Republic of Zimbabwe

Risk Management Framework and Guidelines for the Public Sector

Issued by the Ministry of Finance and Economic Development, January 2023

Table of Contents

FOREWORD

I am pleased to introduce the Risk Management Framework and Guidelines for the Public Sector. Its implementation will mark a major achievement in helping government institutions manage their risks to achieve the desired objectives.

Statutory Instrument 135 of 2019, Public Finance Management (General) Regulations section 50 mandates Ministries, Departments, and Agencies (MDAs) to adopt Risk Management to promote a coherent approach towards the adoption of Risk Management and to understand the requirements for managing risk. Treasury has released this Risk Management Framework and Guidelines as an element of good corporate governance in the public sector.

The effective management of risks assists public sector entities to:

i. Set and achieve strategic objectives;
ii. Proactively anticipate and manage risks;
iii. Comply with legal and policy obligations;
iv. Improve decision-making;
v. Allocate and utilise resources effectively.

The process for managing risk should be logical, systematic, and embedded in strategic planning, decision-making, and performance management. All public sector entities must ensure that risk management is an integral and ongoing part of their management process.

Further, it is important for all of us to understand that the responsibility for risk management vests at all levels of management and is not limited to the Accounting Officer, Management, and the Internal Audit. Therefore, the decision-making processes must at all times consider both risk and reward whilst meeting the needs and expectations of our stakeholders and partners.

I, therefore, implore Ministries, Departments, and Agencies to ensure the implementation of risk management within the public sector which will result in the efficient and effective delivery of services.

Hon. Prof. M. Ncube

Minister of Finance and Economic Development

PREFACE

The public sector operations are becoming increasingly more complex. In the context of this growing complexity, the significance of effective risk management becomes more and more essential to the achievement of public sector objectives as enunciated in the national development strategies. The adoption of pro-active risk identification, analysis, evaluation, treatment, management and communication of key organisational or program risks to those charged with governance aids in enhancing efficiency in public sector operations and service delivery.

Statutory Instrument 135 of 2019, Public Finance Management (General) Regulations section 50 states that Ministries, Departments and Agencies (MDAs) shall adopt Risk Management hence the production of these guidelines for the public sector.

The framework is based on ISO 31000 and all Ministries, Departments and Agencies are expected to have risk management policies modelled along ISO 31000 which will improve their practices in risk management. The guidelines set a standard in Ministries, Departments and Agencies to ensure uniformity in implementing risk management.

These guidelines provide an overview of the stakeholders on risk management responsibilities, the services it provides and the relationships with key stakeholders. Ministries, Departments and Agencies are expected to observe these guidelines in order to embed risk management in operations. It is expected that all Accounting Officers, Chief Executive Officers, and those charged with governance, understand these guidelines and appreciate their roles in risk management.

Government of Zimbabwe is committed to enterprise-wide risk management to ensure its corporate governance responsibilities are met and its strategic goals are realized. Due to the volatility of the operational environment Treasury shall review these guidelines from time to time and issue operational instructions in the form of circulars.

George T. Guvamatanga

Secretary for Finance and Economic Development

DEFINITION OF TERMS

Accounting Officer: Refers to the Secretary for a Ministry and Head of Government Departments, Agencies and Constitutional Entities.

Assurance Services: An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization.

Audit Committee: It is an independent committee constituted to review the control, governance, and risk management within the Government institution, established in terms of Section 84 of the Public Finance Management Act [Chapter 22:19].

Consequence: Is an outcome of an event affecting objectives expressed qualitatively or quantitatively.
It can be certain or uncertain and can have positive or negative effects on objectives.

Consulting Services: Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility.

Control: Any action taken by management, the Board and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.

Governance: The combination of processes and structures implemented by Ministries, Departments, Agencies and Boards to inform, direct, manage, and monitor the activities of the organization towards the achievement of their objectives.

Governing Board: It is an organization's apex body, such as a board of directors, supervisory board, head of an agency or legislative body, board of governors or trustees of a non-profit organization, or any other designated body of the organization. In the Government of Zimbabwe, it includes the highest-level governing body either as an individual or charged with the responsibility to guide and or oversee the organisation's activities and hold senior management accountable.

Enterprise-wide Risk Management (ERM): A structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.

Event: Is an occurrence or change of a particular set of circumstances. An event can be one or more occurrences and can have several causes. An event can consist of something not happening. An event can sometimes be referred to as an "incident" or "accident".

Facilitating: Working with a group and or individuals to make it easier for that group and or individuals to achieve the objectives that the group has agreed for the meeting or activity.

Impact: The degree of loss or damage that would result from an occurrence of the risk event.

Inherent Risk: Is the probability of loss based on the nature of an organization's business, without any changes to the existing environment.

Likelihood: A chance of something happening. It refers to the probability of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically such as a probability or a frequency over a given time period.

Monitoring: Involves continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected. Monitoring can be applied to a Risk Management Framework, Risk Management Process, risk or control.

Residual Risk: Refers to the remaining risk after risk treatment. Residual risk can contain unidentified risk. Residual risk can also be known as 'retained risk'. It is the risk remaining after implementing a risk management strategy. ***Residual Risk = Inherent Risk – Managed Risk - Transferred Risk***

Review: It is the activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives. Review can be applied to a Risk Management Framework, Risk Management Process, risk or control.

Risk: It is the effect of uncertainty on objectives. It is the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

Risk Identification: Is the process of finding, recognizing and describing risks.

Risk Analysis: It is a process to comprehend the nature of risk and to determine the level of risk. Risk analysis provides the basis for risk evaluation and decisions about risk treatment. Risk analysis includes risk estimation. It utilizes the likelihood and impact on occurrence of an event.

Risk Appetite: The level of risk that an organization is willing to accept.

Risk Assessment: Overall process of risk identification, risk analysis and risk evaluation.

Risk Attitude: Organization's approach to assess and eventually pursue, retain, take or turn away from risk.

Risk Champion: A champion of risk management is an officer who has a delegated authority to promote risk management awareness and benefits in an organization and advise management and staff on the actions they need to take to implement the Risk Management Framework.

Risk Evaluation: Is the process of comparing the results of risk analysis with risk criteria to determine whether the risk and its magnitude is acceptable or tolerable. Risk evaluation assists in the decision about risk treatment.

Risk Management: A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

Risk Management Framework: Is the set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization. It is the totality of the structures, methodology, procedures and definitions that an organization has chosen to use to implement its Risk Management Processes.

Risk Management Plan: Refers to a scheme within the Risk Management Framework specifying the approach, the management components and resources to be applied to the management of risk. It is a document prepared to show how risk management programs of an organisation will be rolled out.

Risk Management Process: Is the systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk.

Risk Management Policy: Refers to a statement of the overall intentions and direction of an organization related to risk management.

Risk Maturity: The extent to which a robust risk management approach has been adopted and applied, as planned, by management across the organization to identify, assess, decide on responses to and report on opportunities and threats that affect the achievement of the organization's objectives.

Risk Owner: Is the person or entity with the accountability and authority to manage a risk. Is the process owner or a senior officer responsible for the day-to-day management of the specific organizational process that may be impacted by the risk.

Risk Profile: It is a description of any set of risks. It arises from the process of risk assessment.

Risk Response: The action that an organization elects to manage individual risks.

Risk Register: A comprehensive list of the identified and evaluated risks describing their likelihood and potential impact and includes controls to mitigate or manage risks to acceptable levels.

Risk Source: Element which alone or in combination has the intrinsic potential to give rise to risk.

Risk Tolerance: The boundaries of risk taking outside of which the organisation is not prepared to venture in the pursuit of its long-term objectives.

Risk Treatment: Is the process taken by an organisation on how to modify risk.

Risk universe: The full range of risks which could impact, either positively or negatively, on the ability of the organisation to achieve its long-term objectives.

PART I: RISK MANAGEMENT

1.1 Introduction

Risk Management has been associated with the private sector until only a few years ago, when the concept was embraced by the public sector by some governments across the world. Managing risk is now a very important aspect of governance in both the public and private sectors as there has been increasing calls by various stakeholders to achieve objectives through robust risk management.

Recent developments across the world, and in Zimbabwe too, have exposed public sector institutions to volatile, uncertain, complex and ambiguous environmental situations that call for more risk management, transparency and accountability.

It is therefore prudent for Ministries, Departments and Agencies to adopt and execute a Risk Management Framework that will enable institutions to actively look for and respond to risks so as to achieve planned government objectives.

Public institutions are bound by their legal mandates to provide services or products in the interest of the public. Failure by public sector entities to effectively manage risks negatively impact the attainment of the government strategic, operational, reporting and compliance objectives at different entity levels. This places an extra duty of care on public sector administrators to make choices that contain risks within acceptable limits hence, risk management has now become part of good governance in the public sector.

1.2 What is Risk?

There is no one universally agreed definition of the terms 'risk' and 'risk management'. ISO 31000: 2018, Risk Management Guidelines, defines risk as "*the effect of uncertainty on objectives*" as set out in ISO Guide 73. COSO Enterprise Risk Management-Integrating with Strategy and Compliance, 2017, defines risk as "*the possibility that events will occur and affect the achievement of strategy and business objectives*".

Risk may be positive, negative or a deviation from the expected, and that risk is often described by an event, a change in circumstances or a consequence. Risk is measured in terms of impact and likelihood.

It is critical to define the relationship between risk and objectives as risks cannot be prioritized without knowing the objectives of the entity, which would enable appropriate mitigation strategies to be determined.

Estimating risks is fraught with uncertainty due to the challenge of forecasting the future with imperfect information. Risk factors including sources, potential events, their consequences and their likelihood interact to create uncertainty.

1.3 What is Risk Management?

ISO 31000: 2018, Risk Management Guidelines, defines Risk Management as *"the coordinated set of activities to direct and control an entity with regard to risk."* Risk management also refers to the process of identifying, assessing, managing and controlling potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives. Risk management does not mean elimination of risk, a task which would imply stopping business operations in its strictest sense. It focuses on identifying and assessing events that can disable organisations from achieving their objectives. Risk management is a valuable management tool which increases prospects of success through minimising negative outcomes and optimising opportunities.

Risk management also entails an understanding of the nature of risks and helping management to evaluate and treat risks to within risk tolerance limits thus reducing negative consequences and improving the probability of achieving entity objectives. In these guidelines, the term risk management has been used and has the same meaning as the term enterprise risk management.

While risk management was traditionally managed in silos, Enterprise Risk Management brings on board a variety of merits as defined in section 1.4 below. Enterprise Risk Management is applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives' (COSO 2003).

1.4 Merits of Enterprise Risk Management

Unlike traditional methods of managing risks which focused on specific departments or processes, Enterprise Risk Management can make a major contribution towards helping an organisation manage the risks to achieve its objectives. The benefits include:

i. Greater likelihood of achieving objectives
ii. Consolidated reporting of disparate risks at Governing Board level
iii. Improved understanding of the key risks and their wider implications
iv. Identification and sharing of cross business risks
v. Greater management focus on the issues that really matter
vi. Fewer surprises or crises
vii. More focus internally on doing the right things in the right way
viii. Increased likelihood of change initiatives being achieved
ix. Capability to take on greater risk for greater reward, and
x. More informed risk-taking and decision-making.

Sources: Institute of Internal Auditors Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management, 2009.

1.5 Risk Management Principles

According to ISO 31000:2018, Risk Management Process must satisfy a minimum set of principles:

i. Risk management protects value
ii. Risk management is an integral part of organizational processes
iii. Risk management is part of decision-making
iv. Risk management is systematic, structured, and timely
v. Risk management is based on the best available information
vi. Risk management is tailored
vii. Risk management is transparent and inclusive
viii. Risk management is dynamic, iterative, and responsive to change
ix. Risk management facilitates continual improvement and enhancement of the organization.

Sources: John Fraser Betty J. Simkins, ENTERPRISE RISK MANAGEMENT: Today's leading research and best practices for tomorrow's executives.

Ministries, Departments and Agencies should adopt these principles if their risk management efforts are to be successful.

1.6 Nature and Impact of Risk

Risks can impact an organisation in the short, medium and long term. These risks are related to operations, tactics and strategy, respectively. Strategy sets out the long-term aims of the organisation, and the strategic planning horizon for a Ministry, Department or Agency will typically be five (5) or more years for the National Development Plans. Tactics define how an organisation intends to achieve change. Therefore, tactical risks are typically associated with projects. Operations are the routine activities of the organisation.

Ministries, Departments and Agencies shall implement and maintain effective, efficient and transparent systems of risk management and internal control to achieve, among other things, the following outcomes needed to underpin and enhance performance:

i. more sustainable and reliable delivery of services
ii. informed decisions underpinned by appropriate rigour and analysis
iii. innovation
iv. reduced waste
v. prevention of fraud and corruption
vi. better value for money through more efficient use of resources, and
vii. better outputs and outcomes through improved project and programme management.

1.7 Why should Entities develop a Risk Management Framework?

Organisations should avoid managing risk in a manner which lacks consistency. A Risk Management Framework helps Ministries, Departments and Agencies to manage risks effectively through the application of systematic, consistent and pre-planned strategies across the entity.

PART II: RISK MANAGEMENT POLICY AND GUIDELINES

2.1 Introduction

This Risk Management Framework is meant to provide policy and guidelines on Risk Management to Ministries, Departments and Agencies under the Government of Zimbabwe.

The policy is crafted against a background of leading governance, risk and control standards and best practices with the International Organisation on Standardization guidelines on Risk Management (ISO 31 000) being the primary guideline.

This Framework takes cognisance of the Public Finance Management Act (Cap. 22:19), other Acts of Parliament, and various regulatory publications in as far as they regulate governance and give guidance on Risk Management practices and expectations in Ministries, Departments and Agencies.

The Framework also takes into account the positions articulated in various governance frameworks across the world which include but are not limited to the following:

i. Zimbabwe National Code of Corporate Governance
ii. King IV (South Africa)
iii. The Combined Code (United Kingdom)
iv. Sarbanes Oxley Act (United Sates of America)
v. International Corporate Governance Network, 2015.

Reference will be made to these persuasive guidelines, explicitly or by implication.

2.2 Guiding Legislation on Risk Management

The Public Finance Management Act (Chapter 22:19) Section 7(3), articulates the directive and control in this statement: "*For the purpose of effectively supervising the public resources of Zimbabwe, the Minister shall, subject to this Act and any other enactment, be responsible for the management of the Consolidated Revenue Fund and the supervision, control and direction of all matters relating to the public resources of Zimbabwe."* Section 78 (1)(x) further states that, "*Treasury may prescribe or issue instructions or directions to Ministries, whether individually or collectively, concerning financial management and control".*

Public Finance Management (General) Regulations (SI 135 of 2019) explicitly call all Ministries, Departments and Agencies to adopt Risk Management as articulated in the following sections:

Sec 50. (1) The Accounting Officer of a Ministry, Public Entity, and Constitutional Entity shall ensure that a risk assessment is conducted at least annually to identify emerging risks.

Sec 50. (2) A risk management strategy, which shall include a fraud prevention plan, shall be used to set internal audit priorities and to determine any changes to systems, processes, practices, and staff skills to improve controls and to manage risks.

Sec 50. (3) The risk management strategy shall be communicated to all officials to ensure that the strategy is incorporated into the work of the Public Entity, Ministry or Constitutional Entity.

2.3 Purpose of the Framework

The purpose of the Framework is to provide a consistent approach for Ministries, Departments and Agencies to develop institutional risk management frameworks and processes for efficient and effective management of risks throughout the public sector. The Framework also aim to support Ministries, Departments and Agencies to improve and sustain their performance by enhancing their systems of risk management to protect against adverse outcomes and optimise opportunities.

The guidelines serve the following purposes:

i. To reiterate the position of the Government of Zimbabwe's commitment to the adoption and implementation of risk management practices in all Ministries, Departments and Agencies.
ii. To appraise Accounting Officers and Governing Boards of Ministries, Departments and Agencies on the concept and principles of Risk Management and its importance on the achievement of objectives.
iii. To give guidance on how Ministries, Departments and Agencies should develop and implement their own Risk Management Frameworks.
iv. To give guidance to the public sector internal auditors on how they should provide independent assurance to the Governing Boards and Accounting Officers of their organisations.
v. To set a standard in Ministries, Departments and Agencies ensuring uniformity in implementing risk management, sensitise and train public officers on risk management

2.4 Adoption of Risk Management Standards and Guidelines

The Government of Zimbabwe developed these guidelines to guide Ministries, Departments and Agencies in implementing Risk Management.
This Framework is based on ISO 31000 and all Ministries, Departments and Agencies are required to have Risk Management Policies that are modelled along ISO 31000 and seek to improve their current practices in risk management.

2.5 Risk Management Implementation Requirements

Institutions shall, in accordance with these guidelines, implement and maintain effective, efficient, and transparent systems of risk management and internal control. Accounting Officers shall ensure that:

i. Each Ministry, Department and Agency has a Risk Management Policy that has been approved by its Accounting Officer.
ii. Each Ministry, Department and Agency has implemented a Risk Management Process which is in line with international standards for risk management.

iii. Each Ministry, Department and Agency shall make the Risk Management Process part of its strategic and operational planning process for all activities.
iv. Risk Management documents (covered in Section III) of this Framework are in place
v. Each Ministry, Department and Agency shall put in place processes for monitoring and reviewing risk management and governance systems.

2.6 Application of the Guidelines

These guidelines shall apply to all Ministries, Departments and Agencies. Their responsibilities of managing risks extend beyond the effective management of the entity's specific risks. Arrangements for addressing shared risks and national critical risks must be part of the entities risk management framework.

The Risk Management Framework is a guideline used to identify, eliminate and minimize risks. The Framework will lead to improved decision-making, evidenced by adoption and integration of risk management in strategic decision-making and operational monitoring processes.

The Government of Zimbabwe has adopted ISO 31000 Risk Management as a benchmark for risk management in all Ministries, Departments and Agencies.

Ministries, Departments and Agencies are expected to develop their systems of risk management by adopting the said principles, standards and adapting the models and operational practices to match their specific institutional requirements.

Ministries, Departments and Agencies shall, in addition to these guidelines, comply with risk management guidelines issued by their respective industry regulators.

2.7 Structure and Scope of the Guidelines

PART	TITLE	SCOPE
I	Risk Management	This introductory section takes the users through the basics of risk management in general.
II	Risk Management Guidelines	Provides for the general government policy statements, adopted standard, as well as implementation requirements and responsibilities.
III	Government Risk Policy Statement	The Government of Zimbabwe has taken a position with regards to the implementation of risk management. In this part of the guidelines, government requirements on risk management are outlined.
IV	Roles and Responsibilities	This section addresses the specific roles and responsibilities that various stakeholders play for risk management to be effective.
V	Risk Management Framework	This section explains the Risk Management Framework that the Government of Zimbabwe requires all Ministries, Departments and Agencies to comply with.
VI	Execution of the Risk Management Framework	This section gives procedural outlines of the specific tasks that are carried out during implementation of risk management. It addresses risk management requirements from establishing the context of the entity through risk treatment.
VII	Reporting on Risk Management	Governing Boards and Accounting Officers need to be given assurance regarding the effectiveness of risk management arrangements that will have been implemented by Ministries, Departments and Agencies. This part describes ways of providing such assurance and the need for such assurance.
VIII	Monitoring and Evaluation	This section of the guidelines gives brief guidance on the need for monitoring risk management systems and how continual improvements to the Risk Management Processes can be achieved.
IX	Appendices	This section provides samples and templates of essential documents for risk management.

2.8 Review of the Risk Management Guidelines and Framework

These guidelines are developed with a view to address risk management issues in a manner that captures contemporary challenges in Zimbabwe and the global world. It is therefore necessary that the Secretary for Finance, and the Head of the Central Internal Audit Unit (CIAU) set a timeframe for the review of these guidelines so that they remain relevant.

Changes in laws and regulations in specific sectors of government and industry, as well as changes in laws and regulations in other countries also trigger the need for changes to these guidelines.

PART III: ROLES AND RESPONSIBILITIES IN RISK MANAGEMENT

3.1 Introduction

Risk Management is a recent development that was initially adopted by the private sector until only a few years ago, when the concept was embraced by the public sector in some governments across the world. Since then, managing risk is now a very important aspect of governance in both the public and private sectors as there has been increasing calls by various stakeholders to achieve institutional objectives through robust risk management.

In implementing formal risk management, the main challenge that has stalled risk management practices over the whole world is the question of '*who should do what'* with regards to risk management roles and responsibilities. Many institutions in both the private and public sector have not addressed the question, leaving gray areas in the adoption and implementation of risk management.

It is therefore critical that Ministries, Departments and Agencies craft a policy that clarifies the roles and responsibilities of the governing body, senior management, and employees with regards to Risk Management in their institutions.

3.2 Roles and Responsibilities

Ministries, Departments and Agencies need to establish and assign clear risk management roles and responsibilities to different officers across the organisation. While risk management is a responsibility of everyone in an organisation, there is need to be very clear on the roles and responsibilities at senior level within the organisation.

The section below identifies key executives in a public sector organisation who are key to an effective implementation of risk management. While ISO 31000 outlines generic responsibilities for risk management, at organisation level there is need to customize these roles and responsibilities so that they are aligned to their organizations' structure and context.

3.2.1 Secretary for Finance

The Ministry of Finance and Economic Development is best positioned to drive the risk management agenda for the Government of Zimbabwe. To that end, the Secretary shall have the mandate to drive risk management on behalf of Government. The Secretary shall have the overall responsibility and accountability for ensuring effective Risk Management Processes across all public institutions in Zimbabwe.

3.2.2 Accounting Officers

At Ministries, Departments and Agencies level, it is the Accounting Officer who shall steer risk management and is accountable for the overall effectiveness of the Risk Management Process. The

Accounting Officer shall provide oversight on the crafting and execution of an appropriate Risk Management Framework that is suitable for the public organisation's core business, structure and context. Among other duties, the Accounting Officer has the following tasks:

i. Providing guidance to management in determining strategic approaches to risk and set risk appetite.
ii. Advising management in establishing an appropriate structure for risk management.
iii. Demonstrating an appropriate attitude through supporting the adoption and execution of effective risk management practices.
iv. Driving the design and implementation of the Risk Management Framework.
v. Assigning or delegating responsibilities for risk management to various officers across the organisation.

Leading management in the implementation of recommendations of various stakeholders with regards to addressing risk management challenges.

3.2.3 Ministry, Department and Agencies Audit Committees

The Audit Committee, shall have specific responsibilities that include oversight over the Risk Management Framework commensurate with the complexity of the Ministries, Departments and Agencies. This does not remove accountability for risk management from the Accounting Officer and Senior Management as they remain responsible for the final approval of the risk policy and risk management. The Committee has the following functions:

i. Oversight of risk appetite and risk tolerance.
ii. Review of policies and procedures relating to risk management governance, risk management practices and risk control infrastructure for the entity as a whole.
iii. Oversight over processes and systems for identifying and reporting risks and risk-management deficiencies, including emerging risks, on an enterprise-wide basis.
iv. Monitoring of compliance with the organisation's risk management governance, practices and risk controls.
v. Effective and timely implementation of corrective actions to address risk management deficiencies.

3.2.4 Ministry, Department and Agencies Senior Management

Senior management include all heads of functional departments, directors and chief directors. Functions of senior management with respect to risk management include executing their responsibilities outlined in the risk management strategy and integrating risk management into the operational routines. Management also has high-level responsibilities that include:

i. Executing their responsibilities as set out in the risk management strategy.
ii. Empowering officials to perform effectively in their risk management responsibilities through proper communication of responsibilities, comprehensive orientation and ongoing opportunities for skills development.

iii. Aligning the functional risk management methodologies and processes with the institutional process.
iv. Devoting personal attention to overseeing the management of key risks within their area of responsibility.
v. Maintaining a co-operative relationship with the Risk Coordinator and Risk Champion by providing risk management reports as and when requested.
vi. Maintaining the proper functioning of the control environment within their area of responsibility.
vii. Monitoring risk management within their area of responsibility.
viii. Holding officials accountable for their specific risk management responsibilities

3.2.5 Risk Management Coordinator

Each Ministry, Department and Agency shall appoint a Risk Coordinator with a delegated responsibility to run with risk management initiatives on a day-to-day basis. The Risk Coordinator's responsibilities shall include the following:

i. Leading in the development of the Risk Management Policy and keep it up to date.
ii. Documenting the internal risk policies and structures.
iii. Coordinating the risk management and internal control activities.
iv. Compiling risk information and preparing reports for the Accounting Officer.
v. Assisting the Accounting Officer in establishing specialist risk policies.
vi. Leading in the development of specialist contingency and recovery plans.
vii. Assisting and supporting investigations of incidents and near misses.

3.2.6 Head of Central Internal Audit Unit

The Secretary for Finance holds overall accountability for risk management across all ministries. The Secretary will be assisted by the Head of Central Internal Audit Unit in the implementation of risk management.

The Head of Central Internal Audit Unit shall be responsible for:
i. Championing the implementation of risk management practices across all Ministries, Departments and Agencies in Zimbabwe.
ii. Developing and issuing policies and guidelines regarding public sector risk management practices.
iii. Researching and providing support, training, resources, and guidance on best practices in risk management for the public sector.
iv. Monitoring and carrying out reviews and assessments on the adequacy and effectiveness of risk management in public institutions.
v. Carrying out oversight on risk management assurance by internal audit.

3.2.7 Heads of Internal Audit

The primary responsibility for risk management rests with the Accounting Officer in each Ministry, Department and Agency. The Internal Audit Activity shall be responsible for:

i. Giving assurance on the risk management processes.
ii. Giving the assurance that the risks are correctly evaluated.
iii. Evaluating risk management processes.
iv. Evaluating the reporting of key risks.
v. Reviewing the management of key risks.

The internal audit activity can also carry out legitimate internal audit roles as shown in the figure 1 below.
An Institute of Internal Auditors Position Paper, '*The Role of Internal Auditing in Enterprise-wide Risk Management',* provides an illustration that presents a range of risk management activities and indicates which roles an effective professional internal audit activity should and, equally importantly, should not undertake. It gives three categories of risk management responsibilities which internal audit can undertake.

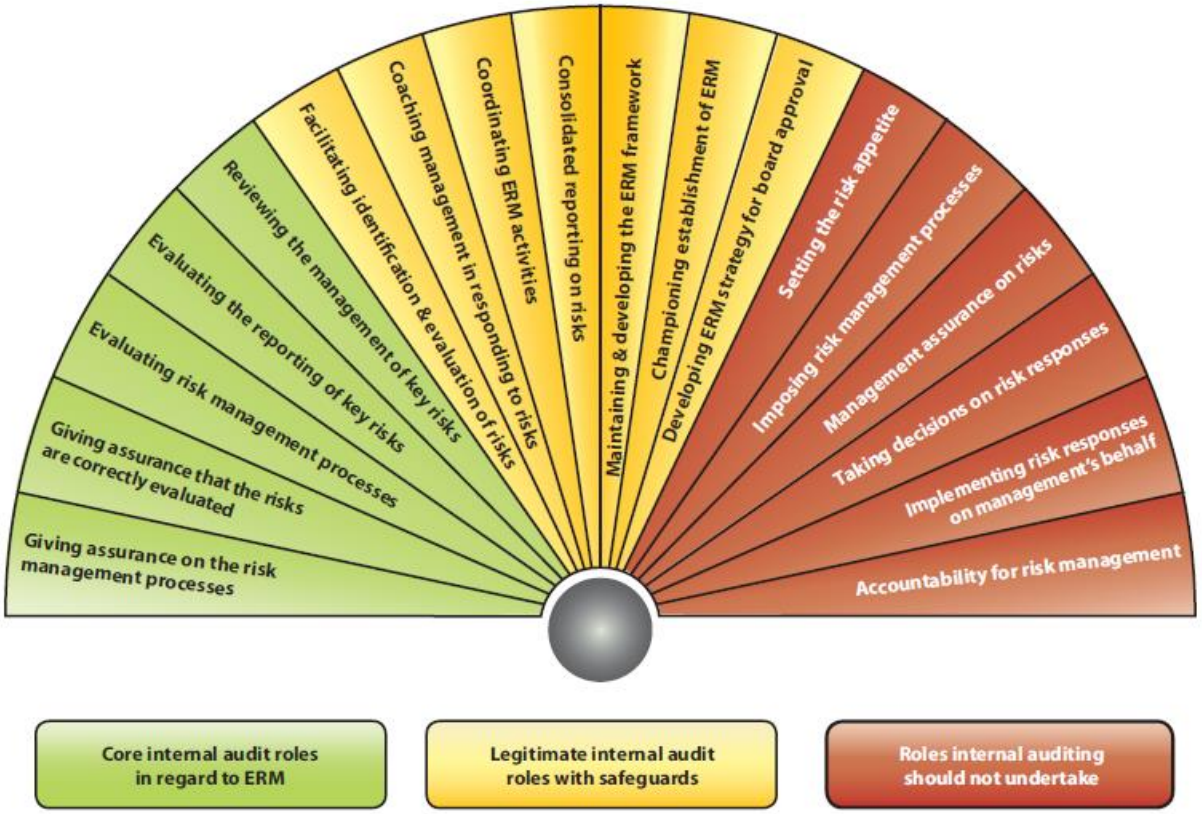

Figure 1: Internal Audit Role in ERM

Source: Internal Auditing's Role in Risk Management: Institute of Internal Auditors (2011).

3.2.8 Auditor General

By virtue of the powers and responsibilities vested in the Auditor General through the Constitution of Zimbabwe and the Public Finance Management Act (Chapter 22:19), the Auditor General's office gives assurance to government and the electorate with regards to risk management across all Ministries, Departments and Agencies. The Auditor General has the mandate to provide an

independent opinion on the adequacy and effectiveness of risk management in public sector organisations.

In expressing the audit opinion, the Auditor General:

i. Assesses whether the Risk Management Framework put in place by the Ministries, Departments and Agencies is appropriate.
ii. Assesses the effectiveness of the execution of the Risk Management Framework.
iii. Reviews the reporting and resolution of significant risks, including new and emerging risks, and
iv. Reviews the risk identification and evaluation process to determine if it is adequate to facilitate timely and accurate risk ratings and mitigation measures.

3.2.9 Risk Champions

Each functional department shall appoint a Risk Champion who will represent the department or unit and work closely with the Risk Management Cordinator. Risk champions act as the focal point between the department and the Risk Management Coordinator. Their responsibilities are outlined below:

i. Creating the risk management plan for specific units or departments based upon the Ministries, Departments and Agencies' standard risk methodology or on best practice international standards, for example ISO 31000.
ii. Facilitating the identification of risks through risk workshops, brainstorming sessions, interviews etc., using standard approved risk tools for the department or unit.
iii. Ensuring that each risk is assessed quantitatively, where appropriate, using risk quantification techniques.
iv. Taking part in any specific functional risk analysis reviews to ensure risks are understood and reflected in all risk analyses.
v. To be familiar with risk tools required to support the team, for example risk registers and the analysis tools that support risk analysis.
vi. Assisting in the development of risk responses (threat mitigation and opportunity realization) and associated actions and contingency plans for the unit or department.
vii. Providing support as required to risk owners to help them routinely and accurately report progress for the risk response plans and to complete their actions in a timely manner.
viii. Championing the process of risk management within the unit or department to ensure commitment to and energy for the risk management process.
ix. Contributing to the continuous improvement of risk management within the unit or department.

3.2.10 Employees of Ministries, Departments and Agencies

Employees are the most important stakeholder in risk management. Their responsibilities with regards to risk management are outlined below:

i. Familiarising themselves with the overall Risk Management Strategy, Risk Management Policy and the Anti-Fraud Strategy and Fraud Response Plan.
ii. Acting in accordance with the Framework.
iii. Acting within the risk appetite and tolerance levels set by the Governing Board.

iv. Adhering to the circulars, policies, and regulations.
v. Providing information and cooperation with other role players.
vi. Participating in risk identification and risk assessment within their section, department, and directorate.
vii. Implementing risk responses to address the identified risks, etc.

PART IV: RISK MANAGEMENT FRAMEWORK

4.1 Introduction

The success of risk management will depend on the effectiveness of the management framework which provides the foundation that will embed it throughout the organization at all levels. The framework assists in managing risks effectively through the application of the Risk Management Process at varying levels and within specific contexts of the organization.

The Risk Management Framework ensures that information about risks derived from the Risk Management Process is adequately reported and used as a basis for decision-making and accountability at all relevant organizational levels.

4.2 Elements of a Risk Management Framework

ISO 31000 describes the components of a risk management implementation framework. Figure 2 below provides a simplified version of this implementation framework. It includes the essential steps in the implementation and ongoing support of the Risk Management Process.

All Ministries, Departments and Agencies must come up with a Risk Management Framework that outlines the seven risk management components:

a. Mandate and commitment to the Risk Management Framework

i. Agreement in principle to proceed with the Risk Management Framework.
ii. Context for framework.
iii. Design of framework.
iv. Implementation plan.

b. Risk Management Policy

i. Policies for the Enterprise-Wide Risk Management framework, its processes and procedures.
ii. Policies for risk management decisions, that is. risk appetite, risk criteria and internal risk reporting

c. Integration of Enterprise-Wide Risk Management in the organization

d. Risk Management Process

i. Context.
ii. Risk identification.
iii. Risk assessment.
iv. Risk treatment.
v. Monitoring, review and actions.
vi. Communications and consultation.

e. Communications and reporting

f. Accountability

i. Risk ownership and risk register
ii. Managers' performance evaluation

g. Monitoring, review and continuous improvement

i. Responsibility for maintaining and improving Risk Management Framework
ii. Approach to continuous improvement of the Risk Management Framework.

Sources: John Fraser Betty J. Simkins, ENTERPRISE RISK MANAGEMENT: Today's leading research and best practices for tomorrow's executives.

These risk management guidelines provide further details to each of the elements of the Risk Management Framework.

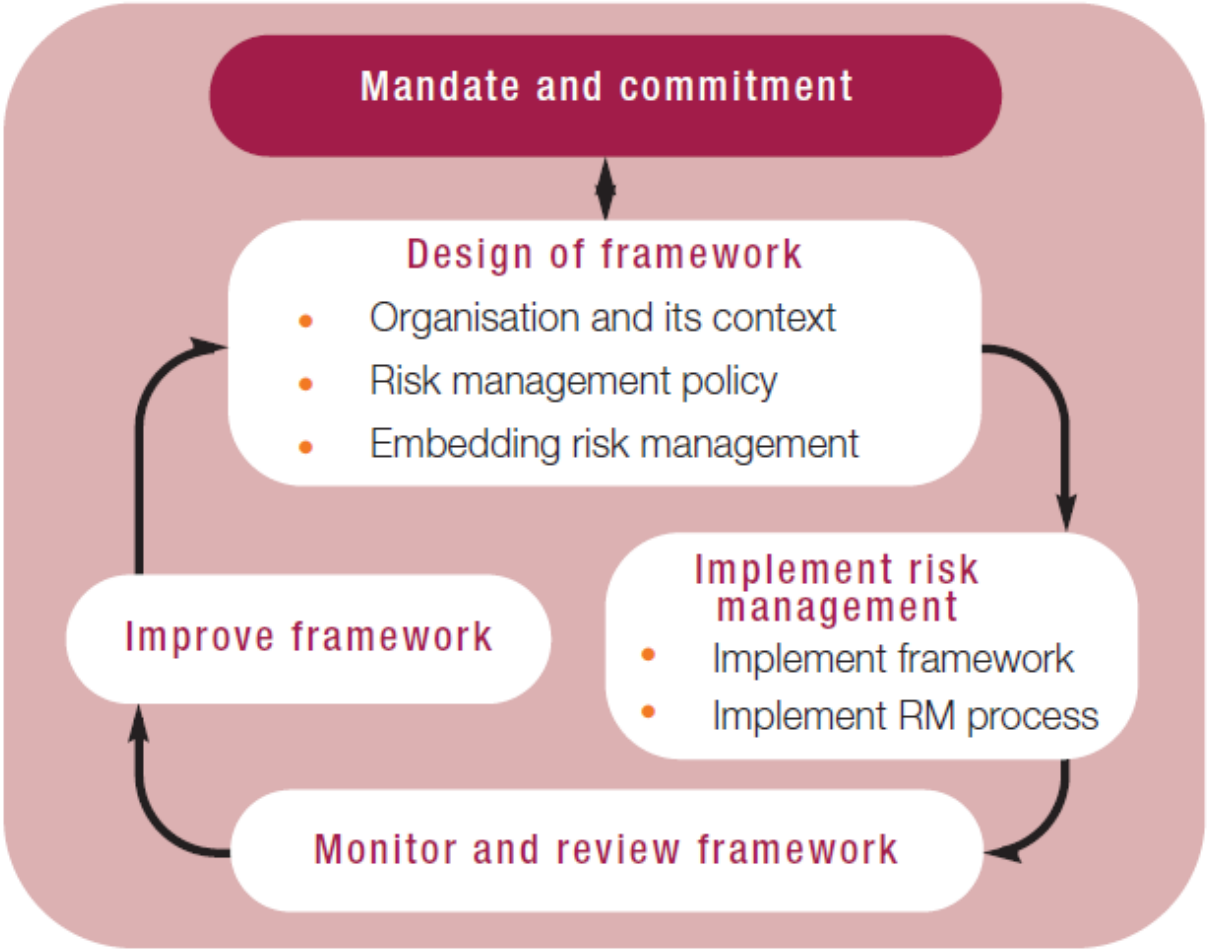

Figure 2: Framework for Managing Risk (ISO 31000)
Source: A structured approach to Enterprise Risk Management, AIRMIC, Alarm, IRM: 2010

4.3 How to develop a Risk Management Framework

The development of a Risk Management Framework should follow the generic method of coming up with conceptual frameworks in other areas of business.

The stages that should be followed in developing the Risk Management Framework are, by their order of implementation:

i. The formulation of a Risk Management Policy.
ii. The design of the risk management governance structure.
iii. The development of risk management procedures.
iv. Documenting the Risk Management Framework.
v. Getting top management approval and sponsorship.
vi. Creating risk management awareness and getting people-buy in.

These stages should be followed in the order outlined so as to ensure the involvement of the executives and Governing Boards at the right time.

4.4 Formulation of a Risk Management Policy

The Risk Management Policy should clearly state the organization's objectives for, and commitment to risk management. It should articulate the organization's rationale for managing risk as well as link the organization's objectives and policies and the Risk Management Policy.

The policy should also clarify accountabilities and responsibilities for managing risk and show a commitment to make the necessary resources available to assist those accountable and responsible for managing, measuring and reporting risks.

A Risk Management Policy should include the following sections:

i. Risk management and internal control objectives.
ii. Statement of the attitude of the organisation to risk (risk strategy).
iii. Description of the risk awareness culture or control environment.
iv. Level and nature of risk that is acceptable (risk appetite).
v. Risk management organisation and arrangements (risk architecture).
vi. Details of procedures for risk recognition and ranking (risk assessment).
vii. List of documentation for analysing and reporting risk (risk protocols).
viii. Risk mitigation requirements and control mechanisms (risk response).
ix. Allocation of risk management roles and responsibilities.
x. Risk management training topics and priorities.
xi. Review and monitoring of risks.
xii. Allocation of appropriate resources to risk management.

Source: A structured approach to Enterprise Risk Management, AIRMIC, Alarm, IRM: 2010

4.5 Crafting of the Risk Management Architecture

The policy should also describe the risk architecture of the organisation. It is vital that everyone is made aware of their risk management responsibilities, both individually and collectively.
The structure of each Ministry, Department and Agency has an effect on the Risk Management Architecture of the entity. Risk management roles and responsibilities should be designed, and it generally involves assigning tasks to the following:

i. The Governing Board

ii. Accounting Officer
iii. Audit Committee
iv. Risk Management Coordinator
v. Senior Management
vi. Risk Owners
vii. Risk Management Champions
viii. Other staff, contractors and stakeholders

Generic risk architectures for Ministries, Departments and Agencies are given in Figures 3 and 4 below, respectively. This helps identify relationships and responsibilities in risk management.

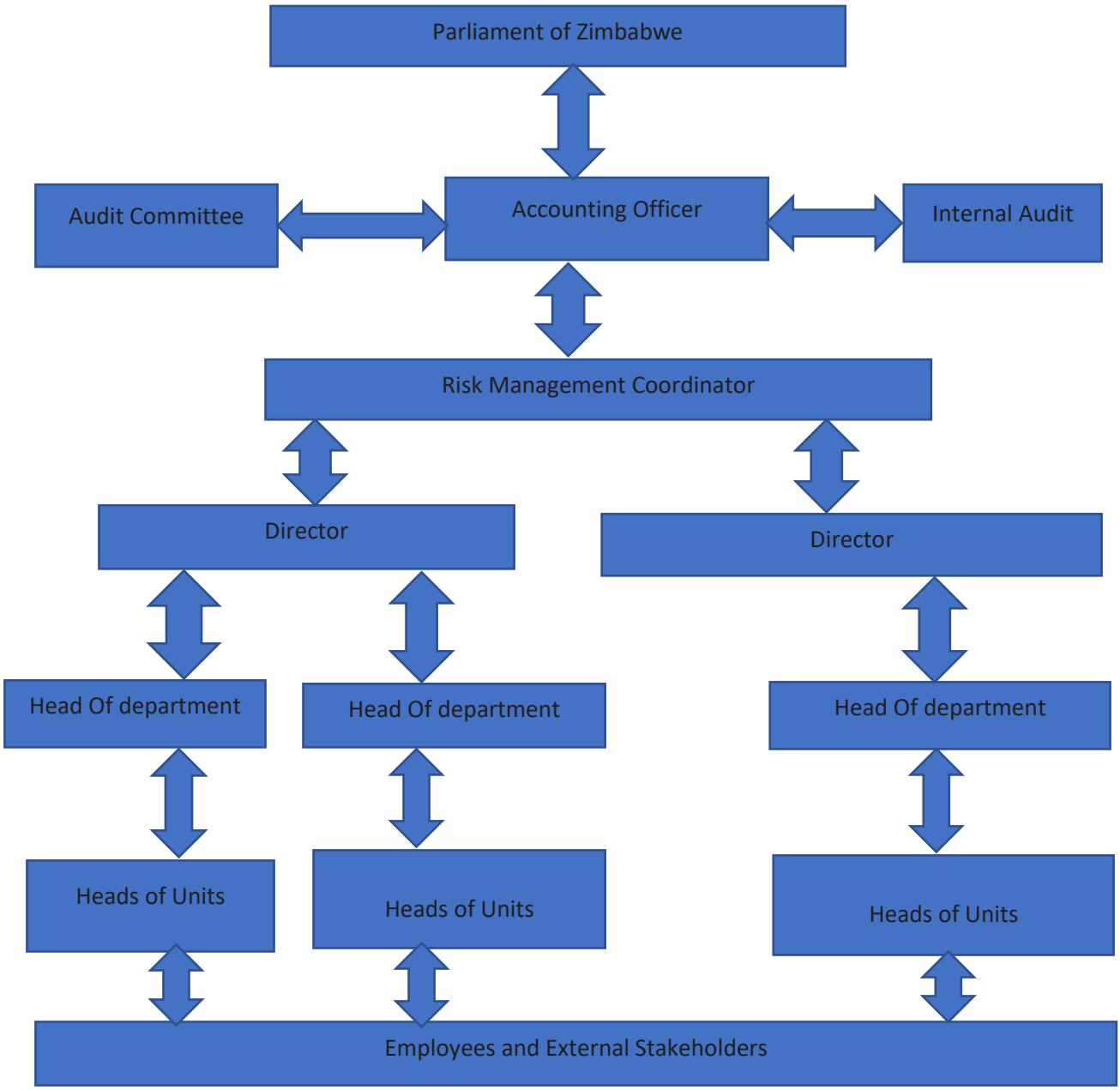

Figure 3: Ministry Risk Management Architecture
Source: Primary data

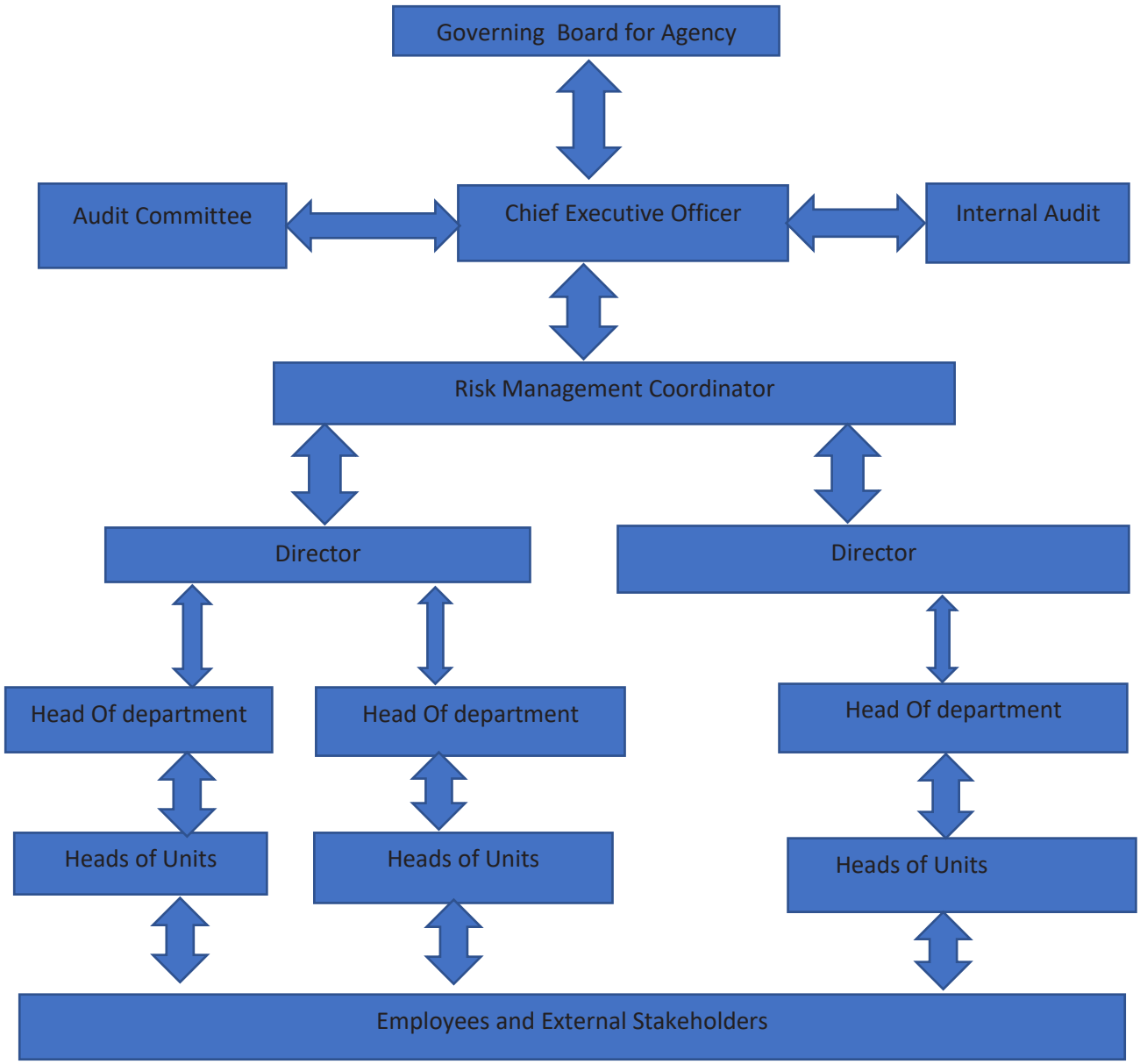

Figure 4: Agency Risk Management Architecture

Source: Primary data

4.6 Development of Risk Management Process

Risk management must be systematic and orderly. There is need to write down the specific processes and procedures that should be followed in carrying out risk management. The critical aspect is to start by crafting the Risk Management Process, followed by the detailed procedures. Figure 5 below shows the Risk Management Process as suggested by ISO 31000.

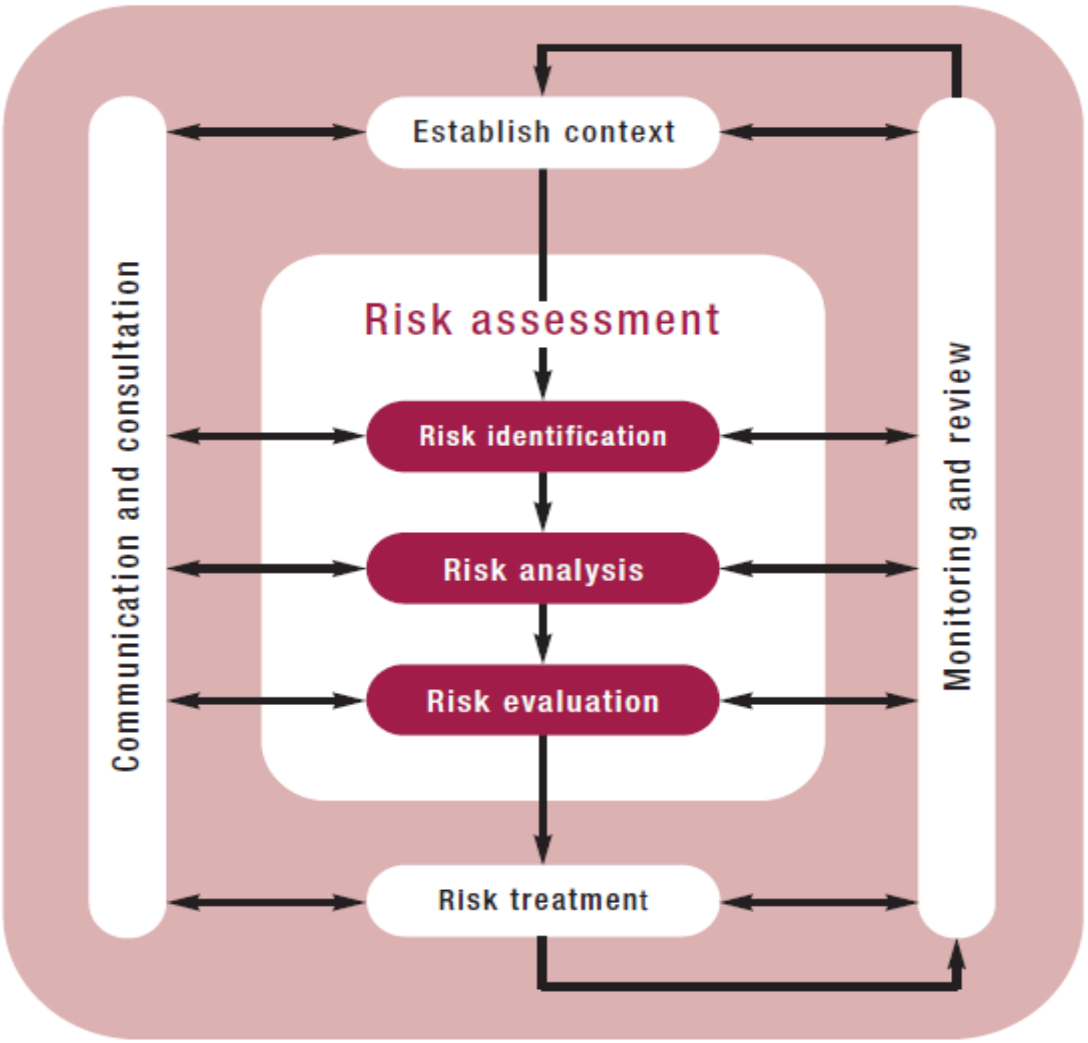

Figure 5: Risk Management Process (ISO 31000)

Source: A structured approach to Enterprise Risk Management, AIRMIC, Alarm, IRM: 2010

4.7 Documentation of the Risk Management Framework

For the purpose of effective guidance and accountability, the Risk Management Framework should be concisely documented, communicated and shared as widely as possible with stakeholders on a need basis. The document should succinctly clarify the following aspects;

i. The Risk Management Policy Statements (purpose, policy statements, principles).
ii. Risk Management Architecture.
iii. Risk Management Procedures which clarify the methodology in conducting risk assessments, treatment and reporting.
iv. Risk Management Templates for key documents.

4.8 Risk Management Framework Approval

Any risk management arrangements that Ministries Departments and Agencies wishes to put in place should be endorsed by those charged with governance.

Before submission to the Ministry of Finance, the Risk Management Framework must first be tabled before the Ministries, Departments and Agencies' Audit Committee by the Accounting Officer. The approval process should be subjected to the normal approval process for new policies and frameworks.

There is need for consultation before seeking approval of the framework. Various levels of each Ministry or organisation should be consulted with regards to the risk management proposals that will be under development.

4.9 Creation of Risk Management Awareness

After the approval of the Risk Management Framework, it is critical that appropriate awareness and training sessions are conducted so as to inform stakeholders of the risk management expectations and as well as building risk management skills across all Ministries, Departments and Agencies as per the requirements of the Risk Management Framework.

The Governing Board as well as all employees should be subjected to appropriate training on a need basis at different workshops so as to address the different roles and responsibilities of these participants. The workshops can be arranged to train participants as illustrated in the table below:

Category	**Objective of the training**
Governing Board Executive Directors	i. To inform the Governing Board of its risk management mandate ii. To create knowledge and awareness on risk management arrangements of the entity.
Management Employees Stakeholders	i. To provide an understanding of risk management in general ii. To create awareness of the entity's Risk Management Framework and the roles that participants should play. iii. To develop basic skills required in the Risk Management Process.

Table 1: Risk Management Workshops

PART V: EXECUTION OF RISK MANAGEMENT FRAMEWORK

5.1 Introduction

These guidelines have a wide range of components and this part shall focus on the Risk Management Process. These procedures require that the Ministries, Departments and Agencies to carry out the following;

i. Develop a plan to implement the Risk Management Framework.
ii. Link Risk Management Process and the strategic planning process.
iii. Conduct the Risk Management Process.
iv. Report on the implementations of risk management initiatives.

Each of the activities above are important aspects of the implementation which need appropriate communications and approvals as well.

5.2 Develop a Plan for Risk Management Implementation

Using the organisation's normal planning process, develop and seek approval of a risk management execution plan for the whole organisation. The plan should outline how you will implement your Risk Management Framework.

The risk management implementation plan should be concise but should outline the main activities that will be carried out to ensure successful execution of the risk management strategy. The plan shall cover the following aspects:

i. Timelines for the risk management rollout
ii. Assignment of roles in the implementation plan
iii. Resource requirements
iv. Deliverables of the whole process
v. Capacity building and training.

There is need for the Ministries, Departments and Agencies to develop an implementation plan suitable to their operations. The Governing Board or the Accounting Officer should play a pivotal role and assume accountability for the effective execution of the risk management plan. It is therefore necessary to have a Gantt Chart for the roll-out of risk management plan.

5.3 Link the Risk Management Process with Planning Process

Risk management serves the purpose of ensuring the achievement of objectives. Accordingly, there is need to intertwine the Risk Management Process with planning processes in the organisation. The importance of linking risk management and planning should be anchored on the premise that all planning should be preceded by risk assessments. This will ensure risks are managed at the appropriate level and in a proactive manner in the organisation.

5.4 Allocate Appropriate Resources for Risk Management

The organization shall allocate appropriate resources for risk management. The Risk Management Implementation plan shall clarify the resources necessary for effective management of risk in the specific Ministries, Departments and Agencies.
Consideration shall be given to the following critical resources:

i. People, skills, experience and competences.
ii. Resources needed for each step of the Risk Management Process.
iii. The organization's processes, methods and tools to be used for managing risk.
iv. Documented processes and procedures.
v. Information and knowledge management systems.
vi. Training programmes.

5.5 Conduct the Risk Management Process

The approved Risk Management Framework of Ministries, Departments and Agencies is the foundation of the Risk Management Process. The procedures to be carried out shall be benchmarked on the provisions of ISO 31000:2009 illustrated in figure 6 below.

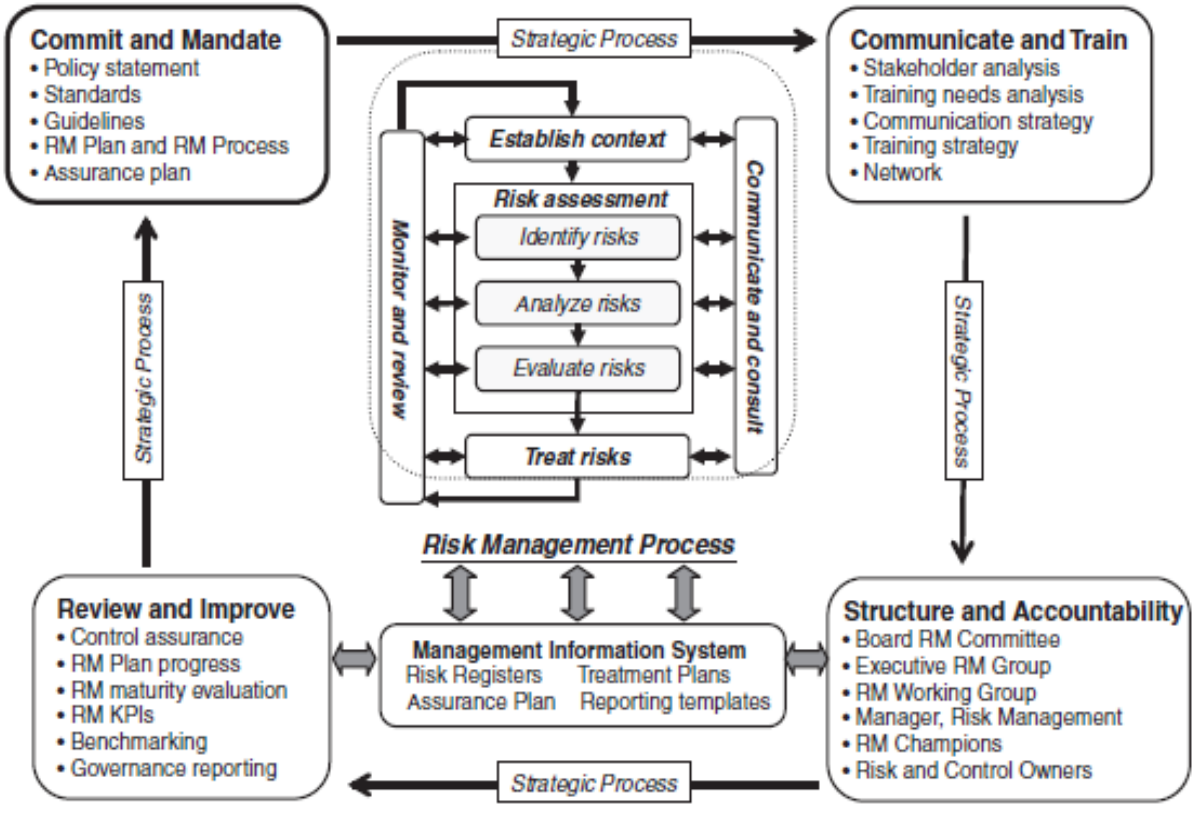

Figure 6: Framework for Implementing Risk Management (ISO 31000)

Sources: John Fraser Betty J. Simkins, ENTERPRISE RISK MANAGEMENT: Today's leading research and best practices for tomorrow's executives.

The implementation of each of the activities on figure 6 are detailed in the sections below.

5.5.1 Establish Context

Establishing the context involves defining the external and internal parameters to be considered when managing risk and setting the scope and risk criteria for the Risk Management Policy. It is concerned with five important aspects:

i. Understand the organisation's external context

This refers to the environment in which the organization seeks to achieve its objectives. The external context includes cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environments, etc. Understanding the external context is important to ensure that stakeholders and their objectives are considered when developing risk management criteria to address externally generated threats and opportunities.

ii. Understand the organisation's internal context

Refers to the internal environment in which the organization seeks to achieve its objectives. The internal context includes governance, organizational structure, roles and accountabilities; policies, objectives, and the strategies that are in place to achieve them; the capabilities understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies among other things). Understanding the organization is required before commencing any risk management activity as it identifies the goals and objectives of the organisation that may be affected by risk events.

iii. Develop your risk management context

Following an analysis of the internal and external context, the organisation must develop its own risk management context. In coming up with the context of the organisation, consider the following aspects:

a) The mandate of the organisation (objectives and strategies)
b) The structure of the organisation
c) Resources required.

The process of developing the organisation's context ensures that the risk management arrangements developed are appropriate for the achievement of organisational objectives.

iv. Set the organisation's Risk Appetite

Risk appetite is the amount of risk that the organisation is willing to accept in pursuit of the achievement of its objectives. Setting risk appetite shall take cognisance of the fact that an organisation should have several risk appetite statements relating to different risk exposures.

There is need for periodic review and setting of risk appetite due to changes in strategies, emerging risks and changes in the risk attitudes of the stakeholders. Setting risk appetite is the responsibility

of the Governing Board or Accounting Officer. The risk appetite statements must be communicated to appropriate employees across the organization and included in the strategic document.

v. Determine Risk Tolerance

All Ministries, Departments and Agencies must determine the extent to which they are prepared to accept or tolerate certain risks without developing further strategies to modify the level of risk. Risk tolerance is determined by the organisation's executive management and will depend on the organisation's internal and external context.

The following must be done in defining risk appetite:

i. Distinguish between risk appetite and risk tolerance. Avoid setting arbitrary risk tolerances that do not track back to an overall risk appetite or assume that a general statement of risk appetite gives decision-makers enough operational guidance to stay within its parameters
ii. The Audit Committee shall be available as a resource for helping senior executives understand and reconcile various views on risk within the organisation.

Table 2 below gives examples of risk appetite and tolerance statements.

Risk Appetite	**Risk Tolerance**
The organization has a higher risk appetite related to strategic objectives and is willing to accept higher losses in the pursuit of higher returns.	While we expect a return of 18% on this investment, we are not willing to take more than a 25% chance that the investment leads to a loss of more than 50% of our existing capital.
The organization has a low-risk appetite related to risky ventures and, therefore, is willing to invest in new business but with a low appetite for potential losses.	We will not accept more than a 5% risk that a new line of business will reduce our operating earnings by more than 5% over the next ten years.
A health services organization places patient safety amongst its highest priorities. The organization also understands the need to balance the level of immediate response to all patient needs with the cost of providing such service. The organization has a low-risk appetite related to patient safety, but a higher appetite related to response to all patient needs.	We strive to treat all emergency room patients within two hours and critically ill patients within 15 minutes. However, management accepts that in rare situations (5% of the time) patients in need of non-life-threatening attention may not receive that attention for up to four hours.
A retail company has a low-risk appetite related to the social and economic costs for sourced products from foreign locations that could be accused of being child sweatshops or having unhealthy working conditions.	For purchasing agents, the risk tolerance is set at near zero for procuring products that do not meet the organization's quality and sourcing requirements.

Table 2: Model Risk Appetite and Tolerance Statements

Source: Enterprise Risk Management — Understanding and Communicating Risk Appetite | Thought Leadership in ERM, COSO.

5.5.2 Defining Risk Criteria

The organization should define criteria to be used to evaluate the significance of risk. The criteria should reflect the organization's values, objectives and resources. Some criteria can be imposed by or derived from legal and regulatory requirements and other requirements to which the organization subscribes.

Risk criteria should be consistent with the organization's Risk Management Policy, be defined at the beginning of any Risk Management Process and be continually reviewed. When defining risk criteria, factors to be considered should include the following:

i. The nature and types of causes and consequences that can occur and how they will be measured
ii. How likelihood will be defined
iii. The timeframe of the likelihood and consequence
iv. How the level of risk is to be determined
v. The views of stakeholders
vi. The level at which risk becomes acceptable or tolerable.

5.5.3 Identify Risks

Risks associated with any decision must be identified and placed in a risk register or risk log before they can be treated, even if it is later determined that the risk levels with existing controls are acceptable.
It should be assumed that not all risks will be identified and like any of the Risk Management Process activities there needs to be provision for monitoring and review to add risks to the register.

Risk identification may use historical data, often categorized in terms of credit risks, operation risks, market risks, technological risks, human behavior risks, country risks, and other convenient mutually exclusive categories that assist in risk identification. The objective of risk identification is to generate a comprehensive list of risks based on those events and circumstances that might enhance, prevent, degrade or delay the achievement of the objectives. The following are the steps in risk identification:

i. Establish the strategic, tactical and operational objectives of the organisation.

Establishing the objectives of the organisation is a critical stage in risk identification since an event only qualifies to be a risk if it has some effect on the achievement of objectives.

ii. Collect information to identify a list of risks events.

Historical information about your organisation, industrial cluster or similar organizations is a starting point in risk identification. However, emerging risks also need to be identified to ensure completeness of the risk identification process. The risks associated with not pursuing opportunities should also be identified.

iii. Select risk identification tools and techniques

There are various techniques and tools which can be adopted by an organisation to carry out risk identification. The techniques or tools used should be suitable to the nature of activities undertaken by the Ministries, Departments and Agencies. Table 3 below summarises the tools and techniques that can be used by an organisation.

Technique	**Brief description**
Questionnaires and checklists	Use of structured questionnaires and checklists to collect information to assist with the recognition of the significant risks
Workshops and brainstorming	Collection and sharing of ideas and discussion of the events that could impact the objectives, stakeholder expectations or key dependencies
Inspections and audits	Physical inspections of premises and activities and audits of compliance with established systems and procedures
Flowcharts and dependency analysis	Analysis of processes and operations within the organisation to identify critical components that are key to success
HAZOP and FMEA approaches	Hazard and Operability studies and Failure Modes Effects Analysis are quantitative technical failure analysis techniques
SWOT and PESTLE analyses	Strengths Weaknesses Opportunities Threats (SWOT) and Political Economic Social Technological Legal Environmental (PESTLE) analyses offer structured approaches to risk recognition

Table 3: Risk Assessment Techniques
Source: A structured approach to Enterprise Risk Management, AIRMIC, Alarm, IRM: 2010

iv. Questions to ask during risk identification process

During identification of risks, there are key issues which the risk identifiers must raise questions on. Among the issues to question are:

a) Situations which increase or decrease the effective achievement of objectives
b) Situations that make the achievement of the objectives more efficient
c) Situations that cause stakeholders to take action that may influence the achievement
d) Produce additional benefits
e) When, where, why, how are these risks likely to occur and who might be involved or impacted?

v. Categorize the identified risks

An important part of analysing a risk is to determine the nature, source or type of impact of the risk. Evaluation of risks in this way may be enhanced using a risk classification system. Risk classification systems are important because they enable an organisation to identify accumulations of similar risks.

A risk classification system will also enable an organisation to identify which strategies, tactics and operations are most vulnerable.

Risk classification systems are usually based on the division of risks into those related to financial control, operational efficiency, reputational exposure and commercial activities. However, there is no requirement that Ministries, Departments and Agencies shall adopt a single risk classification system as they should choose what is best for them.

vi. Document the risks identified

Identified risk events must be documented in a Risk Identification and Analysis Sheet and each risk will have its own sheet. The Risk Identification and Analysis Sheets will be used as source documents to compile the Risk Register. The documentation must clarify the causes and impact of the risk events. The Risk Identification and Analysis Sheet and the Risk Register templates are illustrated in Table 9 and Table 10 in the Appendices, respectively.

5.5.4 Analyse Risks

Risk analysis involves developing an understanding of the risk. Risk analysis provides an input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. Risk analysis can also provide an input into making decisions where choices must be made, and the options involve different types and levels of risk.

Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. Factors that affect consequences and likelihood should be identified. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be considered.

The purpose of risk analysis is to provide the decision maker with enough understanding of the risk to ensure that they have the appropriate level of knowledge about the risk to make decisions on risk treatment and acceptance. Risk analysis methods can vary from quantitative mathematical models to qualitative expressions of expert opinions or even organized and structured gut feelings.

The following steps should be taken in risk analysis:

i. Identify and assess the effectiveness of existing controls

Controls should be considered based on:

a) Design effectiveness i.e. is the control 'fit for purpose' in theory and designed appropriately for the function for which it is intended
b) Operational effectiveness i.e. does the control work as practically intended.

Each risk, if identified and analyzed, is assessed by comparing the residual risk after risk treatment. The risk is then accepted as treated or not accepted and subjected to further risk treatment. The risks associated with controls and their implementation are also considered in the risk evaluation and the risk analysis.

ii. Determine risk likelihood and impact

The impact of an event and its likelihood should be assessed considering the effectiveness of the existing controls. In assessing impact and likelihood, the organisation must make use of the following sources among others:

a) Practical and relevant experience
b) Relevant published literature
c) Market research
d) Past records
e) Results of a survey or interview, and
f) Expert judgment.

In cases where no reliable or relevant past data is available, subjective estimates may be used to evaluate the risks.

iii. Rate the risk likelihood and impact:

Risk likelihood and impact can be rated on either a 3-band rating scale, a 5–band rating scale or other alternative rating scales. For starters, a 3-band rating scale is convenient as it not complex and reduces subjectivity. As the organisation matures, a more complex rating scale may be used to take care of different scales of risk impact or likelihood.

When using a 3-band rating scale, risks are rated as High, Medium or Low for both likelihood and impact as depicted on Table 4 below.

Number	**Impact**	**Likelihood**
3	High (H)	High (H)
2	Medium (M)	Medium (M)
1	Low (L)	Low (L)

Table 4: Risk Ratings in 3-Band Rating Scale

When using a 5-band rating scale, risks for both impact and likelihood are measured as Very High, High, Medium, Low, or Very Low as depicted on Table 5 below.

Number	**Impact**	**Likelihood**
5	Very High (*Catastrophic)*	Very High (*Almost certain)*
4	High (*Major)*	High (*Likely)*
3	Medium (*Moderate)*	Medium (*Possible)*
2	Low (*Minor)*	Low (*Unlikely)*
1	Very Low (*Insignificant)*	Very Low (*Rare)*

Table 5: Risk Ratings in 5-Band Rating Scale

Classification Guidance on Risk Impact

Rank	Score	Explanatory Note
Very High *(Catastrophic)*	5	• Non-delivery of services/ impact that would result in failure to achieve three or more of our strategic aims, objectives or key performance targets • Significant financial loss (e.g. budget reduction by 20%) • Multiple loss of life and/or loss of reputation or image that may take more than five (5) years to recover or involves litigation • Event that involves significant management time
High *(Major)*	4	• Non-delivery of services/ impact that would result in failure to achieve one to two of our strategic aims, objectives or key performance targets • High financial loss (e.g. budget reduction by 10%) • Multiple loss of life and/or loss of reputation or image that may take 2-5 years to recover or involves litigation • Event that involves relatively higher management time
Medium *(Moderate)*	3	• Partial delivery of services/ restricted ability to achieve one or more of our strategic aims, objectives or key performance targets • Moderate financial loss (e.g. budget reduction by 5%) • Moderate loss of life and/or loss of reputation or image that may take 1 year to recover
Low *(Minor)*	2	• Delivery of services with acceptable levels of problems/ some aspects of one or more of our strategic aims, objectives or key performance targets • Minor financial loss (e.g. budget reduction below 5%) • Event that involves little management time
Very Low *(Insignificant)*	1	• No impact • Insignificant financial Loss

Classification Guidance on Risk Likelihood

Rank	Score	Explanatory Note
Very High *(Almost Certain)*	5	• The adverse event will definitely occur, probably multiple times in a year.
High *(Likely)*	4	• The adverse event is expected to occur in most circumstances eg from 60% onwards chance of occurring in the next 12 months or 6 out of every 10 years. History of events in the institution or similar organizations.
Medium *(Possible)*	3	• The risk event should occur at sometime e.g. between 10%-59% chance of occurring in the next 12 months or between 2- 5 out of every 10 years. i.e. (50/50 chance of occurring within the next year).
Low *(Unlikely)*	2	• The risk event may occur only in exceptional circumstances e.g. below 10% chance of occurring in the next 12 months or once in 10 years
Very Low *(Rare)*	1	• Highly unlikely to occur in the next 5 years. No history of adverse event in the organisation

iv. Determine the overall risk rating

After the organisation has rated the likelihood and impact, the two elements are then combined to determine the overall risk rating. This is done by multiplying likelihood by the impact.

A 3-band rating scale would therefore have a maximum score of 9 and a lowest score of 1. Guidance on using the resultant risk rating is shown on the Table 6 below.

Table Risk status (Impact x Likelihood)	Color	Meaning and Response Required
1, 2	Green	Low concern; occasional monitoring. Tolerate; continue with existing measures and review annually.
3,4,5	Yellow	Moderate concern; steady improvement needed. Possibly review biannually
6,7,8,9	Red	Very serious concern; highest priority. Take immediate action and review regularly.

Table 6: 3-Band Risk Rating Scale

A 5-band rating scale would therefore have a maximum score of 25 and a lowest score of 1. Guidance on using the resultant risk rating is shown on the Table 7 below.

Total Risk/ Risk Status (Impact x Likelihood)	Description	Expression in Colour	Meaning and Responses
15-25	Extreme or severe	Red	Very serious concern; highest priority. Take immediate action and review regularly.
10-14	High	Light brown	Serious concern; higher priority. Take immediate action and review at least three times a year
5-9	Moderate	Yellow	Moderate concern; steady improvement needed. Possibly review biannually
1-4	Low	Green	Low concern; occasional monitoring. Tolerate/ Accept. Continue with existing measures and review annually.

Table 7: 5-Band Risk Rating Scale

5.5.5 Evaluate Risks

i. Develop Risk Heat map

Risk evaluation is the process of comparing the results of risk analysis with risk criteria to determine whether the risk and its magnitude is acceptable or tolerable. Risk evaluation assists in the decision about risk treatment. The output of a risk evaluation exercise is a prioritized list of risks that require further action.

Rank the risks using the Risk Heat Map (Risk Matrix), either qualitatively or quantitatively. This uses colour-codes with each colour indicating the level of risk. The Risk Heat map reflects the risk tolerance level of the organization. Figure 7 below depicts a model Risk Heat Map.

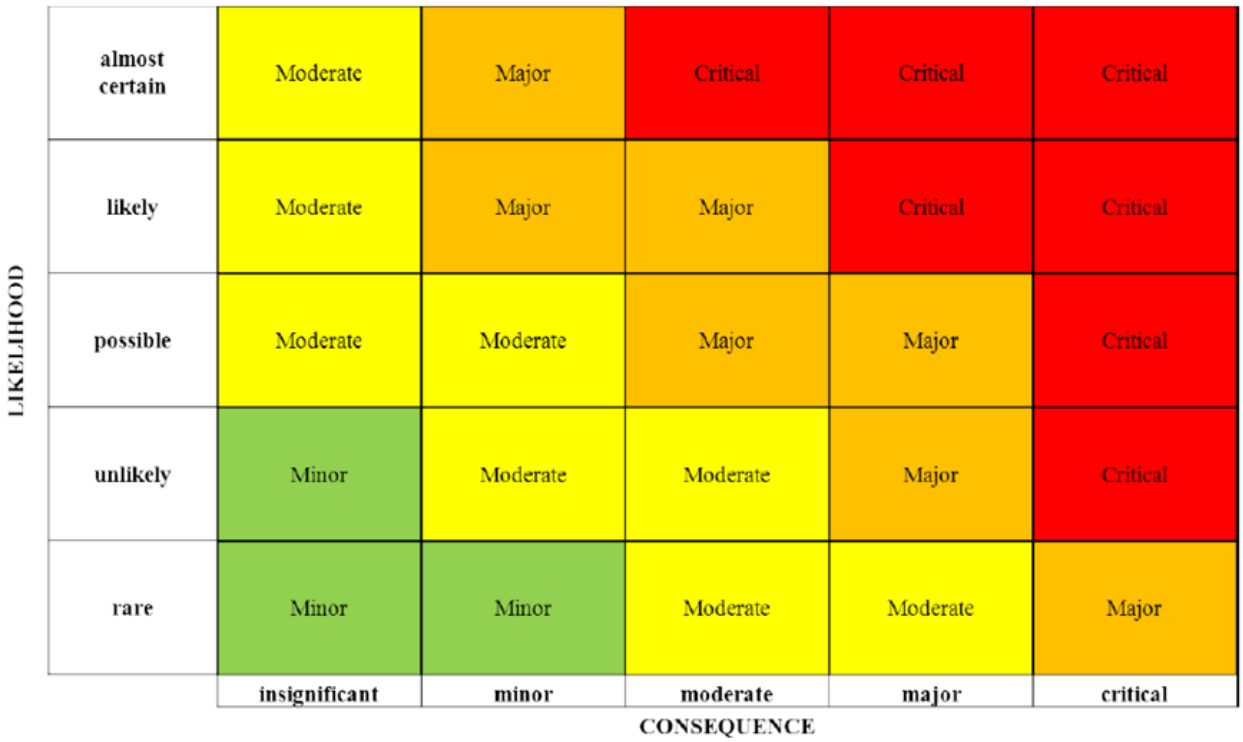

Figure 7: Model Risk Heat Map

ii. Draft the Top 'X' Risk Profile

The Ministries, Departments and Agencies shall identify, rank, and share the top risks they are facing. This is often called a 'Top X List'. The term 'Top X List' denotes a short yet important list of risks. It is easy to use because it is not an exhaustive list that confuses and often becomes unmanageable. The Ministries, Departments and Agencies shall keep the list simple and easy to communicate.

The 'Top X List' risk profile provides a ranked listing of the most significant risks facing an organization and likely to impact the organization's ability to meet its stated objectives. It helps to inform the allocation of resources to manage risks, both non-financial and financial. It also helps to advise the Governing Board on how to treat each significant risk.

5.5.6 Prepare a Risk Register

A Risk Register is a comprehensive list of the identified and evaluated risks describing their likelihood and potential impact and includes controls to mitigate or manage risks to acceptable levels. While the output of the risk assessment process is the Risk Identification and Analysis Sheets, the ultimate purpose of capturing the risks on those sheets is to populate the Risk Register.
The Risk Register allocates ownership and management of each risk to senior management to manage the risks identified. Table 10 in the Appendices shows a Risk Register template.

5.5.7 Craft and Execute Risk Treatment Strategies

i. Choose Risk Management Strategy

Risk Treatment refers to the process taken by an organisation on how to modify risk. The decision on how to treat risks should be based on a comprehensive understanding of how risks arise. Common risk treatment strategies are:

i. Avoiding the risk by deciding not to start or continue with the activity that gives rise to high risk.
ii. Taking or increasing risk in order to pursue an opportunity.
iii. Removing the risk source.
iv. Changing the likelihood.
v. Changing the consequences.
vi. Sharing the risk with another party or parties (including contracts and risk financing).
vii. Retaining the risk by informed decision.

The above risk management strategies can be graphically depicted as in Table 8 below.

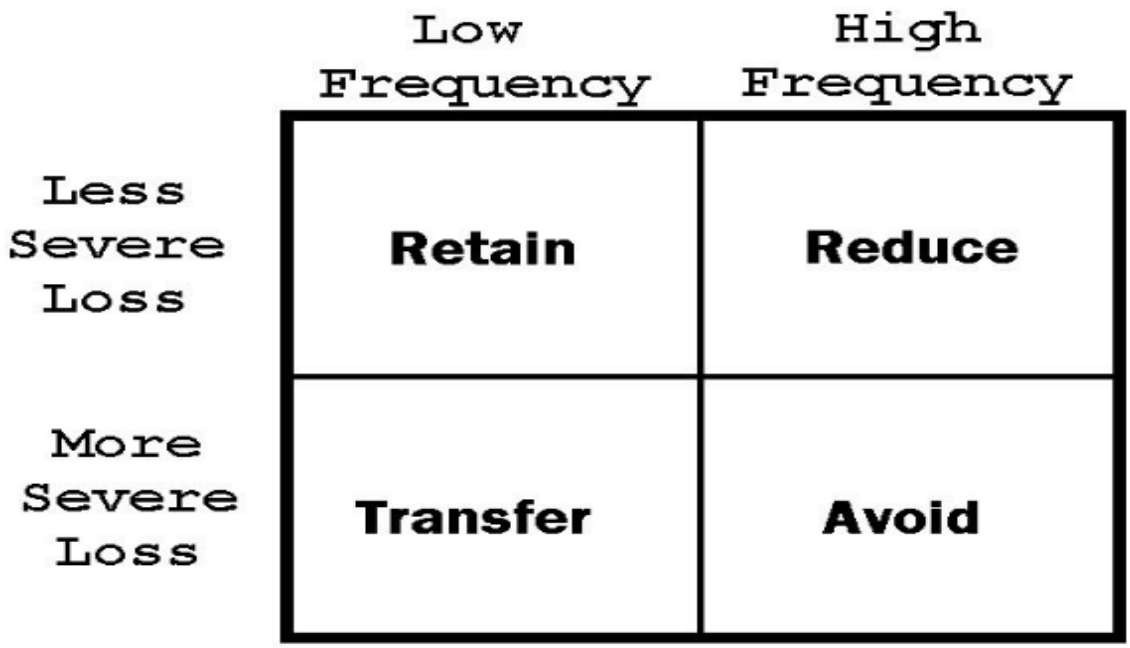

Table 8: Risk Management Strategies

ii. Accountability

The Risk Management Framework shall specify or have a process that will specify who is accountable for every identified risk in the organization as well as who is responsible for controls to treat the risk. Managers should have the authority for managing the risks or controls they are accountable for and their performance should be evaluated and appropriately rewarded.

Continuous improvement of the controls and the Risk Management Process is also part of ownership.
Everyone in the organization should know who 'owns' each risk or risk control and this is usually contained in a management information system consisting of a collection of risk registers, treatment plans, reporting templates, and assurance plans.

5.5.8 Communicate and Consult with Stakeholders

Because of the uncertainty about effects of risk on objectives, there is a strong incentive for communication and consultation. There must be extensive communications among team members, and consultations with other experts in the organization to ensure the accuracy and effectiveness of activities in the Risk Management Process in the Ministries, Departments and Agencies.

Like monitoring and reviewing, communication and consultation is a part of all the other tasks in the Risk Management Process. Communication improves the effectiveness of risk management for positive consequences as well as negative consequences. Communication and consultation are also key to success in risk assessment, treatment, and evaluation activities.

Effective communication and consultation on Risk Management Processes yield a wide variety of benefits to include the following:

i. Getting a common and better understanding of the context, risks and effects of risk treatments options.
ii. Building awareness and understanding about risks identified in the organization.
iii. Learning from both internal and external stakeholders.
iv. Influencing the target audience.

Communication and consultation should therefore be adequately provided for in terms of both resources and time.

PART VI: COMMUNICATION, CONSULTATION, AND REPORTING

6.1 Communication, Consultation and Reporting

Modern day governance is anchored on the principles of accountability, transparency and disclosure. Communication, consultation and reporting contribute to good governance as it provides information to Secretary for Finance, Accounting Officers, Governing Boards, Auditor General, Central Internal Audit Unit and Accountant General a regarding the organisation's risks management process and its effectiveness and adequacy. This information shall be used to support management decision-making.

6.1.1 Communication and Consultation

Each Ministry, Department and Agency shall implement arrangements to communicate and consult about risk in a timely and effective manner with both internal and external stakeholders throughout all the steps of the risk management process to inform decision making. Communication and consultation refer to, "continual and iterative processes that an organization conducts to provide, share or obtain information and to participate in dialogue with stakeholders and others regarding the management of risk," (ISO Guide 73).

i. Communication and consultancy cover the information relating to the existence, nature, form, likelihood, severity, evaluation, acceptability, treatment or other aspects of the Risk Management Framework adopted by the Ministry, Department and Agency. The information shall be shared with stakeholders to promote their understanding of risks, the basis on which some decisions are made and the reason why certain actions and accountabilities are required. Communication about the framework and its elements is needed both for internal and external stakeholders. This is necessary to inform and to be informed. Internal communications during the implementation of risk management are important to ensure that everyone in the organization knows what the Risk Management Framework is and what is expected of them.
ii. Consultation is a process of informed communication between an organization and its stakeholders on an issue prior to making a decision on a particular issue. It is a process not an outcome, which impacts on a decision through influence rather than power and about inputs to decision making, not joint decision making. Internal communication and consultation should be appropriately recorded.
iii. Continuous communication and consultation with appropriate internal and external stakeholders should be held throughout all the steps of the risk management process to improve the quality of decisions while making appropriate measures to protect the confidentiality and integrity of information.
iv. Providers of outsourced services and partners in public and private sectors have responsibilities to manage risks based on their contracts and service level agreements. Their responsibilities should extend to identifying and reporting risks to relevant risk owners and actively support risk mitigation strategies.

v. Each Ministry, Department and Agency shall implement arrangements to understand and contribute to the management of shared risks that extend across entities and may involve sectors, community, industry or administrative areas or jurisdictions.
vi. Ministries, Departments and Agencies shall make appropriate disclosures on risk management and internal control to contribute to fair balanced and understandable annual reports.

6.1.2 Risk Reporting

If the Governing Board has delegated primary risk oversight responsibility to a committee that committee should meet in executive sessions with the designated Risk Management Coordinator in a manner similar to the Audit Committee and its regular sessions with the Head of Internal Audit and with senior management in connection with key issues reported quarterly.

The Risk Management Coordinator and senior management must feel comfortable in informing the Governing Board or relevant committee of rapidly emerging risk exposures that require their immediate attention. The reporting channels must always be open as a complement to regular reporting procedures.

The committee charged with risk oversight should make regular reports to the Accounting Officer or Governing Board to keep them apprised of important changes in the Ministries, Departments and Agencies risk profile and exposure to key risks.

6.1.3 Special Reporting on Compliance Risk (Legal and Regulatory)

The Ministries Departments and Agencies Risk Management Framework must be designed on the basis of the enterprise-wide Risk Management Framework promulgated by ISO 31000. Executive management should therefore provide the Accounting Officer or Governing Board with a comprehensive review of the organisation's legal and regulatory compliance programs and how they affect the Ministries, Departments and Agencies risk profile.

There are principles to consider when assessing the adequacy of compliance efforts. There should be a strong and visible "tone at the top" emanating from both the Governing Board and senior management that emphasizes that non-compliance with corporate policy will not be tolerated. Actions of the Governing Board and the senior executive team should provide an unambiguous signal to the organization that policies and procedures are to be followed scrupulously.

The compliance program should be designed by individuals with the appropriate level of legal expertise. The Governing Board, Accounting Officer and Executive Management must review compliance policies periodically in order to assess their effectiveness and to make any revisions deemed prudent or necessary to conform to changes in applicable laws.

6.1.4 Principles of Effective Reporting

The following principles should be remembered when developing a risk reporting solution:

i. Reporting must be tailor-made. No single risk report style meets the expectations of all stakeholders in different Ministries, Departments and Agencies. There is need to tailor reports to address the needs of the specific organisation.
ii. Organizations with a mature Risk Management Framework may produce several customized risk reports to meet the needs of different stakeholder groups.
iii. Incorrect and incomplete risk identification, assessment, prioritization and treatment outputs will lead to ineffective risk management and risk reporting.
iv. Accounting Officer or the Governing Board will typically prefer a summary of risks and risk trends, focusing on high risk and strategic rather than providing too much information in risk reports.

In preparing reports on risk management, the Risk Management Coordinator must observe these principles to ensure effectiveness.

6.1.5 Preparation and Frequency of Reporting

The Risk Champions shall submit sectional risk reports to the Ministries, Departments and Agencies Risk Management Coordinator for consolidation and onward submission to the Governing Board or Accounting Officer. The Risk Management Coordinator must be responsible for coordinating and drafting risk reports to ensure consistency in standards and format.

The Risk Management Coordinator must ensure that there is a strong link between risk and the strategic document. The ultimate risk reports should reflect the relationship so as to get adequate attention for the Governing Board or Accounting Officer and ensure that risks are linked to strategic objectives and functions.

The general reporting requirement is that where there is a Governing Board which is required to have Governing Board meetings, a risk report must be produced for each Governing Board meeting. The frequency of risk reporting should be guided by the Ministries, Departments and Agencies regular internal reporting cycle, for example quarterly.
In an environment that is stable and where everything is constant, an organization can have the comfort of producing risk reports with much less frequency compared to an organisation operating in an environment full of uncertainties.

Risk reports shall be compiled using the 'Risk Management Quarterly Implementation Report' illustrated in Table 11 in the Appendices.

6.1.6 Content and Format of the Risk Dashboard

Risk reports should be tailored to suit the requirements and strategy of the organisation. However, there is need for Ministries, Departments and Agencies to include generic risk report components in their risk reports to the Governing Board, Accounting Officer and Senior Management.

The risk report should provide standard information for use by the Governing Board, Accounting Officer or Senior Management. The report should address risks relating to both strategic and operational level risks.

i. Strategic level risk report

Risk heat maps are used to show the top risks faced by the organisation in strategic risks reports. They are easy to understand as they are graphical illustrations. The reports should also provide a summarized implementation status of risk treatment action plans.

ii. Operational risk report format

When reporting operational risks, Ministries, Departments and Agencies shall use table format risk reports as they provide more detail. This is a summary of key components of the Risk Treatment Action Plans as illustrated in Table 12 in the Appendices.

Such reports are used by Audit Committees, Risk Coordinators and Risk Owners to monitor, manage, update, implement and review identified risks. By having drill down facilities, the details of risks can be provided as supporting information to summary executive reports. Risk reports in the form of tables or spreadsheets can be easily filtered or sorted to meet the reporting requirements of different stakeholders. They are also easy to modify as risk events change.

PART VII: MONITORING AND EVALUATION

7.1 Introduction

Feedback mechanisms are important in all aspects of an organisation's life**.** ISO 31000 recognises the importance of feedback by way of two mechanisms. These are Monitoring and Review of performance and Communication and Consultation. Monitoring and review ensure that the organisation monitors risk performance and learns from experience. Communication and consultation are presented in ISO 31000 as part of the Risk Management Process, but it may also be part of the supporting framework.

7.2 Risk Management Monitoring and Review

Monitoring and review together with risk communication and consultation are two Risk Management Process activities that are applied to the three "line" activities of context, assessment, and treatment. Monitoring and review are key to the continuous improvement of risk management and lead to observable actions towards improvements in risk management and subsequently to better decision making.

Every aspect of the Risk Management Process needs to be monitored and reviewed. Monitoring will see management asking questions such as listed below, among others:

i. Has the risk changed in character due to trends?
ii. Are there new risks evolving or emerging?
iii. Has the context for the risk management changed?
iv. Is the risk treatment plan being implemented as planned?
v. Are controls effective?
vi. What is the appropriate frequency of monitoring?
vii. Should monitoring be done by internal audit, third party, or self-assessment?
viii. Based on actual outcomes for objectives, was the risk assessment accurate?
ix. Can monitoring be improved by identifying better key performance indicators?

7.3 Performance Indicators for Risk management

Without setting key performance indicators for monitoring and evaluating effectiveness and adequacy of risk management, the implementation of risk management may be taken as a box-ticking exercise. There is need for Treasury to come up with key performance indicators for risk management processes in each Ministry, Department and Agency.

The Accounting Officers shall be evaluated by the Audit Committees on their performance in leading the risk management process through the following indicators among others:

i. Risk management maturity trend in the Ministry, Department and Agency as measured in terms of an appropriate Risk Management Maturity Model.
ii. Performance against key indicators, including comparison of year-on-year performance.
iii. Reactiveness to key risks when compared with prior year(s).

iv. Percentage change in unauthorized expenditure, wasteful expenditure and irregular expenditure based on year-on-year comparisons.
v. Percentage change in incidents and quantum of fraud based on year-on-year comparisons; and
vi. Progress in securing improved audit outcomes in regular and performance audits.

These key performance indicators should be set for the Accounting Officers and the process should be cascaded downwards for the various players in risk management.

7.4 Role of Internal Audit in Monitoring

ISO 31000 assigns the following three roles to the internal audit function with regards to risk management:

i. ***Giving Assurance***
The internal audit function gives assurance after assessing the control system's effectiveness and Risk Management Processes. This will help the auditor to conclude whether risks are correctly evaluated or not.

ii. ***Evaluating***
The internal audit function also evaluates Risk Management Processes for adequacy and also assesses if reporting of material risks is being done in an appropriate manner.

iii. ***Reviewing the management of material risks***
The internal audit function must perform risk-based auditing. In the process of auditing, auditors evaluate and review the Risk Management Process. Through such assessments, the internal audit function reports to the Audit Committee and Accounting Officer. Such reports by internal auditors are used to reconsider risk management arrangements for purposes of improvement.

7.5 Continuous Improvement

In the initial years of implementation, Risk Management Frameworks may be limited to areas with high benefits and ease of implementation. Even after several years of implementation, the framework will be in a state of change because of "continuous improvement" in the framework.
The effectiveness of risk management is usually monitored and continuously improved through a hierarchy of four review processes:

i. Self-evaluation by the individual manager, perhaps with cooperative assistance from other managers in a mutual mentoring situation.
ii. Internal audit of a department, including the functioning of risk management, particularly the Risk Management Process component (Risk Management Assurance).
iii. External audit of critical risks and controls often as a regulatory activity, for example, to ensure public safety.
iv. External review of risk management through participation by the organization in standards organizations and industry-wide user groups.

The organisational Enterprise Risk Management framework should specify a set of rules for determining the appropriate degree of oversight needed for individual risk or risk control owners. Monitoring and review of the framework on a periodic basis should look at the framework and the risk culture in the organization. Issues that should be asked among others are:

i. Is the framework implemented?
ii. Are the framework policies still appropriate?
iii. Do managers accept the framework as the norm?
iv. Are risk treatments reducing the effect of uncertainty on objectives?

Each Ministry, Department and Agency should ensure continual improvement in risk management through the setting of organizational performance goals, measurement, review and the subsequent modification of processes, systems, resources, capability, and skills. Risk management should use key performance indicators designed to measure success in meeting the organization's objectives.

7.6 Risk Management Training and Development

Ministries, Departments and Agencies must ensure they provide continuous education to members of Governing Boards, senior management and staff with the intention of keeping them abreast with best practices and current developments. The Accounting Officer and executive should develop plans to stay informed about developments in risk management practices and emerging risk areas.

The following guidelines can assist in developing education and training initiatives to:

i. Stay abreast of leading practices as risks evolve and as management updates its risk management methods.
ii. Understand new risks associated with new businesses and locations and how changes in regulations in foreign jurisdictions can increase or decrease risk.
iii. Periodically benchmark risk governance practices of peers, competitors, customers, and suppliers in order to understand evolving practices and expectations of business partners and investors.
iv. Keep up to date on risk disclosure requirements in external/public communications.
v. Offer orientation programs for new Audit Committee and Risk Committee members.

The initiatives that are identified during monitoring and review activities should be followed up and then included within the risk management strategy and plans.

PART VIII: APPENDICES

8.1 Risk Identification and Analysis Sheet

Risk title: Provide a brief title of the risk	**Risk ID: Provide a unique identity**

Overview	
Risk	Provide a brief description of the risk
Principal Risk Owner	Include title of the person managing the risk and the area where the risk fails.
Supporting owner(s)	Provide title of other persons affected by risk
Risk Category	Is it financial, technical etc. (see template)
Objective/plan	List the objective impacted by the risk

Details	
Causes *Provide the causes that may cause risk materiality*	***Consequence (s):*** *Provide description of what will happen if the risk materialize.*

Inherent risk analysis (tick the appropriate ratings basing on the scenario that current controls do not exist or completely fails.						
Inherent Risk	**Impact**	***VERY HIGH***	***HIGH***	***MODERATE***	***LOW***	***VERY LOW***
	Likelihood	***VERY HIGH***	***HIGH***	***MODERATE***	***LOW***	***VERY LOW***
Risk rating	**Impact x Likelihood**	• *Multiply the ratings from impact and likelihood* • *Shade this area with an appropriate colour (see the table 7 in section 3.3.6)*				

Key risk mitigation / controls currently in place and their weaknesses: -briefly describe the current controls existing to reduce the inherent risk, also point out the main weaknesses for the current controls.

Inherent risk analysis (tick the appropriate ratings basing on the scenario that current controls do not exist or completely fails.						
Inherent Risk	**Impact**	***VERY HIGH***	***HIGH***	***MODERATE***	***LOW***	***VERY LOW***
	Likelihood	***VERY HIGH***	***HIGH***	***MODERATE***	***LOW***	***VERY LOW***
Risk rating	**Impact x Likelihood**	• *Multiply the ratings from impact and likelihood* • *Shade this area with a appropriate colour (see the table 7 in section 3.3.6)*				

Actions / mitigation controls to be taken :(propose feasible treatment actions to be put in place to reduce the risk at tolerable levels, including resources required for each treatment action – financial, physical assets, or human)	
Treatment	**Resource required**
1.	1.
2.	2.
3.	3.

Table 9: Risk Identification and Analysis Sheet

8.2 Snapshot of a Risk Register

RISK REGISTER TEMPLATE

Ref	Objective	Strategic action	Risk Description	Consequence of risk on the objective	Likelihood rating	Impact rating	score (likelihood* impact)	Existing Management Controls	adequacy and effectiveness of Controls	Residual Risk	Additional Controls	Date of Execution	Risk Owner

Table 10: Snapshot of a Risk Register

8.3 Risk Management Quarterly Implementation Report

Department/Unit: .....
Risk Management Quarterly Implementation Report for the Quarter Ending.....
Prepared by: ..... Date: .....

Risk title & ID (From Risk Register in priority order)	**Proposed Treatment/Control Options** (From Risk Identification Sheet)	**Person Responsible for Implementation of Treatment Options** (as in the risk identification sheet)	**Time-table for Implementation** (Give specific start and end dates)	**How will this risk and treatment options be monitored**	**Status of Implementation** (completed, on-going, not done)	**Remarks and/or Comments**

Table 11: Risk Management Quarterly Implementation Report

8.4 Risk Treatment Action Plan

Department/Unit: .....
Date of review: ..... **Compiled by:** ..... **Date:** .....
Reviewed by: ..... **Date:** .....

Risk title & ID (From Risk Register in priority order)	Proposed Treatment/Control Options (From Risk Identification Sheet)	Person Responsible for Implementation of Treatment Options (as mentioned in the risk identification sheet)	Time-table for Implementation (Give specific start and end dates)	How will this risk and treatment options be monitored

Table 12: Risk Treatment Action Plan