, is responsible for coordinating monitoring activities and compiling reports thereof;
- v. *Risk owners* – plan and implement risk treatments and provide reports on the status of implementation or specific issues of concern. Respond to monitoring questions and submit quarterly (or any specified time interval) to the risk management coordinator; and
- vi. *Other staffs* – comply and implement monitoring activities as directed.

### 5.2.3 Prepare a Performance Monitoring Plan

The Risk Management Performance Monitoring Plan (or PMP) is a very important tool for organizing, planning, and implementation of monitoring activities. If properly prepared, the PMP will list all the steps needed for monitoring activities on respective priority risks. As exhibited in [Template 14](#), the following is a minimum content of a typical risk management PMP:

- i. Risk title and ID – only risks prioritize for monitoring purposes (see sub-section 5.1.4 on risk prioritizing);
- ii. Treatment/control option – risk treatment option as agreed and indicated in the risk treatment action plan;
- iii. Performance indicator – indicators or evidence that the treatment has been implemented;
- iv. Timetable for implementation – timeline of risk treatment as indicated in risk treatment action plan;

- v. Data collection methods/tools – how will information on the indicator will be collected by the monitoring authority;
- vi. Sources of data – where will the monitoring authority obtain information on indicators;
- vii. Frequency of data collection – at what intervals or when will information on indicators be collected? and
- viii. Data collection responsibility – person assigned with the collection of data on a particular indicator.

It should be noted that the list of activities above is not necessarily exhaustive. It is advised that one should customize the PMP so as to suit the specific information need in the PSE.

#### 5.2.4 Prioritize Risks to Monitor

Review of the Risk Register to identify the most critical risks to the PSE's objectives.

- a) Depending on the format of the register, this information could readily be found in the Register's Risk Heat-map, which is arranged with risks across difference tolerance level (see Table 6);
- b) Risks in the red region (severe risks) needs to be considered first before those in the light brown region (high risks), and yellow (moderate risks) and green (low risks) regions; and
- c) It is advised to prioritize risks for monitoring purposes in the following order:
  - i. *First priority* – SEVERE risks in the **red region**;
  - ii. *Second priority* – HIGH risks in the **light brown region**;
  - iii. *Third Priority* – MODERATE risks in the **yellow region**; and
  - iv. *Other priority* list depending on the scope that the monitoring system (mostly will end at yellow region).

### 5.2.5 Identify Planned Risk Mitigation Strategies

The prioritization of risks should lead to the identification of strategic objectives that are affected with the risks and the respective risk owners responsible for implementing risk treatment options.

- a) The main source of risk mitigation strategies is the Risk Treatment Action Plan, which must have been developed by risk owners and collected by the Risk Management Coordinator; and
- b) The mitigations identified should be correspondent to the prioritized risks in the previous sub-section.

### 5.2.6 Identify Performance Indicators

Performance indicators provide evidence on the performance of a given risk management activity.

- a) For monitoring purposes, of interest are the output/process indicators (as opposed to outcome/impact indicators – mainly used in evaluation process);
- b) The output indicators measure the degree to which risk mitigation/control activities are being implemented;
- c) To be effective, the information on indicators should be sufficient and suitable (i.e., relevant, reliable and timely); and
- d) Relevance of indicators is obtained either directly or indirectly:
  - i. *Direct information* - e.g., by observing the mitigation control in operation, re-performing them, or otherwise evaluating their operation directly. This is highly relevant for monitoring purposes because it gives an unobstructed view of risk mitigation control operation.
  - ii. *Indirect information* – this is information that shows a change or failure in the operation of risk mitigation control. This includes, for example, operating statistics, key risk indicators (KRI), key performance indicators (KPI), and comparative industry metrics.

### 5.2.7 Determine Data Source and Collection Methods and Tools

Selection of data source should be decided carefully in advance and included in the PMP.

- a) However, in risk treatment activities, most of the indicators would be obtained from risk owners mentioned in the risk register and risk treatment action plans;
- b) Methodology for data collection is vital component of monitoring activities. This usually depends on type of indicators. As indicated earlier, the focus for monitoring activities is on the output/activities level; and
- c) In this case, most of the data collection methods will be through the regular reporting mechanism between those responsible for implementing risk mitigation controls (i.e., risk owners) and the risk management coordinator.

### **5.2.8 Decide on Data Collection, Analysis and Reporting Frequency**

Monitoring of reports are more frequent than evaluations. This is because monitoring is usually inbuilt within the daily implementation of risk management process.

- a) Data collection intervals should also be well aligned with the reporting intervals arranged in the PSE's risk management reporting cycle (i.e., on quarterly and annual basis);
- b) Data collection on performance indicators for risk treatment should be on quarterly basis same as for risk management reports;
- c) The analysis of data collected, and result should lead to the conclusions as to whether the mitigations, as planned in the risk treatment action plan, has not only been implemented but also are working to mitigate the risks in question to the level consistent to the PSE's appetite; and
- d) It is at this stage where one will identify the deficiencies for possible corrective actions or improvement on the mitigations.

### **5.2.9 Prioritize Findings on Treatment Indicators**

Not all deficiencies identified in the assessment of evidence are worth reporting to all levels of management or Audit Committee.

- a) Like it was done in the prioritization of risks, the Risk Management Coordinator should prioritize the deficiencies; and
- b) This will allow to determine the levels to which to report the deficiency, and the urgency and type of corrective action, if any, that should be taken.

### 5.2.10 Report the Findings and Make Follow-up

Reporting of monitoring results depends on the established risk management protocols (in the risk management framework).

- a) Internal to the PSE, the results of monitoring activities should be reported to senior management and the board/audit committee (whichever is applicable); and
- b) External to the PSE, also depending on the external reporting requirements, it may be useful to report on the monitoring results (on quarterly basis) to the IAG who has the overall responsibility for risk management in PSE.

The responsibility of Risk Management Coordinator does not end up by reporting the monitoring results. The responsibility continues to include the arrangements for follow-up activities.

Follow up will mainly include the assessment of adequacy of corrective activities as directed either by the Accounting Officer or Board/Audit committee.

## 5.3 Reviewing the Risk Management Framework

The reviews deal with the risk management framework as a whole. The main focus is to assess the risk management framework in four hierarchies, namely: outcomes, outputs, process, and inputs.

Preliminary requirements are the same to those discussed in the monitoring process, including setting the tone at the top for commitment and following a proper reporting structure for results of the review process.

### 5.3.1 Decide the Interval for the Review

Unlike monitoring activities, reviews are not done continuously but periodic. The PSE should therefore plan to conduct a risk management framework review at a specific interval (e.g., annually, one in every three years) or whenever a need to do so has arisen.

### 5.3.2 Decide and Appoint the Reviewer

Decision should be made on who will conduct the review exercise. There are different ways of doing a review.

Some of the more common terms you may have come across are:

- i. *Self-evaluation* - This involves a PSE holding up a mirror to itself and assessing how it is doing in risk management, as a way of learning and improving practice. It takes a very self-reflective and honest organization to do this effectively, but it can be an important learning experience. This has however serious objectivity issues;
- ii. *External reviewer* - This is done by a carefully chosen outsider or outsider team. The outsider could be a consultant, a peer PSE, or team from the IAGD risk management unit. This is a more objective approach, and suitable when independent assurance is of value; and
- iii. *Interactive evaluation* - This involves a very active interaction between an outside evaluator or review team and the staff in the PSE being reviewed. Here an insider may be included in the review team to provide a balance and local knowledge of the PSE.

### 5.3.3 Provide Written ToR to the Reviewer

The appointed reviewer should be given written Terms of Reference (ToR) on the assignment. The ToR for the reviewer should have included, among other issues, the following:

- i. *Background* - This is background information about the PSE, and something about the problem and need for risk assessment evaluation;
- ii. *Purpose* - Here you would say what it is that the PSE wants the evaluation to achieve?
- iii. *Key evaluation questions* - What the central questions are that the evaluation must address?
- iv. *Specific objectives* - What specific areas, internal and/or external, to be evaluated?
- v. *Methodology* – Give a broad parameter of the kind of approach in evaluation; and
- vi. *Logistical issues* - These would include timing, costing, and requirements of team composition and so on.

### 5.3.4 Prepare a Risk Management Review Matrix

The evaluation matrix is based on the Risk Management Pay-off Model which was designed following an M & E model, that characterizes risk management into four hierarchies/levels of evaluation, namely:

- i. *Inputs* – Everything the PSE need to accomplish risk management. This could be in terms of finance, human resources, infrastructure etc.
  - a) The evaluators seek to assess the organization’s ability to develop an appropriate internal environment — risk appetite, culture and infrastructure — to respond to external forces.
  - b) The response should be to anticipate risks and allocate resources in its corporate strategy, and to develop specific risk management strategies to deal with these risks effectively is critical and is reflected in the strategic fit.
- ii. *Processes* – A collection of functions (actions, jobs, tasks) that consume inputs and deliver benefits or impacts.
  - a) There is an internal risk management capability that is embedded in leadership sponsorship and commitment, people skills and buy-in, integration into strategy, policies, structures and procedures; and
  - b) Risk management is fully embedded into PSE’s context, strategy, structure and processes. Risks to strategic and operational objectives are identified, assessed, and adequately responded to. Risk mitigations are implemented and reported, with appropriate on monitoring activities in place.
- iii. *Outputs* – These “can be immediate and intermediate...” direct products and services generated through risk management processes or activities without specific reference to their ultimate purpose of risk management.
  - These include intermediate outputs, such as improved regulatory compliance, business process continuity, or enhanced internal and external reporting, and final outputs, such as reduced overall costs and increased revenues.
- iv. *Outcomes* – A changed state of being. They describe the effects, benefits or consequences that occur due to the outputs or programs, processes or activities.

The realization of the outcome has a time factor and can be in either the medium or long-term.

- Ultimately, effective risk management should lead to improved overall success of the PSE, especially in meeting financial and operational targets.

From the four levels, the matrix has four columns that require the evaluator to develop/collect the following: evaluation question; indicators; data to be collected; and methods of data collection.

- a) Evaluation questions, indicators and data collection methods given in Risk Management Evaluation Matrix (see [Template 15](#)). Questions in the template are for illustration purposes. They should not be taken to be exhaustive; and
- b) Evaluators are advised to formulate their own set of evaluation questions, indicators, and data collection methods so as to fit their Evaluation Matrices with the PSE's context.

The next sections give more guidance on how to formulate the performance questions, indicators, data to be collected and methods.

### 5.3.5 Develop Review Questions

Review questions are the central questions the evaluation process should answer.

- a) They are not simple questions and should seldom give a “yes” or “no” answer. They should only be answered by collecting “information/evidence” on the earlier planned indicator; and
- b) Design the question at the planning stage of an evaluation by focusing on the four main aspects of a log-frame:
  - i. Level 1 – questions on the expected or planned overall outcome/impact of the overall risk management in the PSE;
  - ii. Level 2 – questions on the output of the risk management processes (both at the framework and process levels);
  - iii. Level 3 – questions on processes in developing a risk management framework and risk assessment.

Questions on the framework and processes should base on the accepted risk management principles, standard/model that the PSE has adopted (e.g., COSO, or ISO 31000), and the requirements from the Guidelines issued by the IAGD;

- iv. Level 4 – questions on inputs that go into the risk management processes, ranging from knowledge from the external environment, skills, physical financial and human resources, etc.

[See 1st column of Template 15](#) - The Risk Management Evaluation Matrix for examples of evaluation questions.

### 5.3.6 Select Indicators for Evaluation

Indicators are measurable or tangible signs that something has been done or that something has been achieved.

In evaluating risk management, the evaluator should select indicators that measure inputs, processes, outputs, outcomes.

The evaluator needs to decide early on what his/her indicators are going to be so that he/she can begin collecting the information immediately.

Choosing the most appropriate indicators can be difficult, but a good indicator should:

- a) Closely track the objective (evaluation question) that it is intended to measure; and
- b) Be precise and unambiguous so that different people can measure it and get similarly reliable results.

Some questions that may guide the selection of indicators are:

- a) Does this indicator enable one to know about the expected result or condition?
- b) Is the indicator defined in the same way over time? Are data for the indicator collected in the same way over time?
- c) Will data be available for an indicator?
- d) Are data currently being collected? If not, can cost effective instruments for data collection be developed?
- e) Will this indicator provide sufficient information about a condition or result to convince both supporters and sceptics?

[See 2<sup>nd</sup> column of Template 15](#) - the Risk Management Evaluation Matrix for examples of indicators.

### 5.3.7 Design and Implement Methods to Collect Data on Indicators

Before starting data collection, the evaluator needs to answer the following questions on each indicator:

- i. What are the sources of data? and
- ii. What are the data collection methods?

[As it can be seen in 3rd and 4th columns of Template 15](#) – Risk Management Evaluation Matrix, data on indicators can be collected from various sources such as PSE’s annual reports and other official documents, survey for target people, trained observer ratings, study using special technical report, and field interviews. The choice of data collection methods should be appropriate for the type of indicator in question.

## 5.4 Assessing Maturity of the Risk Management Framework

Maturity assessment is also part of review or evaluation process, but with the aim of examining the capability level of the PSE’s risk management framework.

### 5.4.1 Select a Risk Maturity Model

Maturity assessment should base on an internationally validated maturity model. In these guidelines, the OECD Model as expanded by RIMS (2006) is used. The model places an enterprise risk management (ERM) into 6 different capability levels, namely:

- i. Level 5 – leadership;
- ii. Level 4 – management;
- iii. Level 3 – repeatable;
- iv. Level 2 – initial;
- v. Level 1 – ad hoc; and
- vi. Level 0 – non-existent.

All the levels are compared using specific seven attributes/features’ attributes.

### 5.4.2 Develop a Risk Maturity Assessment Questionnaire

Like in the evaluation process, a maturity assessment should be done using a tool i.e., a maturity assessment questionnaire or matrix.

- [Template 16](#) is an example of a maturity assessment questionnaire. As shown in Table 7 below, the questionnaire has 4 columns, with 6 rows in each column, as follows:

Table 7: Extract of Risk Maturity Assessment Questionnaire

ATTRIBUTE	LEVELS	FEATURE	TICK
	0 – non-existent		
	1 – ad hoc		
	2 – initial		
	3 – repeatable		
	4 – Managed		
	5 – leadership		

- i. *Column 1 – Attributes:* fill in any of the 7 attributes under review (e.g., ERM approach, ERM process management, Risk Appetite, etc.);
- ii. *Column 2 – Levels:* the maturity levels from 0 to 5, these will appear in all the 7 attributes;
- iii. *Column 3 – Features:* these are the specific features/questions that the assessor will look for in each of the attribute and at each level of maturity;
- iv. *Column 4 – Tick:* this is where the assessor ticks when it is confirmed that a specific feature is available in a given level of maturity under an attribute.

#### 5.4.3 Collect and Assess Information on Maturity Attributes and Features

After the tool has been developed as above, the maturity assessor proceeds to collect evidence of existence of features. Data collection methods are as in the evaluation process which includes documentary reviews, interviews, and if possible, observations.

However, the main focus is to be able to place the PSE's risk management capability on a specific level of maturity (i.e., 0 to 5). In this case, it is crucial that the ticking of the features should strictly be one tick only, in one feature, in one level of maturity. There should be no more than one tick in one attribute.

The assessment of the information is simply a look at the frequency of ticks appearing in each level of maturity (0 to 5) in each of the 7 attributes.

## SECTION VI

### 6. TEMPLATES

#### Template 1: Example of Risk Management Policy Statement

##### **RISK MANAGEMENT POLICY**

This forms an overall risk policy of PSE: XYZ. It provides the purpose for the policy, specific risk policy statement, the risk appetite, and applicable principles.

##### **Purpose**

The purpose of PSE: XYZ Risk Management Policy is to formalize and communicate the PSE: XYZ commitment and principles towards the management of risks across the PSE. Specifically, Risk Management Policy serves the following purposes:

- i. To ensure that all the current and future material risk exposures of the PSE: XYZ are identified, assessed, quantified, appropriately mitigated and managed;
- ii. To establish a framework for PSE: XYZ's risk management process and ensure entity-wide implementation;
- iii. To ensure systematic and uniform assessment of risks related with PSE: XYZ;
- iv. To enable compliance with appropriate regulations, wherever applicable, through the adoption of best practices; and
- v. To assure growth of PSE: XYZ operations.

##### **Risk Policy Statement**

The Risk Management Policy specifies that PSE: XYZ:

- i. Recognizes that risk is inherent in its vision, mission, objectives, and activities.
- ii. Recognizes that the management of risk is a key element of sound governance and an important strategy for the achievement of its mission, vision and supporting objectives.
- iii. Is committed to embedding risk management principles and practices into its organizational culture, decision-making processes, business information systems, strategic and operational planning of programs and activities.
- iv. Will pro-actively identify, analyse and manage its risks and opportunities at all levels of the PSE.

- v. Ensures that all risk identification, analysis, evaluation and treatment are to be reported and updated within its Risk Register.
  - vi. Will promote continuous improvement and review of risk management through regular training, monitoring, audit and reporting processes.
  - vii. Will update its Risk Management Framework after every five years to align with its Five Years Rolling Strategic Plan cycle. However, the Framework may be reviewed at any given time to accommodate substantive changes, which may make the existing Framework, or any of its sections, redundant.
  - viii. Will update its Risk Register to align with its planning and budgeting cycle.
- Include also risk management principles as part of the risk management policy.

## Template 2: Examples of Risk Categories, Appetite Statement and Ratings for Risk Categories

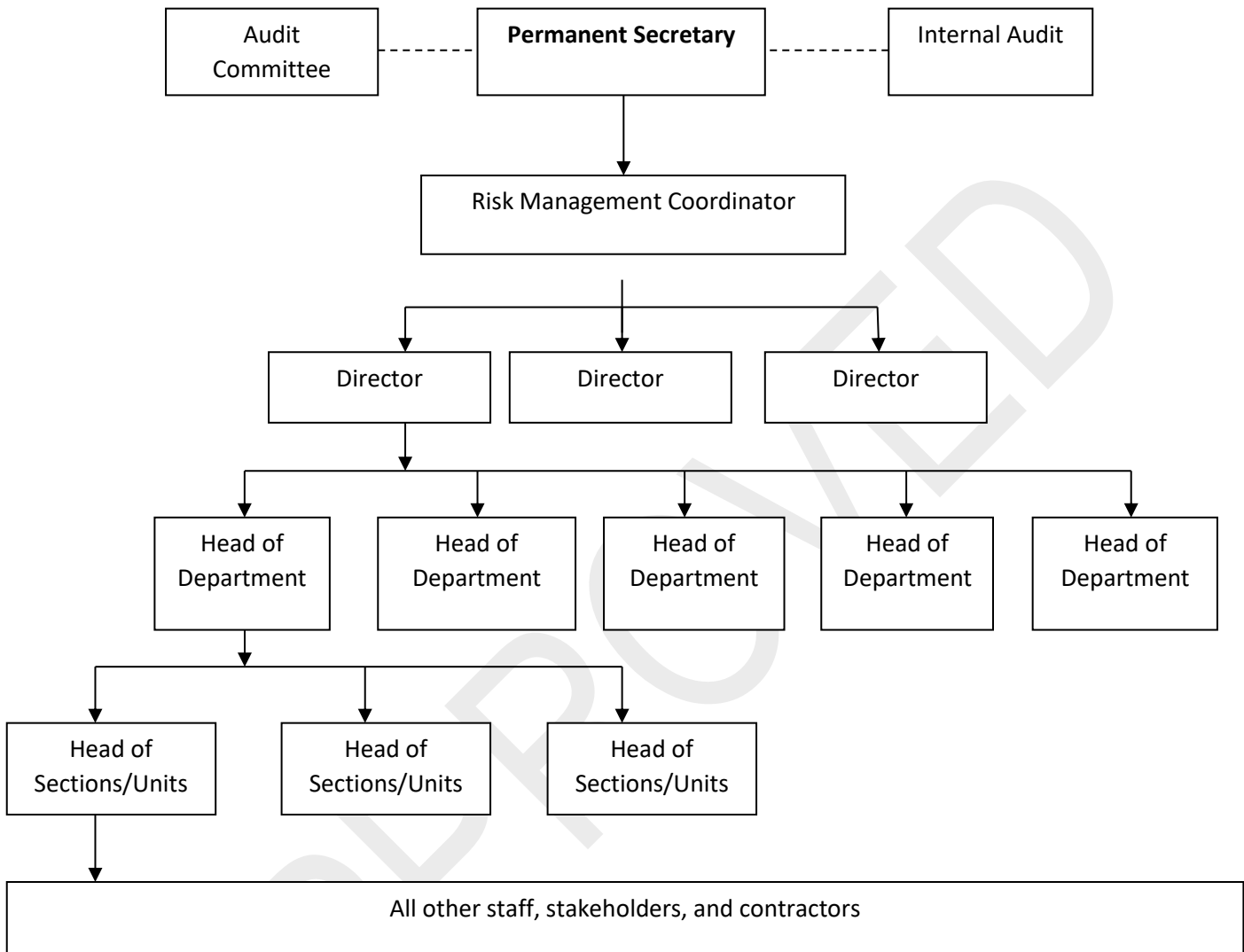
Risk Category	Appetite Rate <sup>12</sup>	Risk Appetite Statement
Strategic	Moderate appetite	<p>The PSE faces a number of risks in the course of strategy selection; prioritization, modification, and implementation. Such risk jeopardizes achievement of the strategic goals and objectives at high levels and may not have control.</p> <p>The PSE has <i>moderate appetite</i> to strategic risks, and they shall be managed through detailed risk assessment processes for scan external environment and making the PSE resilient to such issues from higher-level decisions and radical changes to the operating environments.</p>
Operational	Moderate appetite	<p>Operational risk may include people, processes, systems, or external events that are likely to impede the PSE's ability to meet its objectives.</p> <p>The PSE has <i>moderate appetite</i> to operational risks, especially those relating to process efficiency, governance processes, and business continuity.</p>
Service delivery	High appetite	<p>The PSE delivers a range of services to clients who are the main reason for its existence. The PSE is open to creativity and innovation and is willing to take some level of risk to deliver efficiencies, enhance capabilities and provide services of highest standards.</p> <p>The PSE has a <i>high appetite</i> to take risks geared to service enhancement.</p>
Environmental	Low appetite	<p>The PSE recognizes the importance of conserving the environment and curbing global warming. The PSE strive to minimize the effect our activities have on the environment and with all mean to choose green solutions.</p>

<sup>12</sup> See meanings of ratings and related color on next page.

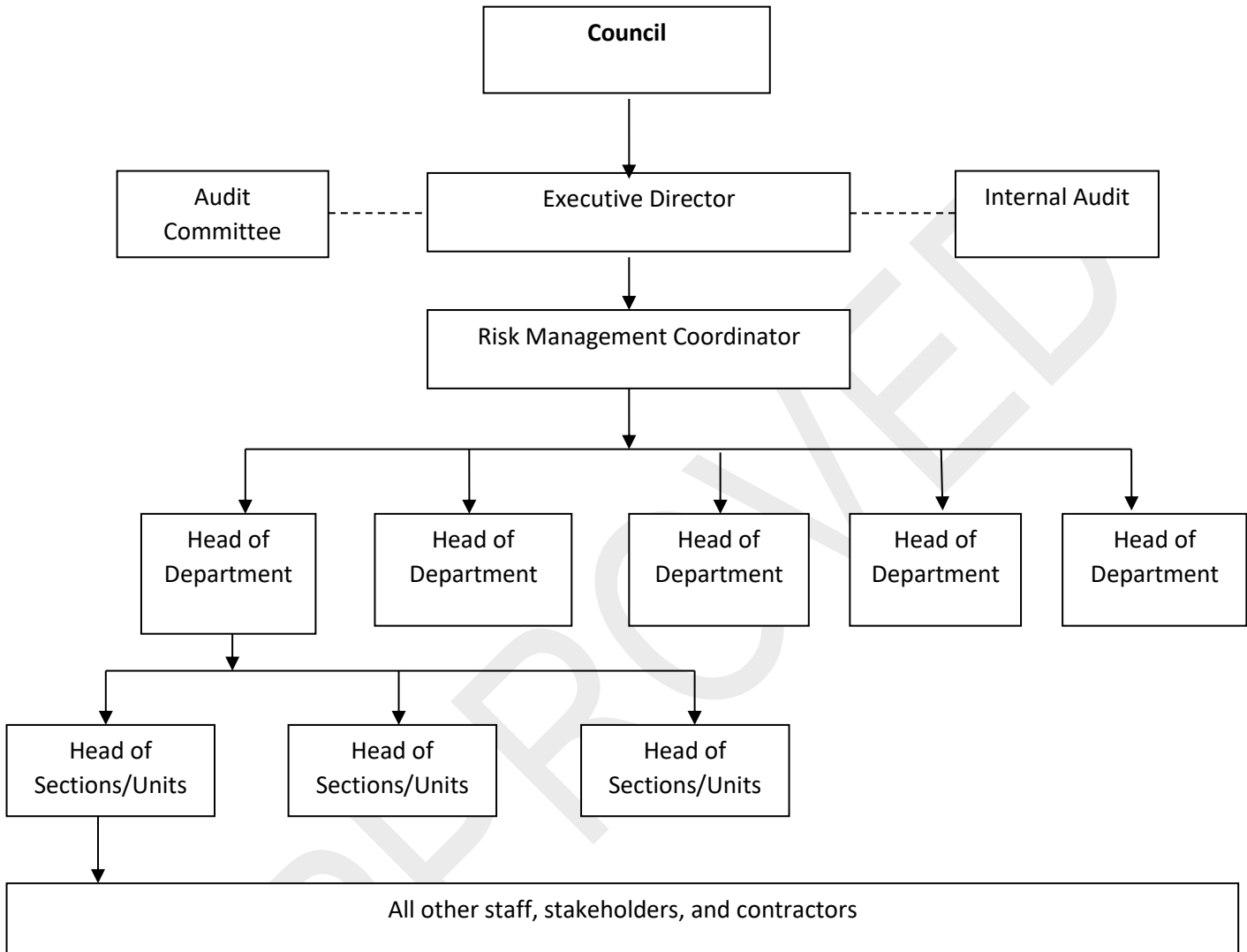
Risk Category	Appetite Rate <sup>12</sup>	Risk Appetite Statement
		The PSE has a <i>low appetite</i> for activities that have environmental impacts.
Financial	Zero appetite	<p>The PSE recognizes the financial risks involved in delivering its services, especially in procurement and capital development projects.</p> <p>The PSE has <i>low appetite</i> to activities that lead to financial fraud, wastage, misappropriation and/or threaten financial sustainability.</p>
Reputation	Zero appetite	<p>These risks may originate from negative perceptions by stakeholder hence jeopardize credibility.</p> <p>The PSE has <i>zero appetite</i> to any incidences of putting its reputation to be questionable among its stakeholders.</p>
Compliance	Zero appetite	<p>Risk that the agency does not fulfil its obligations under applicable laws, regulations, federal directives, mandates, or executive orders or has gaps in mission-critical functions to supervise, license, and maintain a sound federal banking system.</p> <p>The PSE has <i>zero appetite</i> to risks related to non-compliance with applicable laws, regulations, government directives, and executive orders; risks linked with failure to abide by contractual obligations; or poor employee conduct.</p>
Technology	Low appetite	<p>Technology risk may include:</p> <ul style="list-style-type: none"> <li>• Risks to data availability: Access to required information at critical times to perform job functions, thereby strengthening business continuity, operations, and processes.</li> <li>• Risks to data integrity, corrupted, incomplete, or inaccurate information from failures in input and processing controls (i.e., not</li> </ul>

Risk Category	Appetite Rate <sup>12</sup>	Risk Appetite Statement
		<p>manual input error) negatively affects applications, systems, and outputs, limiting management's decision-making capabilities.</p> <ul style="list-style-type: none"> <li>• Risk to privacy breach or risks associated with large-scale theft or loss of information and data security.</li> <li>• Infrastructure: Risks associated with information systems and telecommunications, and related infrastructure. Consistency and reliability of technology across the organization to support the current and future information requirements of the business in an efficient, cost-effective, and well-controlled method.</li> </ul> <p>The PSE has <i>low appetite</i> to risks that will jeopardize its information systems that may corrupt the quality, reliability and availability of information.</p>

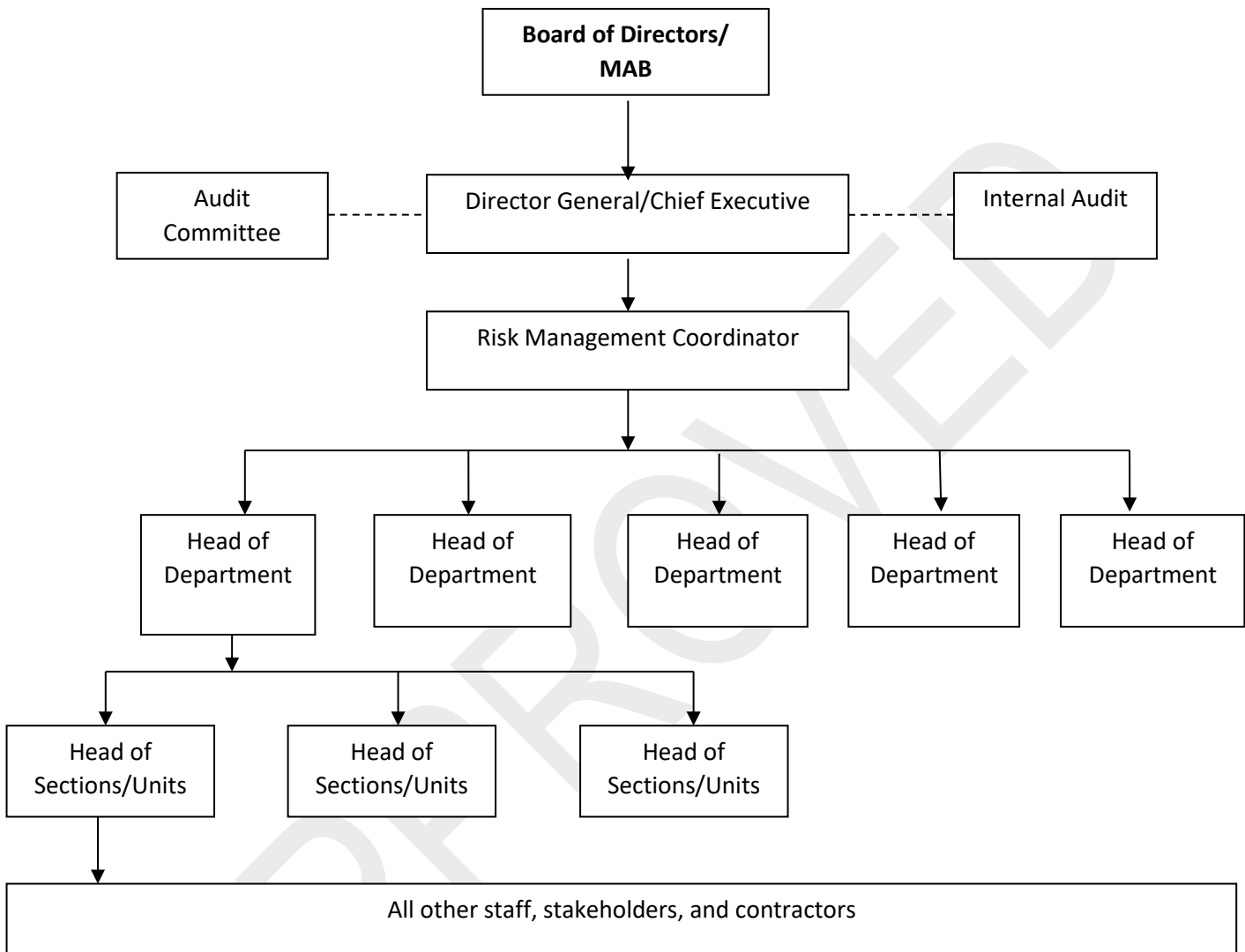
### Template 3: Indicative Risk Management Governance Structure in Ministries



Template 4: Indicative Risk Management Governance Structure for LGAs



Template 5: Indicative Risk Management Governance Structure for Departments/ Parastatals



## Template 6: Sample Outline of a Risk Management Framework

### SECTION ONE

#### 1.0 INTRODUCTION AND BACKGROUND INFORMATION

1.1 Background

1.2 Purpose

### SECTION TWO

#### 2.0 RISK MANAGEMENT POLICY

2.2 Risk Policy Statements

2.3 Risk Appetite Statement

2.4 Risk Management Principles

### SECTION THREE

#### 3.0 RISK MANAGEMENT ROLES AND RESPONSIBILITIES

3.1 Board of Directors

3.2 The Audit Committee

3.3 Executive Director

3.4 Directors, Heads of Departments and Units

3.5 Risk Management Coordinator

3.6 Chief Internal Auditor

3.7 All Staff, contractors etc

### SECTION FOUR

#### 4.0 RISK MANAGEMENT PROCEDURES

4.1 Adopted Standards

4.2 Scope, Context and Criteria

4.3 Risk Assessment

4.3.1 Risks Identification

4.3.2 Risk Analysis and Evaluation

4.4 Risk Treatment

4.5 Monitoring and Review

4.6 Communication and Consultation

### SECTION FIVE

#### 5.0 ANNEX

5.1 Risk Identification and Analysis Sheet

5.2 Risk Treatment Schedule and Action Plan

5.3 Quarterly Implementation Report

5.5 Framework Update

## Template 7: Sample of Outline of an Annual Risk Management Plan

<p><b>COVER PAGE</b></p> <p><b>[WITH PSE's NAME AND LOGO]</b></p> <p><b>INDICATIVE OUTLINE OF THE RISK MANAGEMENT PLAN</b></p> <hr/>
<p><b>1. Introduction</b></p> <ul style="list-style-type: none"><li>1.1. Background</li><li>1.2. Objectives of the plan</li></ul>
<p><b>2. Context</b></p> <ul style="list-style-type: none"><li>2.1. Legal issues related to risk management.</li><li>2.2. A description of how risk management activities support the pursuit of the organization's objectives;</li><li>2.3. An outline of roles and responsibilities of relevant oversight committees, governing bodies and key stakeholders and the expectations and responsibilities for each of these groups.</li></ul>
<p><b>3. Scope of the Plan</b></p> <ul style="list-style-type: none"><li>3.1. Financial year and coverage</li><li>3.2. Areas of the PSEs (e.g., HQ, branches, Zones, etc. where applicable)</li><li>3.3. Number of activities and timeframe for each area of risk management<ul style="list-style-type: none"><li>3.3.1. Risk governance,</li><li>3.3.2. Risk assessment,</li><li>3.3.3. Reporting,</li><li>3.3.4. Monitoring and Evaluation,</li><li>3.3.5. Capacity building/trainings,</li><li>3.3.6. Meetings (Board/Audit Committee, management, etc.)</li><li>3.3.7. Etc.</li></ul></li></ul>
<p><b>4. Resourcing Requirements</b></p> <ul style="list-style-type: none"><li>4.1. Budget/finances,</li><li>4.2. Human resources (skills set and number),</li><li>4.3. Information systems,</li><li>4.4. Physical assets,</li><li>4.5. Etc.</li></ul>

**5. Performance measures**

- 5.1. Annual evaluations,
- 5.2. Audits and performance assessments,
- 5.3. Etc.

**6. Attachment: Schedule of Planned Activities, Expected Output and Timeframe**

No.	Activity	Output	Due Date	Responsible Person
<i>Risk Governance</i>				
1.	Develop the Risk Management Policy, Strategy and Implementation Plan	Finalize and internal approval of Risk Management Policy, Strategy and Implementation Plan	26 August, 202x	Accounting Officer
		Final Review by the IAG Team	1 September, 202x	Risk Coordinator
		Approval of the Risk Management Framework by the Board	30 <sup>th</sup> September, 202x	Accounting Officer /BoD
		Communicate contents of the Risk Management Policy, Strategy and Implementation Plan to all staff members	November, 202x	DAHRM/ Permanent Secretary
2.	Nominate Risk Management Champions and Risk Coordinator	Appointment letters issued by the Director General to the risk management Champions and Coordinator	October, 202x	Accounting Officer
3.	Risk Champions documentation on Terms of Reference	Approved Risk Champions Terms of Reference	October, 202x	Risk Coordinator/ Accounting Officer

	updated, approved and implemented			
4.	Embed risk management into daily business operations and decision making	Staff and Management meeting agendas to include discussion on status of risk management processes and emerging risks for escalation to the risk registers	November, 202x	DCS/ Accounting Officer
5.	Finalize, approve and implement a Risk Management Implementation Plan	Approved Risk Management Implementation Plan	November, 202x	DCS/Director General
<b><i>Risk Identification, Analysis and Evaluation</i></b>				
6.	Quarterly review and approval of the strategic risk register	Risk registers approved by the Management	Quarterly	Accounting Officer
7.	Quarterly review and approval of the operational risk registers	Risk registers approved by the Directors and communicated to staff	Quarterly	Accounting Officer
<b><i>Risk Recording and Reporting</i></b>				
8.	Quarterly report to the risk committee and Audit Committee	Include updated and approved risk register on the risk committee and Audit Committee agenda	Quarterly	Risk Coordinator
9.	Submit the risk register to internal audit	Latest available approved risk register submitted to internal audit for	February, 202x	Risk Coordinator

		the internal audit plan		
10.	Submit relevant risk information to external audit	Risk documentation to be provided during the annual audit process	October, 202x	DCS
<b><i>Risk Monitoring and review</i></b>				
11.	Evaluates effectiveness of risk management in Management Team	Minutes of meetings indicating the review and evaluation of risk management	January, 202x	Risk Coordinator
12.	Job descriptions and Performance agreements to include risk management responsibilities of relevant staff members	Updated and agreed job descriptions and performance agreements	March, 202x	DCS
13.	Consideration and incorporation of risk management in the annual planning and budget process of the Board	Risks incorporated into annual planning and budget documents	December, 202x	DCS
<b><i>Capacity Building, Risk Awareness and Training</i></b>				
14.	Communicate the main principles of the approved Risk Policy and Strategy to the staff	Communications to staff	November, 202x	DCS
15.	Provide training to the	Training held and an attendance register of	Annually	DCS

	relevant role players in terms of their roles and responsibilities in risk management at Management Team	role players at the training		
16.	Develop risk orientation (induction) program for new employees.	All new employees orientated on risk management.	Annually	DCS

APPROVED

## Template 8: List of Common Examples of Risks

Please be aware that this list does not represent a complete list of possible risk areas, nor will all of these risks be applicable to all organizations. The list has been created to stimulate discussion on risk, rather than as a comprehensive checklist.

### **STRATEGIC**

**Including: Governance, Stakeholder Relationships, Reputation, Environment**

- Changes in services provided
- Loss of customers to private sector companies
- Services/goods not provided within budget
- Change in ability to supply services/goods
- Change in public demand for services/products
- Loss of customers to other state organization
- Political change
- Poor market knowledge
- Change in interest rates
- Undefined or unclear strategic vision
- Inaccurate forecasting
- Unethical business practices
- Incomplete or inaccurate resource planning
- Poor organizational design/Inappropriate reporting lines
- Strategic plan not implemented
- Business Continuity Planning inadequate/or not developed
- Stakeholders not identified
- Poor/deteriorating stakeholder relationship
- Expectations of stakeholders not understood
- Poor community relationships
- Negative/hostile/inaccurate press coverage
- Ineffective communication strategy/plans
- Joint ventures/ partnerships not managed
- Loss of customer loyalty/revenue
- Failure to meet sustainability targets
- Water shortages
- Fuel shortages
- Failure to assess and understand environmental impact of organizational activities
- Contamination of water supply
- Damage to/ development of protected sensitive natural habitats

- Breach of environmental protection/ sustainability legislation
- Sustainability costs making service provision uneconomical
- Air or water pollution

**FINANCIAL:****Including Capital Management, Budgeting, Revenue and Expenditure, Reporting**

- Incorrect valuation of capital assets
- Declining market value of assets
- Capital assets not maintained/deterioration
- Equipment obsolescence
- Customer revenue/collections targets not met
- Unauthorized and irregular expenditure
- Wasteful or unproductive expenditure
- Changes in funding allocations
- Over/under spending budget allocations
- Inaccurate revenue forecasting
- Inaccurate expenditure forecasting
- Financial reporting requirements not understood
- Reporting deadlines not met
- Errors/omissions in financial statements
- Reporting not in correct format
- Fraud

**OPERATIONAL:****Including Human Resources, Procurement, Legislative, Asset Management**

- Absenteeism
- Inability to attract and retain staff/Staff turnover
- Poor service provided by staff
- Strikes and workplace unrest
- Wrongful termination
- Uncompetitive remuneration
- Job roles/accountabilities unclear
- Workplace injury: Burns, falls, food poisoning, car accident etc.
- Pandemic and Infectious Disease Outbreak
- Failure of/No fire suppression system
- Sexual harassment/violence
- Equipment obsolescence
- Failure to maintain/repair assets
- Unauthorized use/Misuse of fleet vehicles

- Failure to maintain assets/equipment
- Theft
- Natural Disasters: Fire, Flooding, Bushfires
- Underinsurance/Assets not insured
- Power failure
- Terrorist attack/Bomb threat etc.
- Tender evaluation requirements not defined
- Overpayment for goods and services
- Failure to comply with procurement legislation/processes
- Conflicts of interest in tender award process
- Failure/closure of service provider
- Unethical service provider actions
- Goods/services not meeting quality requirements
- Non-delivery of goods and services by supplier
- Breach of contract
- Legislative requirements not clear/not understood
- Conflicting requirements of different legislation
- Actions taken exceeding mandated authority
- Disputed authority between multiple agencies/departments
- Delays in finalizing legislation
- Changes in legislation
- Poor process design
- Poor process integration
- Project budget over-runs
- Failure of project
- Project scope not defined

#### **KNOWLEDGE AND SYSTEMS:**

##### **Including Data, IT Security, Software, Hardware, Intellectual Property**

- Inadequate system security/Confidential information not adequately protected
- IT systems not integrated
- Network failure/network unavailability
- Unauthorized system access/IT security breach or failure
- IT system/software obsolescence
- Ineffective Disaster Recovery Plan
- Poor choice of software/IT solution/IT solution does not support business requirements
- System not scalable/cannot meet increased capacity requirements
- Loss of data/information

## Template 9: Guide to Wording of Risks

The wording for risk must be consistent with future orientation in the definition of risks.

The applicable guide is to start with wording such as “if .... then ...’ or “The possibility of ..... due to .... resulting into ....”

**Example:** **Possibility of** cyber-attack due to failure to update ICT firewall leading to data loss.

If we don't update the ICT firewall, then we shall suffer a **cyber-attack** leading to loss of data.

The proper risk description must follow the **A+S+E+C** best practice:

- A (Asset)** What asset(s) are at risk? (Vulnerability), it can be a process or system or physical asset.
- S (Source)** What are the hazards or threat actors that might lead to the risk manifesting?
- E (Event)** What incident is being considered? What about likelihood of attack?
- C (Consequence)** What is the likely impact of this risk?

On the example above:

***The possibility of cyber-attack due to failure to update ICT firewall leading to data loss.***

- Asset** ICT System,
- Source** Un-updated firewall,
- Event** Cyber-attack, and
- Consequence** Loss of data.

## Template 10: Risk Assessment Sheet

## Template 10: Risk Assessment Sheet

<b>Objective/Target</b>	Write the objective impacted by the risk						
<b>Target (Optional)</b>	Write the Target impact by the risk (at Division)						
<b>Risk Title</b>	Provide a brief title of the risk	<b>Risk ID</b>	Define the identity of the risk				
<b>Risk Description</b>	Provide a brief description of the risk						
<b>Principal risk owner</b>	Include the title of the person managing the risk and the area where the risk falls						
<b>Supporting owner(s)</b>	Provide the title of other persons affected by the risk						
<b>Risk Category</b>	Is it a financial, technical, etc						
<b>Key Risk Indicator</b>	Provide numerical. Traffic light or Percentage early warning						
<b>Sector</b>	Agriculture, Mining, Tourism etc						
<b>Risk Causes and Consequences</b>							
<b>Causes</b> (Provide a list of sources or causes that may lead to risk materializing e.g., events, decisions, actions, and processes)				<b>Consequences</b> (Provide a description of what will happen if the risk materializes)			
1.		1.					
2.		2.					
3. etc.		3.e tc.					
<b>Inherent risk analysis</b> (Tick the impact and likelihood of risk assuming the current controls do not exist or completely fails)							
<b>Inherent risk</b>	<b>Impact (I):</b>		VERY HIGH	HIGH	MODERATE	LOW	VERY LOW
	<b>Likelihood (L):</b>		VERY HIGH	HIGH	MODERATE	LOW	VERYLOW
<b>Risk rating</b>	<b>I x L:</b>						<b>HIGH</b>
<b>Key risk mitigation/controls currently in place:</b> (List mitigations in place, rate and color effectiveness and document separately weakness if control is rated below effective)							
<b>No.1</b>	<i>Mitigation/Control</i> (Write in the summary of the existing control)	Effectiveness of preventive controls (Indicate appropriate color, <i>effective</i> , <i>partially effective</i> , or <i>ineffective</i> )	R at in g	Effectiveness of corrective controls (Indicate appropriate color, <i>effective</i> , <i>partially</i> )	Rating		

					<i>effective, or ineffective)</i>		
1.		Partially - Effective		Partially - Effective			
2.		Effective		Ineffective			
3.		Ineffective		Ineffective			
		Average Preventive		Average Corrective			
<b>Residual risk analysis</b> ( <i>tick the impact and likelihood of the risk that remains after considering how the current mitigation have reduced the inherent risks based on corrective or preventive control</i> )							
<b>Residual risk</b>	<b>Impact:</b>		VERY HIGH	HIGH	MODERATE	LOW	VERY LOW
	<b>Likelihood :</b>		VERY HIGH	HIGH	MODERATE	LOW	VERY LOW
<b>Risk rating</b>	<b>I X L:</b>		<b>MODERATE</b>				
<b>Proposed Mitigating/ Control to be taken:</b> ( <i>List mitigations/controls that must be taken to mitigate the residual risk base your proposal on: Unmitigated cause to the risk or identified weakness in current control</i> )							
<b>No.</b>	<b>Proposed control</b>			<b>Key Control Indicator (KCI)</b>		<b>Resources Required</b>	
1.							
2.							
3. etc.							

OBJECTIVE/ TARGET (Write the objective affected by the risk)	RISK TITLE (As it appears in the identification sheet)	CATEGORY OF RISK (As described in the identification sheet)	RISK ID (As in the identification sheet)	RESIDUAL RISK ASSESSMENT (As in the identification sheet)		RISK RATING (I X L) [Product (in number) of multiplying Impact by Likelihood]	RISK STATUS (Write either EXTREME, HIGH, MEDIUM, or LOW and shade it with the appropriate colour)	PRINCIPAL RISK OWNER (As in the identification sheet)	PAGE (Write the page number to refer to the attached identification sheet)
				IMPACT (I)	LIKELIHOOD (L)				
Objective A  (The objectives numbers or	Risk A.01								
	Risk A.02								
	Risk A.02								
	Etc.								
	Etc.								

reference should be identical to those appearing in the organization's strategic plan document)									
<b>Objective B</b>	Risk B.01								
	Risk B.02								
	Etc.								
	Etc.								

Template 11: Extract of a Risk Register

Template 12: Extract of Risk Treatment Action Plan

<b>RISK MITIGATION ACTION PLAN</b>
------------------------------------

<b>Principle Risk Owner:</b>			
<b>Compiled by:</b>		<b>Date of Compilation:</b>	
<b>Reviewed by:</b>		<b>Date of Review:</b>	

ID :	Risk Title [From Risk Register in order of priority]	Objective/Target/ Area Affected [Indicate objective affected]	Risk Rating [From residual risk rating = I x L]	Proposed Treatment/ Control Options to be taken. [From Risk Identification Sheet]	Cost-benefit analysis/ feasibility [A = accept, R = reject, P = postponed]	Officer/ Person Responsible [For Implementation of Treatment Options]	Timetable for Implementation [Give specific start and end dates]	How will this risk and treatment options be verified/monitored? [Write Key Control Indicator (KCI)]

## Template 13: Risk Management Quarterly Implementation Report

*Main contents of a Detailed Periodic Risk Management Report include the following information as minimum:*

### 1. INTRODUCTION

1.1. Organizational background

1.2. Risk Management Background, Frameworks, Coordinator and Champions

1.3. Purpose of the Report

1.4. Scope of the Report

### 2. REVIEW OF RISK MANAGEMENT ANNUAL PLAN

2.1. Planned Activities for the Period

2.2. Status of Implementation and Challenges

### 3. TOP TEN RISKS AND THEIR STATUS

3.1. Risk Heat Map

3.2. Risk Register

### 4. STATUS OF IMPLEMENTATION OF MITIGATION PLAN

4.1. Planned Mitigation

4.2. Implemented

4.3. On-going Implementation

4.4. Not Implemented

5. CHALLENGES AND WAY FORWARD

6. CONCLUSION

APPENDIX: Summary of Risk Implementation

RISK MANAGEMENT REPORT SHEET			
<b>Department/Unit</b>		<b>Principle Risk Owner</b>	
<b>Quarter Ending</b>		<b>Prepared By</b>	

<b>ID :</b>	<b>Risk Title</b> [From Risk Register in order of priority]	<b>Objective/ Target</b> [Indicate objective affected]	<b>Risk Rating</b> [From residual risk rating = I x L]	<b>Proposed Treatment/Control Options to be taken.</b> [From Risk Identification Sheet]	<b>Officer/Person Responsible</b> [For Implementation of Treatment Options]	<b>Timetable for Implementation</b> [Give specific start and end dates]	<b>Key Control Indicator (KCI)</b>	<b>Status of Implementation</b>	<b>Remarks / Comments</b>

### Appendix 14: Risk Management Performance Monitoring Plan

<b>RISK MANAGEMENT PERFORMANCE MONITORING PLAN</b>	
<b>Name of Evaluator</b>	
<b>Date of Evaluation</b>	

<b>Risk title &amp; ID</b> <small>(Prioritized for monitoring)</small>	<b>Agreed Treatment/Control Options</b> <small>(From Risk Treatment Action plans of individual risk owners)</small>	<b>Performance Indicator</b> <small>(As indicated in risk treatment action plan)</small>	<b>Timetable for Implementation</b> <small>(Dates for implementation – arrange chronologically)</small>	<b>Data Collection Methods/tools</b> <small>(Approach in collecting evidence on indicator)</small>	<b>Source of Information</b> <small>(Where to get information on indicators)</small>	<b>Data Collection Frequency</b> <small>(Timing of collecting information on indicators)</small>	<b>Data Collection Responsibility</b> <small>(Who will collect evidence on indicators)</small>

## Appendix 15: Risk Management Evaluation Matrix

**RISK MANAGEMENT EVALUATION MATRIX**

<b><i>Evaluation question</i></b>	<b><i>Indicators</i></b>	<b><i>Data to be collected</i></b>	<b><i>Methods/Tools of data collection</i></b>
<b><i>OUTCOME:</i></b> Effective risk management should lead to improved overall success of the PSE.			
<b><i>Evaluation question</i></b>	<b><i>Indicators</i></b>	<b><i>Data to be collected</i></b>	<b><i>Methods of data collection</i></b>
Is there a measurable increase in the overall PSE's financial and operational performance?	Increase (%) in performance/KPIs/financial surplus etc. Achievement of targeted outputs (%) Achievement (%) service levels Etc.	Performance reports (financial and operational)	Documentary reviews.  Interviews with key stakeholders.
<b><i>OUTPUTS:</i></b> Risk management contributes to the achievement of the four categories of objectives —strategic, operations, reporting and compliance.			
<b><i>Evaluation question</i></b>	<b><i>Indicators</i></b>	<b><i>Data to be collected</i></b>	<b><i>Methods of data collection</i></b>
1. Is there improvement in general achievement of PSE's strategic objective?	Increase (%) in achievement of performance targets over time.	Annual performance reports: • Operational	Documentary reviews at strategic level.
2. Is there improvement in general achievement of operational targets?	Increase (%) in achievement of operational targets over time.	Annual performance reports: • Operational reports.	Documentary reviews at functional level.

<b>Evaluation question</b>	<b>Indicators</b>	<b>Data to be collected</b>	<b>Methods/Tools of data collection</b>
3. Is there improvement in the PSE’s reliability and timeliness of financial and other reports and disclosures?	Decrease in audit queries relating to violation of reporting framework (to various external authorities): <ul style="list-style-type: none"> <li>• Financial reports;</li> <li>• Procurement reports;</li> <li>• Operational reports;</li> <li>• Etc.</li> </ul>	Reports from various regulators in which the PSE is accountable to: <ul style="list-style-type: none"> <li>• The CAG reports;</li> <li>• PPRA reports;</li> <li>• IAG reports;</li> <li>• Etc.</li> </ul> Dates of submission of financial reports (vs. reporting timetable).	Documentary reviews.
<p><b>PROCESSES:</b> There is an internal risk management capability that is embedded in leadership sponsorship and commitment, people skills and buy-in, integration into strategy, policies, structures and procedures.</p> <p>Risk management is fully embedded into PSE’s context, strategy, structure and processes. Risks to strategic and operational objectives are identified, assessed, and adequately responded to. Risk mitigations are implemented and reported, with appropriate on monitoring activities in place.</p>			
<b>Evaluation question</b>	<b>Indicators</b>	<b>Data to be collected</b>	<b>Methods of data collection</b>
<b>1. Leadership and integration of Risk Management:</b>			
1. Do the board/CEO/ Audit Committee, and Senior Management support and promote risk management?	<ul style="list-style-type: none"> <li>• Board/CEO or Audit committee endorsement of risk management policy.</li> </ul>	Agenda and minutes from meeting of the board/audit committee or top management.	<ul style="list-style-type: none"> <li>• Documentary review</li> <li>• Interview with board members, audit</li> </ul>

<b>Evaluation question</b>	<b>Indicators</b>	<b>Data to be collected</b>	<b>Methods/Tools of data collection</b>
	<ul style="list-style-type: none"> <li>• Risk management being an agenda in meetings of the Board, audit committee, and top management.</li> <li>• Signed risk management policies/strategy by Board/CEO.</li> <li>• Risk management reports discussed at Board/audit committee/top management meetings.</li> </ul>		committee members, senior management.
2. Are the Board, Audit Committee, senior management aware of key risks and has system in place to keep update with treatment progress?	Summary of key risks/risk register discussed at board/audit committee (agenda/minutes).	Agenda and minutes from meeting of the board/audit committee or top management.	Documentary review.
3. Are there clear roles and responsibilities and accountability in managing risks?	<ul style="list-style-type: none"> <li>• Stipulated risk management roles and responsibilities in the risk management policy/framework.</li> </ul>	Documented and signed risk management policy/framework – see risk governance structure/roles and responsibilities.	Documentary review.

<b>Evaluation question</b>	<b>Indicators</b>	<b>Data to be collected</b>	<b>Methods/Tools of data collection</b>
	<ul style="list-style-type: none"> <li>Establishment of a unit/function responsible for risk management (risk coordinator, chief risk officer, risk champions).</li> </ul>		
4. Are the PSE's staff equipped and supported to manage risks well?	<ul style="list-style-type: none"> <li>Number of staff given training on Risk management.</li> <li>Bulleting and internal memos/or web news on risk management.</li> <li>Financial resources budgeted for risk management.</li> <li>Standing arrangement for staff inputs on issues of risks.</li> </ul>	<p>Training reports on risk management.</p> <p>Example of internal memo/bulleting/website news on risk management.</p> <p>Budget allocations on risk management.</p> <p>Forms and written procedures for staff inputs.</p>	<p>Documentary reviews.</p> <p>Interviews with staff.</p>
5. Is there a clear risk strategy/policy, governance structure and procedures?	Documented and signed risk management policy/framework.	Copy of signed risk management policy/framework.	Documentary review.
6. Is there effective arrangement for managing risks with external stakeholders?	<ul style="list-style-type: none"> <li>Links/arrangements/Letters or communications with external stakeholders on specific risks.</li> </ul>	<ul style="list-style-type: none"> <li>Copies of letters, MoU, communications</li> </ul>	<p>Documentary reviews.</p> <p>Interviews.</p>

<b>Evaluation question</b>	<b>Indicators</b>	<b>Data to be collected</b>	<b>Methods/Tools of data collection</b>
	<ul style="list-style-type: none"> <li>Meetings reports with stakeholders on discussion on specific risks.</li> </ul>	<ul style="list-style-type: none"> <li>with external stakeholders.</li> <li>Minutes of meeting with stakeholders.</li> </ul>	Third party confirmation with stakeholders.
7. Are risk management activities incorporated/ embedded in the PSE's plans, budgets, processes and activities?	<ul style="list-style-type: none"> <li>Budget: Risk management activities, risk treatments are in the PSE budget.</li> <li>Operational activities implemented along risk management activities.</li> <li>Risk management activities are reported along operational reports.</li> </ul>	Budgets and plans.  Reports of operations.  Risk management reports.	Documentary reviews.  Interviews.
<b>2. Risk management framework:</b>			
a) Is there a written risk management policy/framework, or operating principles?	Copy of risk management framework.	Copy of risk management framework.	Documentary review.
b) Does the PSE ensure all staff is informed of the risk management framework?	Memo, circulars on informing staff on risk management framework.	Copy of memos and circulars.	Documentary review.  Interviews with staff.
c) Is there a designated risk management	<ul style="list-style-type: none"> <li>Risk management coordinator/chief risk</li> </ul>	Copy of PSE organization structure.	Documentary review.

<b>Evaluation question</b>	<b>Indicators</b>	<b>Data to be collected</b>	<b>Methods/Tools of data collection</b>
unit/coordinator/champion to oversee the implementation of integrated risk management?	<p>officer/risk management unit.</p> <ul style="list-style-type: none"> <li>• Inclusion of Risk Management in PSE Organization structure.</li> <li>• Risk architecture in the risk management framework.</li> </ul>	Copy of risk management framework (see structure section).	Interview with risk management coordinator.
d) Does the PSE have a risk management committee, or similar?	<ul style="list-style-type: none"> <li>• Risk management committee.</li> <li>• Risk management roles. included in committee ToR.</li> </ul>	Copy of committee ToRs.	Documentary review. Interviews.
e) Does reporting on risk management take place through the existing management processes (e.g., performance reports, internal audit, etc.)?	<ul style="list-style-type: none"> <li>• Quarterly or annual Risk management reports.</li> <li>• Internal audit reports on risk management.</li> </ul>	Copies of risk management reports.	Documentary review.
f) Is the risk management process integrated into the strategic and operational planning?			
g) Does the PSE identify and encourage education, training and	Training reports on risk management.	Training reports.	Documentary reviews.

<b>Evaluation question</b>	<b>Indicators</b>	<b>Data to be collected</b>	<b>Methods/Tools of data collection</b>
development in risk management?	Attendance sheets.		Interviews with sample of trained staff.
h) Is the risk management framework reviewed at least annually?	Updated versions of risk management framework.	Old and newer versions of risk management framework documents.	Documentary reviews.
<b>3. Risk management processes:</b>			
a) Establishing scope, context and criteria:			
<ul style="list-style-type: none"> <li>Has the PSE implemented appropriate processes to identify both internal and external context?</li> </ul>	SWOT analysis in the strategic plan.	Review of the PSE strategic plan.	Documentary reviews.
<ul style="list-style-type: none"> <li>In determining context has the PSE considered both challenges and opportunities?</li> </ul>	SWOT analysis in the strategic plan.	Review of the PSE strategic plan.	Documentary reviews.
<ul style="list-style-type: none"> <li>Has the PSE risks been established with reference to the PSE's objectives and strategic planning?</li> </ul>	Risk Register – risk based on each of the PSE strategic plan/activities/targets.	Review of Risk Register.	Documentary reviews.
b) Risk identification:			
<ul style="list-style-type: none"> <li>Are the risks identified with reference to the PSE's strategic</li> </ul>	Link between risks and PSE objectives.	Comparison between strategic objectives in the Strategic plan vs.	Documentary reviews.

<b>Evaluation question</b>	<b>Indicators</b>	<b>Data to be collected</b>	<b>Methods/Tools of data collection</b>
objectives, and deliverables?		Objectives used in the Risk Assessment.	
<ul style="list-style-type: none"> <li>Does the PSE's identify both challenges and opportunities?</li> </ul>	Positive and negative risks in the Risk register.	Review of risks in the risk register.	Documentary reviews.
<ul style="list-style-type: none"> <li>Does the PSE consider both internal and external risks?</li> </ul>	Internal and external sourced risks in the Risk Register	Review of risks in the risk register.	Documentary reviews.
<ul style="list-style-type: none"> <li>Does the PSE consider all possible sources of risks?</li> </ul>	Categories of risks included in Risk Register (e.g., strategic, financial, compliance, technical, political, etc. risks).	Review of risks in the risk register.	Documentary reviews.
<ul style="list-style-type: none"> <li>Does risk identification involve appropriate stakeholders?</li> </ul>	<ul style="list-style-type: none"> <li>List of participants in risk assessment workshops.</li> <li>List of respondents in risk assessment questionnaire.</li> </ul>	List of participants and correspondents.	Review of risks in the risk register.
c) Risk analysis:			
<ul style="list-style-type: none"> <li>Does the PSE have documented procedures to analyses the likelihood and impact of each risk?</li> </ul>	Written guidelines/procedures for risk assessment.	Review of risk management framework/procedures section.	Documentary reviews.
<ul style="list-style-type: none"> <li>Does the PSE conduct appropriate analysis of</li> </ul>	Samples of risk assessment sheets/matrices showing	Risk assessment sheets/matrices.	Documentary reviews.

<b>Evaluation question</b>	<b>Indicators</b>	<b>Data to be collected</b>	<b>Methods/Tools of data collection</b>
the causes and consequences of risks?	causes and consequences sections.		
<ul style="list-style-type: none"> <li>Are risk analyses adequately documented?</li> </ul>	Copies of filled-in risk assessment sheets.	Risk assessment sheets/matrices.	Documentary reviews.
<ul style="list-style-type: none"> <li>Has the PSE examined and evaluated existing controls in terms of their strengths and weaknesses?</li> </ul>	Copies of risk assessment sheets showing: <ul style="list-style-type: none"> <li>-inherent risks</li> <li>-current controls (with strengths and weaknesses)</li> <li>-residual risks.</li> </ul>	Risk assessment sheets/matrices.	Documentary reviews.
<ul style="list-style-type: none"> <li>Are appropriate levels of management and employees involved in the risk analysis process?</li> </ul>	Attendance schedules including <ul style="list-style-type: none"> <li>-senior managers,</li> <li>-heads of departments</li> <li>-etc.</li> </ul>	Invitation letters and attendance lists.	Documentary reviews.  Interviews with participants.
d) Risk evaluation:			
<ul style="list-style-type: none"> <li>Are risks within the PSE prioritized to ensure treatment of the highest risks is considered first?</li> </ul>	Risk Heat maps showing Risk status.	Risk register – summary of risk profile.	Documentary review.
e) Risk treatment:			
<ul style="list-style-type: none"> <li>Has the PSE fully integrated into its operational plans or established risk treatment plans?</li> </ul>	Inclusion of risk treatment activities in plans and Budgets.	Budgets and operational plans.	Documentary reviews.

<b>Evaluation question</b>	<b>Indicators</b>	<b>Data to be collected</b>	<b>Methods/Tools of data collection</b>
<ul style="list-style-type: none"> <li>Are the managing risks and associated controls assigned to particular officer within the PSE?</li> </ul>	Presences of Chief risk officer/risk management coordinator.	Review of risk management governance structure.  Meeting with person responsible for risk management.	Documentary review.  Observation/interview.
<ul style="list-style-type: none"> <li>Does the PSE have a documented contingency plans or disaster recovery and business continuity?</li> </ul>	Documented contingency plan or Disaster recovery programs.	Review of contingency or disaster recovery plans.	Documentary reviews.
<ul style="list-style-type: none"> <li>Are internal controls/strategies developed and documented to treat identified risks?</li> </ul>	Risk Registers.  Risk treatment action plans.	Copies of current Risk Register and Treatment action plans.	Documentary reviews.
<ul style="list-style-type: none"> <li>Are strategic risks been assigned specific treatment and are these shared with other PSEs?</li> </ul>	Communications or MoU with other PSEs.	Copies of MoUs and communications with other PSEs.	Documentary reviews.  Interviews.
f) Monitoring and review:			
<ul style="list-style-type: none"> <li>Does the PSE have a regular reporting system for progress of implementation of risk treatment plans?</li> </ul>	Written reporting procedures and responsibilities in Risk Management Framework.  Risk treatment reports.	Risk management framework (roles and responsibilities section)	Documentary reviews.

<b>Evaluation question</b>	<b>Indicators</b>	<b>Data to be collected</b>	<b>Methods/Tools of data collection</b>
<ul style="list-style-type: none"> <li>• Does the PSE has a regular monitoring and review process to evaluate:               <ul style="list-style-type: none"> <li>○ Application of risk treatment plans in practice?</li> <li>○ Continuing relevance of treatment plans?</li> </ul> </li> </ul>			
<ul style="list-style-type: none"> <li>○ Application of risk treatment plans in practice?</li> </ul>	Risk treatment reports.	Review of risk treatment action plans.	Documentary reviews.
<ul style="list-style-type: none"> <li>○ Continuing relevance of treatment plans?</li> </ul>	Reviewed treatment plans.	Copies of reviewed risk treatment plans.	Documentary reviews.
<ul style="list-style-type: none"> <li>• Does the PSE have regular/annual review of the risks and risk register?</li> </ul>	Annual Reviewed/Updated Risk Registers and Treatment Plans.	Updated Risk Register	Documentary reviews.
g) Communication and consultation			
<ul style="list-style-type: none"> <li>• Is there a risk management reporting system in place to ensure all relevant parties are kept informed of risks and treatment progress?</li> </ul>	Reporting procedures stipulated in Risk Management Framework. Risk management reports.	Risk management framework (procedure section) Sample of risk management reports at various levels.	Documentary reviews.
<ul style="list-style-type: none"> <li>• Are all staff aware of their responsibilities with respect to risk management?</li> </ul>	Communication/seminar to staff.	Testimonials from staff. Internal memos to all staff about risk	Documentary reviews. Interviews with staff.

<b><i>Evaluation question</i></b>	<b><i>Indicators</i></b>	<b><i>Data to be collected</i></b>	<b><i>Methods/Tools of data collection</i></b>
		management responsibilities.	
<ul style="list-style-type: none"> <li>Is there regular communication between head of internal audit unit and risk management coordinator, or audit/risk committee?</li> </ul>	Letters/reports/memos from internal audit/chief risk officer/audit committee	Copies of letters/reports/memos from internal audit/chief risk officer/audit committee	Documentary reviews, Interviews.
<ul style="list-style-type: none"> <li>Does the risk management coordinator/chief risk officer have access to audit committee/risk management committee?</li> </ul>	Attendance of risk coordinator in Audit Committee meetings.  Invitation letters to audit committee meetings.	Attendance schedules in audit committee meetings.  Testimonials from risk management coordinator on his/her attendance/invitation.	Documentary reviews.  Interviews.
<b>INPUTS:</b> Risk management framework is developed and implemented with due consideration of available human and financial resources, organizational structure and internal and external environment.			
<b><i>Evaluation question</i></b>	<b><i>Indicators</i></b>	<b><i>Data to be collected</i></b>	<b><i>Methods of data collection</i></b>
1. Is the PSE having a system of monitoring its external environments?	SWOT analysis in strategic plan.	Review of strategic plan for consideration of external environment assessment.	Documentary reviews.

<b><i>Evaluation question</i></b>	<b><i>Indicators</i></b>	<b><i>Data to be collected</i></b>	<b><i>Methods/Tools of data collection</i></b>
2. Is there a strategic fit between internal potential and external opportunities?	SWOT analysis in strategic plan.		
3. Are there adequate financial resources set aside for risk management?	Risk management activities in PSE budget.	Review of PSE Budget.	Documentary reviews.
4. Are there specific expertise or skilled built among official responsible for coordinating risk management in the PSE?	Number of training offered/short courses attended by staff responsible for risk management. Certificates of attendance.	Review of training reports/ certificates of attendance. Testimonial from staff attended courses.	Documentary reviews. Interviews with staff responsible for risk management.

## Template 16: Risk Maturity Assessment Questionnaire

**RISK MATURITY ASSESSMENT QUESTIONNAIRE**

<b>ATTRIBUTE</b>	<b>LEVELS<sup>13</sup></b>	<b>FEATURE</b>	<b>TICK<sup>14</sup></b>
1. ERM-based approach	0	No recognized need for risk management process, no formal responsibility for risk management.	
	1	Corporate culture has little risk management accountability. Risk management not consistent.	
	2	Risk culture is enforced by policy interpreted as compliance. One area has used ERM. ERM is based on few champions.	
	3	ERM risk plans are understood by management and the organization. Most areas use ERM process and report on risk issues. Process owners take responsibility of risks.	
	4	Risk culture is associated and career advancement. Risk issues are understood at all levels and risk plans are conducted.	
	5	Risk culture is analysed and reported as a systematic. Executives' sponsorship is strong. ERM is embedded in each business function. All areas use risk management best practices.	
2. ERM process management	0	There is little recognition of the ERM process's importance.	
	1	There are no standard risk management criteria. Risk management roles and responsibilities are only informal.	
	2	Management recognizes a need for ERM process. Risk mitigations are sometimes identified but not often executed.	

<sup>13</sup> Maturity levels i.e., 0 = Non-existent, 1 = Ad hoc, 2 = Initial, 3 = Repeatable, 4 = Managed, 5 = Leadership.

<sup>14</sup> Tick only one box on each attribute of a maturity level i.e., 0 to 5.

ATTRIBUTE	LEVELS <sup>13</sup>	FEATURE	TICK <sup>14</sup>
	3	ERM accommodates all business areas. ERM process is a process of steps to identify, assess, evaluate, mitigate, and monitor. Senior management actively review risk plans.	
	4	Risk management is clearly defined and enforced at each level. ERM is coordinated with managers' active participation. Periodic reports measure ERM progress for stakeholders, including the Board (where applicable).	
	5	ERM is a management aspect, is embedded in all business processes and strategies. The PSE uses and ERM process that improves decision-making and performance.	
3. Risk appetite	0	The need for formalizing risk tolerance and appetite isn't understood.	
	1	Risk management lacks the portfolio view of risk. Risk management is just for meeting compliance requirements.	
	2	Risk management is only implied within senior management and not understood outside senior leadership. There is no ERM Framework for resource allocation.	
	3	Risk assumptions within management decisions are clearly communicated. There is structure for evaluating risks on an enterprise-wide basis.	
	4	Risk appetite is considered in each ERM step. Risk is managed by process owners.	
	5	The management team and risk/audit committee define risk tolerance levels for all departments. Risk appetite is examined periodically as part of planning.	
4. Root cause discipline	0	The effects of risky events might be identified but not linked to objectives/goals.	

ATTRIBUTE	LEVELS <sup>13</sup>	FEATURE	TICK <sup>14</sup>
	1	Risks are not consistently evaluated. Risk indicators and goals are not organized.	
	2	The cause-and-effect chain of risk from top-down and bottom-up is not defined or understood. No organized scheme for risk indicators as a core for risk management framework.	
	3	The cause-and-effect chain of risk from top-down and bottom-up is understood. The ERM is organized around root-cause risk categories (e.g., internal people, external environment, systems, etc.).	
	4	Terminology and classification of collecting risk is fully implemented. Operational, financial, and strategic risks' root-cause drivers are investigated, defined, quantified and routinely monitored.	
	5	There is an obvious focus on root cause to achieve goals and maximize risk's upside. The organization uses post-mortem to deconstruct past events into root cause categories. It is a proactive risk management, rather than problem management.	
5. Uncovering risks	0	There might be a belief that most of the important risks are known, although there is probably little documentation.	
	1	Risk is owned by specialists, centrally or within a department. Risk information is incomplete or dated so there is high risk of misinformed decisions.	
	2	Formal lists of risks for each department are part of the ERM process. Risk indicators are collected centrally, based on past events.	
	3	An ERM team manages a growing list of business area specific risks. Risk indicators are collected by most process owners. Standard criteria for impact and likelihood are used.	

ATTRIBUTE	LEVELS <sup>13</sup>	FEATURE	TICK <sup>14</sup>
	4	Process owners aggressively manage a growing list of business area specific risks locally to create context for risk assessment activities.	
	5	Internal and external best practices, support function, business lines and regions are systematically. Process owners regularly review and recommend risk indicators that best measure their areas' risks.	
6. Performance management	0	No formal framework of indicators and measures of goals and management exists.	
	1	Not all goals have measures and not all measures are linked to goals. Compliance is focused on satisfying external oversight bodies.	
	2	The ERM process is separated from strategy and planning. Motivation for management or support areas to adopt a risk-based approach is lacking.	
	3	The ERM process contributes to strategy and planning. All goals have measures. Risk management criteria are part of management's performance evaluation. Employees understand how risk-based approach helps achieve their goals.	
	4	The ERM process is an integral part of strategy and planning. Risk is aggressively considered as part of strategic planning. Employees at all levels use risk-based approach to achieve goals.	
	5	The ERM process is an important element in strategy and planning. Individuals, management, departmental, divisional, and corporate goals are linked with standard measures.	
7. Business resiliency and sustainability	0	Resilience and sustainability are limited to an IT infrastructure orientation of continuity and disaster recovery.	

ATTRIBUTE	LEVELS <sup>13</sup>	FEATURE	TICK <sup>14</sup>
	1	Management is aware of resilience-related risks and focuses on infrastructure rather than business. The response to major disruption is reactive.	
	2	The organization recognizes that broader planning's importance, highlights the business aspect of disaster recovery.	
	3	Resilience and sustainability are part of every risk plan and considered in each ERM process step.	
	4	A comprehensive approach to resilience considers people, external, relationship, system and process aspects. Logistics, security, resources, and organization of response procedures are well documented.	
	5	All issues are framed within the context of continuity of services to all stakeholders.	

## Glossary of Terms

In these guidelines, unless the context indicates otherwise, the following terms mean:

<b>Term</b>	<b>Definition</b>
<i>“Accounting Officer”</i>	In this Guideline means Permanent Secretary (for Ministries); Head of Independent Department or Agency (for Departments and Agencies); Chief Executive Officers (for Parastatal Entities); Regional Administrative Secretary (for Regional Secretariats) and Council Directors (for Local Government Authorities).
<i>“Audit Committee”</i>	It is a specialist, independent oversight body established to review and give advice to the highest level of governance on the control, governance and risk management within the public sector entity.
<i>“Consequence”</i>	The outcome of an event affecting objectives should the risk occur. (A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives. Consequences can be expressed quantitatively or qualitatively. A consequence can escalate through cascading and cumulative effects).
<i>“Control”</i>	A measure that maintains and / or modifies risk. Controls include, but are not limited to, any process, policy, device, practice, or other conditions and /or actions which maintain and/or modify risk. Controls may not always exert the intended or assumed modifying effects.
<i>“Corporate Governance”</i>	Refers to the set of systems, principles and processes by which the entity is governed. They provide the guidelines as to how the entity can be directed or controlled such that it can fulfil its goals and objectives in a manner that adds to the value of the entity and is also beneficial for all stakeholders in the long term.
<i>“Inherent Risk”</i>	The level of risk associated with the entity, or the individual system being examined before considering the effectiveness of controls.
<i>“Key risk”</i>	A Key risk is a risk or combination of risks that can seriously affect the performance, future prospects or reputation of the entity. These should include those risks that would threaten its business model, future performance, solvency or liquidity. The term can be used interchangeably significant risk.

<i>“Level of risk”</i>	The magnitude of a risk or combination of risks expressed in terms of the combination of consequences and their likelihood.
<i>“Likelihood”</i>	A chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically.
<i>“Public Sector Entity”</i>	The term “Public Sector Entity” has been used in these Guidelines to include all Tanzanian Public Sector Institutions: Ministries, Departments, Agencies, Parastatal Entities, Embassies, Regional Secretariats and Local Government Authorities that are required to or expected to implement sound risk management systems.
<i>“Principal Risk Owner”</i>	A person who is ultimately accountable for ensuring risk is managed appropriately.
<i>“Residual Risk”</i>	The level of risk associated with the entity as a whole, or the individual system being examined after considering the effectiveness of controls.
<i>“Risk acceptance”</i>	It is an informed decision to take a particular risk. Accepted risks are subject to monitoring and review.
<i>“Risk Analysis”</i>	The process to comprehend the nature of risk and to determine the level of risk based on the assessment of the likelihood of the risk occurring and the consequences should it occur. The velocity, proximity, and frequency of risk should also be considered if they are relevant to assessing the risk.
<i>“Risk Appetite”</i>	The amount of risk, on a broad level, an entity is willing to accept in pursuit of value.
<i>“Risk assessment”</i>	The overall process of risk identification, risk analysis and risk evaluation.
<i>“Risk avoidance”</i>	Informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk.
<i>“Risk champion”</i>	A person who by virtue of his/her expertise or authority champions a particular aspect of the risk management process but is not the risk owner.
<i>“Risk criteria”</i>	A set of terms of reference against which the significance of risk is evaluated. It can be derived from standards, laws, policies and other

	requirements. Risk appetite and risk tolerance are terms also used to describe risk criteria.
<i>“Risk description”</i>	A structured statement of risk usually containing four elements: sources, events, causes and consequences.
<i>“Risk drivers”</i>	A factor that has a major influence on risk.
<i>“Risk identification”</i>	Is the process of finding, recognizing and describing risks. It involves the identification of risk sources, events, their causes and their potential consequences.
<i>“Risk Management Framework”</i>	Set of components that provide the foundations and organizational arrangements for integrating, designing, implementing, evaluating and improving risk management across the entity.
<i>“Risk Management plan”</i>	A scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk. Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities. The risk management plan can be applied to a particular product, service, process and project, and part or whole of the entity.
<i>“Risk Management Policy”</i>	A statement of the overall intentions and direction of an entity related to risk management.
<i>“Risk Management”</i>	Coordinated activities to direct and control an organization with regard to risk.
<i>“Risk Owner”</i>	A person accountable for managing a particular risk within an entity.
<i>“Risk Register”</i>	A record of information about identified risks related to a specific entity activity.
<i>“Risk source”</i>	An element that alone or in combination has the potential to give rise to risk.
<i>“Risk Tolerance”</i>	Means the boundaries of acceptable variation in performance related to objectives.
<i>“Risk Treatment Action plan”</i>	A plan which shows how the proposed risk mitigation will be implemented.
<i>“Risk Treatment”</i>	It is the process of selection and implementation of measures to modify risk.

<i>“Risk Universe”</i>	All the possible risks that an entity is exposed to.
<i>“Risk”</i>	The effect of uncertainty on objectives. An effect is a deviation from the expected. It can be positive, negative or both, and create or result in opportunities and threats. Objectives can have different aspects and categories and can be applied at different levels.
<i>“Stakeholder”</i>	A person or entity that can affect, be affected by, or perceive themselves to be affected by a decision or activity.
<i>“Uncertainty”</i>	It is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

APPROVED