PUBLIC SECTOR RISK MANAGEMENT GUIDELINES

November 2020
About these guidelines

These guidelines are for use by public officers in National and County Governments and their entities to enhance capacity and provide guidance in the implementation of risk management.

The guidelines have been developed to conform to the latest international risk management standards. Some text has been quoted from ISO 31000:2018 with permission of Kenya Bureau of Standards, a member body of the International Standards Organization.

Risk assessment tools and techniques are beyond the scope of these guidelines. Additional resources to assist entities in implementing risk management will be provided from time to time at the Public Sector Accounting Standards Board website www.psasb.go.ke and the National Treasury website.

Readers of the guidelines should refer to the glossary of terms provided to understand the meaning attributed to names, words and phrases used in these guidelines.

The guidelines were developed by the Public Sector Accounting Standards Board (PSASB) in collaboration with the Internal Auditor Generals’ department (IAGD) in the National Treasury.

For further information regarding these guidelines contact.

**Chief Executive Officer**
Public Sector Accounting Standards Board
CPA Centre, 8th Floor, Thika Road
P. O. Box 38821-00100
Nairobi, Kenya
www.psasb.go.ke
Email: auditstandards@psasb.go.ke

**Internal Auditor General**
The National Treasury
Treasury Annex (BIMA House, 7Th Floor)
P. O. Box 30007-00100
Nairobi, Kenya
Email: iag@internalaudit.go.ke
Foreword

The Constitution of Kenya 2010 established the frameworks for governance and accountabilities through Articles 10, 201, and 232. In these Articles, the Constitution is driving good governance through accountability.

In a risk averse, blame attributing society, accountability is often seen as a way of shifting responsibility. It should however, be a process that helps public entities and businesses manage risks, protect existing value, and enable further value-creation. A public sector entity is publicly accountable for its successes and challenges. This means demonstrating responsibility for its decision-making. But accountability is more than meeting regulatory requirements or explaining how things went wrong, it is about holding others to account and being accountable to others.

The Public Finance Management Act, 2012 and its attendant Regulations 2015 place a duty on Accounting Officers of all public sector entities, in both levels of government (national and county) to establish and maintain appropriate systems of risk oversight and management for their entities.

To promote a coherent approach to discharging these duties and to assist public sector entities to understand the requirements for managing risk, the National Treasury is releasing this Risk Management Guideline as an element of the Public Management Reform Agenda (PMRA).

One of the guiding principles of the PMRA is that ‘engaging with risk is a necessary first step in improving performance’, and one of the lasting benefits that the reforms are seeking to deliver is ‘a more mature approach to risk across the public sector. To this effect, the Government released the Mwongozo Code of Governance for State Corporations.

The effective management of risks assists public sector entities to:

- Set and achieve strategic objectives;
- Comply with legal and policy obligations;
- Improve decision making; and
- Allocate and utilise resources effectively.

These guidelines have been developed to provide a framework for efficient and effective management of risks in public sector entities, in both levels of government.

The purpose of this policy guide is to set out broad guidelines to the public sector entities to establish risk management policy, risk management framework, and risk management registers for the oversight and management of risk within the respective entities.

The key messages are:

1. Management of risk is the concern of everyone.
2. Management of risk is part of normal day to day business.
3. The process for managing risk is logical and systematic and should be implemented on a routine basis and integrated with service delivery.
4. All public sector entities must ensure that risk management:
   a) Is an integral and on-going part of its management process.
b) Is as simple and straightforward as possible.
c) That structures and responsibilities are clearly defined.
d) Employees and management partner in risk management processes with clear communication channels.
e) All incidents are immediately reported, categorised by their consequences and investigated to determine system failures, using an organisational learning approach.

5. In addition all public sector entities must:
   a) Continuously identify risks that may affect achievement of their objectives.
   b) Evaluate and analyse identified risks in the context of the entity risk criteria.
   c) Determine an appropriate method for treatment of identified risks.
   d) Provide for monitoring and reporting at various levels of management.

6. In addition to the guidelines public entities should comply with risk management guidelines issued by their respective industry regulators.

This policy guideline applies to all public sector entities and their employees, in both levels of government, in any setting where public sector supports and/or services are provided.

Each entity, in both levels of government should develop an implementation plan to comply with these guidelines, clearly providing timelines for the development of a risk management policy, risk management framework, and risk registers. In doing so, entities should clearly define respective risk management structures, repeat the process of risk assessment at least once a year, develop appropriate risk treatment plans for identified risks, and provide for monitoring and reporting at all levels of management and continuously improve its risk maturity.

The performance of the risk management systems will be measured by integration of risk management frameworks and processes within the entity governance, strategic and operation processes; identification and successful treatment of risks, mitigation and control of losses, reduction in costs of risks and achievement of objectives. These should be well documented.

All public entities should fully adopt these guidelines and report to PSASB and the National Treasury through the Internal Auditor General Department on adherence with these guidelines within one year of their gazettlement. Early adoption is recommended.

HON. (AMB) UKUR K. YATANI, EGH
CABINET SECRETARY/NATIONAL TREASURY AND PLANNING
Acknowledgement

Whilst there are already significant levels of disaster reduction, risk management and/or mitigation being practiced within public sector entities, efforts seemed to be fragmented within single public sector entity units.

Public entities tend also to become single-agency focused with annual work plans designed around the needs and priorities of these units. In many instances, these units try to address risk reduction for a range of risks simultaneously from within the limited resources of single units. In such cases, duplication of effort is common and there are usually a number of obvious programme gaps, which tend to impact upon the effectiveness and sustainability of outputs.

These guidelines move the risk management and oversight approach away from just being a response towards a more holistic management containment strategy that is linked intrinsically to development planning.

Although effective response and mitigation mechanisms are important, there needs to be a balance whereby risk is managed through a deliberate and planned sustainable mitigation effort. These guidelines embrace this concept, will be well placed to provide guidance to manage and oversight risk holistically, effectively, efficiently and economically.

The critical ingredients of these guidelines are that they have a holistic entity focus, they seek to involve all entity staff and contractors, and they are modelled on international standards to ensure that they meet accredited standards and recognised regionally and internationally.

These guidelines have been developed by the Public Sector Accounting Standards Board and the Internal Auditor-General Department to assist all public sector entities to develop their risk management policies, risk management framework and risk management registers, as stipulated in the Public Finance Management Regulations 2015.

I would like to appreciate the very resourceful feedback received through individual and corporate public comments from State Corporations, Regulators, County Governments, Professional Firms and professional associations including the Institute of Internal Auditors, Institute of Risk Management and Institute of Certified Public Accountants of Kenya.

I would also wish to acknowledge the significant contribution the Steering Committee jointly led by CPA Fredrick Riaga, The Chief Executive Officer of Public Sector Accounting Standards Board and Mr Alfayo Mogaka, the Internal Auditor-General of the National Treasury.

Specific recognition goes to the four-member taskforce, CPA George Mang’oka and CPA Rose Sambi of the PSASB, Mr Daniel Nyaga and Mr Willis Okwacho of the Internal Auditor Generals Department at the National Treasury for framing the draft guidelines.

The success of risk management and oversight in the public sector is dependent upon the guidelines being mainstreamed in both levels of government (National and County Governments levels) as a viable tool to coordinate the development of risk management tools in all the public sector entities.

JULIUS MUIA, PHD, CBS
PRINCIPAL SECRETARY/NATIONAL TREASURY
Abbreviations

CPA - Certified Public Accountant
COSO - Committee of the co-sponsoring organizations of the Treadway Commission
ERM - Enterprise Risk Management
IAGD - Internal Auditor General Department
IIA - The Institute of Internal Auditors
IRM - Institute of Risk Management
ISO - International Standards Organization
KPI - Key Performance Indicator
KRI - Key Risk Indicator
PFM - Public Financial Management
PMRA - Public Management Reform Agenda
PSASB - Public Sector Accounting Standards Board
RMC - Risk Management Committee
RMO - Risk Management Officer
# Table of Contents

About these guidelines ........................................................................................................... i  
Foreword .................................................................................................................................. ii  
Acknowledgement .................................................................................................................... iv  

**Chapter One: Preamble** ..................................................................................................... 8  
1.1  Understanding the Terms Risk and Risk Management .................................................. 8  
1.2  Rationale for Implementing Risk Management ............................................................ 8  
1.3  Benefits of Risk Management ...................................................................................... 9  
1.4  Legal Basis ................................................................................................................... 9  
1.5  Purpose of the Guidelines ........................................................................................... 10  
1.6  Scope of the Guidelines ............................................................................................... 10  
1.7  Challenges in Implementing Risk Management .......................................................... 10  
1.8  Where to Start ............................................................................................................... 11  
1.9  Effective Date and Review .......................................................................................... 11  
1.10 Structure of the Guidelines ........................................................................................ 11  

**Chapter Two: Risk Management Principles** ..................................................................... 12  

**Chapter Three: Framework** ............................................................................................... 14  
3.0  Introduction .................................................................................................................. 14  
3.1. Leadership and Commitment .................................................................................... 14  
3.2. Integration ................................................................................................................ 15  
3.3. Design ....................................................................................................................... 16  
3.3.1 Understanding the Entity and its Context ............................................................. 16  
3.3.2 Articulate the Risk Management Commitment ..................................................... 17  
3.3.3 Organisational Arrangements ................................................................................. 17  
3.4  Implementation ........................................................................................................... 26  
3.5  Evaluation ................................................................................................................... 26  
3.6  Improvement ............................................................................................................... 27  

**Chapter Four: Risk Management Process** ....................................................................... 28  
4.0  Introduction .................................................................................................................. 28  
4.1  Establishing the Scope, Context and Criteria ............................................................. 28  
4.2  Risk Assessment ......................................................................................................... 30  
4.3  Risk Treatment ........................................................................................................... 33  
4.4  Recording and Reporting ............................................................................................ 34
Chapter One: Preamble

1.1 Understanding the Terms Risk and Risk Management

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”. 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 can have either positive, negative effects or both, and create or result in opportunities and threats.

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. Uncertainty in making decision making in dealing with threats and opportunities has the potential to create, preserve, erode or realise value.

Failure by public sector entities to effectively manage risks negatively impacts the attainment of the entities strategic, operational, reporting and compliance objectives at different entity levels. This, places an extra duty of care on public sector governing bodies and managers to make choices that contain risks within acceptable limits.

Every entity manages risks whether informally or formally. 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”. COSO Enterprise Risk Management-Integrating with Strategy and Compliance, 2017, defines Enterprise Risk Management as “the culture, capabilities, and practices, integrated with strategy-setting and its performance that entities rely on to manage risk in creating, preserving, and realising value”. Risk management focuses on understanding the nature of risks and helps 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.

1.2 Rationale for Implementing Risk Management

Each public sector entity has a constitutional and legislative mandate to provide value to its stakeholders in form of services and goods. Entities set strategies that support their missions and visions and set objectives at different levels to achieve those strategies.

However, public sector entities face a myriad of challenges and poor reputation as a result of alleged corruption, inefficiencies, budget overruns, and pending bills among others that impede service delivery. Public entities operate in environments that are increasingly complex, volatile and ambiguous where factors such as technology, regulation and policy changes, demographics, restructuring, changing service requirements, inaccurate or incomplete data and information, natural calamities; create uncertainty. In addition, challenges such as inadequate capacity and limited resources, excessive bureaucracy, silo mentality, differing expectations from stakeholder groups and infrastructure constraints among others, have compounded management of these entities. Consequently, public entities face the possibility that potential events will occur that will affect their ability to achieve their service performance and business objectives.
1.3 Benefits of Risk Management

In a dynamic and complex public sector context, risk management plays a significant role in strengthening government capacity to recognize, understand, accommodate and capitalise on new challenges and opportunities, in analysing uncertainties within decision-making arrangements, in clarifying accountabilities and in demonstrating how the public interest is best served. Effective risk management systems improve government’s ability to deliver services to its citizens by focusing on performance, encouraging innovation and supporting the achievement of objectives therefore creating and protecting value through continuous review of its processes and systems and improvement. This promotes accountability in use of limited public resources. Benefits that accrue from effective risk management systems include:

(a.) Improved accountability and better governance;
(b.) Improved entity performance and resilience;
(c.) Improved the ability to identify, evaluate, and manage major threats;
(d.) Improved recognition and seize of opportunities;
(e.) Enabling risk-based decision making and strategy-setting;
(f.) Optimised resource allocation to match risk exposure;
(g.) Decreased potential for unacceptable or undesired behaviours such as fraud and other unethical practices;
(h.) Improved financial management;
(i.) Improved communication and consultation within the entity and parties sharing risks;
(j.) Foster risk-informed culture;
(k.) Improved compliance with laws and regulations; and
(l.) Creation and protection of stakeholders’ value and confidence in public entities among others.

1.4 Legal Basis

The Government has undertaken several reforms to promote performance and accountable governance in public sector. As part of the public financial management agenda, the government has over the years set out requirements for managing risk throughout the public sector.

The first Risk Management Guidelines for Government Departments and Agencies, were published by the Internal Auditor-General Department in 2011 following the release of Treasury Circular 3/2009 dated 23rd February, 2009 to introduce formal risk management in Government Departments and Offices and to promote good governance.

Subsequently, risk management was enacted into law through the Public Finance Management Act, 2012, sections 12(2)(i)), 50(1), 59(a)(iii), 62(3)(a), 63, 141, 73(3), and 155(3) and its attendant 2015 Regulations, which requires the Accounting Officer to ensure that entities develop risk management strategies, which include fraud prevention mechanism; and develop a system of risk management and internal control that builds robust business operations.
This was closely followed by Mwongozo Code of Governance for State Corporations, 2015 which in Chapter three requires Governing Bodies to ensure their entities have adequate systems and processes of accountability, risk management and control.

Implementing an effective entity risk management system will support the requirements of:

(i) Articles 10, 201 and 232 of the Constitution of Kenya, 2010 which require all entities and citizens to observe National Values and Principles of Governance, Principles of Public Finance and Values and Principles of Public Service respectively.

(ii) Sections 5 to 9 of the Public Service (Values and Principles) Act, 2015, require all public officers to observe the Public Service Values and Principles of Governance.

The Company Act 2015, Revised 2017, and International Financial Reporting Standards require directors to include a description of the key risks and uncertainties facing the company in the Annual Report and Notes to the Accounts.

Although risk management is enacted in law, implementation has not been systematic and structured across entities and while some entities have more mature risk management systems other entities having no formal processes in place.

### 1.5 Purpose of the Guidelines

The purpose of these guidelines is to provide a consistent approach for public sector entities to develop risk management frameworks and processes for efficient and effective management of risks throughout public sector. The guidelines have been developed to:

(i.) Provide practical guidance in designing a suitable risk management framework;

(ii.) Describe the principles of risk management;

(iii.) Give an overview of the requirements of implementing risk management;

(iv.) Describe accountabilities for risk management implementation and coordination;

(v.) Prescribe best practices in implementing risk management processes;

(vi.) Provides common language for discussing risk management;

(vii.) Provides a baseline for measuring risk management effectiveness; and

(viii.) Sensitise and train public officers on risk management.

### 1.6 Scope of the Guidelines

These guidelines apply to both National and County Governments and their entities including Ministries, Departments and Agencies, Independent Commissions and Offices, State Corporations, Judiciary, Parliament and all other offices in the public service.

Public entities should in addition to these guidelines comply with risk management guidelines issued by their industry regulators.

### 1.7 Challenges in Implementing Risk Management

To effectively implement risk management the entity’s Governing Body and management should overcome the following challenges which can impede successful implementation:
a) Lack of sustained commitment from the Governing Body and top management in implementing risk management.
b) Risk management not being aligned to strategic objectives;
c) Failure to embed risk management in governance and entity processes;
d) Risk management being treated as an extension of compliance or internal audit function resulting into lack of ownership by risk owners;
e) Lack of a clear roadmap and plan for risk management implementation and improvement.
f) Lack of integrated risk management framework resulting in silo approach to risk management;
g) Limitations in the quality and reliability of information used;
h) Past mistakes being overlooked and with no consideration to learn and improve controls;
i) Focus on compliance limiting innovation and change management;
j) Unsupportive risk behaviour and culture such as secrecy and fear of retribution;
k) Entities not keeping abreast with changing business and regulatory environment; and
l) Inadequate risk capacity including skills, experience and resources among others.

1.8 Where to Start

Public entities that do not have a formal risk management system should conduct a gap analysis to these guidelines to guide them in developing a risk management frameworks and an implementation plan before implementing risk management processes. An inventory of existing risk management practices, key strategies and related risk strategies should be conducted and priority areas identified. To sustain the risk management implementation, the support and commitment of the governing bodies and senior management should be sought and resources made available. A senior officer with knowledge and skills in risk management should be designated to coordinate the risk management initiative and a cross functional team put in place to drive the implementation.

Entities that have already implemented risk management should conduct a maturity gap analysis against these guidelines to identify any gaps and develop an improvement plan.

1.9 Effective Date and Review

These guidelines shall be effective on the date approved by the Cabinet Secretary. The guidelines take account of the latest international developments in risk management and shall be reviewed every three years or when circumstances dictate.

1.10 Structure of the Guidelines

Risk management is a system that comprises principles, framework and process. These are outlined in chapter two, three and four of these guidelines respectively. The system should be applied in an integrated manner throughout the entity.
Chapter Two: Risk Management Principles

2.0. Introduction

This Chapter summarizes eight risk management principles which characterise an effective and efficient risk management system. These principles are the foundation for risk management and should guide public entities in establishing and maintaining scalable and context specific risk management framework and processes that support organizational performance. Management should use judgement in applying these principles and ensure they are applied at all levels of the entity. Entities should periodically review and confirm whether the principles continue to be satisfied and develop an improvement plan to address any gaps noted. The eight principles of risk management drawn from ISO 31000: 2018, Risk Management Guidelines.

2.1. Integrated

Risk management should be an integral part of all entity activities including governance, planning and performance management processes at both the strategic and operational level. Risk management is not a standalone activity. The Governing Body provides strategic direction on risk management and delegates responsibility to management to ensure entity objectives are achieved. Risks management should be linked to and inform decision making at all levels of the entity. Risks should be considered in approving plans, budgets, investments, disposals, product or service design, organization structures, system development, contracting and appointments among others. Establishment of risk criteria and early warning systems ensure decisions are taken at the right level with explicit risk considerations.

2.2. Structured and comprehensive

A structured and comprehensive approach to risk management should be used throughout the entity to ensure consistent and comparable results. Each entity faces an array of interrelated and dynamic risks that represent both opportunities and threats. Risk management assimilates previously autonomous risk management roles within a common unifying structure using a clear and consistent approach that provides a portfolio and timely perspective to stakeholders on how the entity identifies, assesses, treats and monitors risks from internal and external environment to inform analysis, decision making, incident investigation and comparison of results to plans.

2.3. Customised

The risk management framework and processes should be customized and appropriate to the entity’s internal and external context related to its objectives. No two entities are structured the same way or have the same portfolio of risks. Risk management should be tailored to the entity’s external context including sector, locations, technologies, markets, regulatory requirements; and its internal context including culture, formal and informal structures, strategies, risk criteria, risk capacity, processes, stakeholder needs and relationships.

There is no one-size-fits-all in risk management. The Accounting Officer and Governing Body should develop customized risk management frameworks including risk management policy, roles, responsibilities, resources, processes and procedures, tools, facilities and
documentation based on the requirements set in these guidelines to meet the entity needs for effective risk management. Entities should use the guidelines to develop and implement risk management systems that are appropriate to their context.

2.4. **Inclusive**

The entity's internal and external stakeholders should be appropriately and timely involved in risk management activities to enable their knowledge, views and perceptions to be taken into account in identifying risks, determining the risk criteria and treatment design. This should result in improved awareness and informed risk management and reduces subjectivity and resistance. Entities should facilitate stakeholder participation through transparent disclosure of information, consultation, communication, feedback and reporting.

2.5. **Dynamic**

Risks can emerge, change or disappear as an entity’s external and internal context changes. The entity’s risk universe is constantly changing, its risk management system should be dynamic, iterative and responsive to change. Risk management processes should anticipate, detect, acknowledge and respond to changes and events in an appropriate and timely manner. The currency of information should be maintained through monitoring and review activities and the risk management framework evolved and improved to ensure it remains valid.

2.6. **Best available information**

Risk management should be based on the best available historical and current information, as well as future expectations. Information should be timely, clear and available to relevant stakeholders. This requires constant collecting, analysing, reviewing, updating and reporting of information on risks and risk management systems to facilitate continuous improvement. However, decision makers should take into account, any limitations of the data or assumptions used or the possibility of divergence among experts.

2.7. **Human and cultural factors**

The effect of human behavior and culture factors on all aspects of risk management should be considered as they have the potential to facilitate and hinder achievement of the entity’s objective. Zero risk is neither possible, nor desirable, and a tolerable level of risk that matches the risk criteria for the entity is needed. A supportive culture recognises uncertainty, supports considered risk-taking and embeds risk management into day-to-day activities is needed to support open sharing of risk information and discussions without fear of retribution and to provide learning opportunities. Risk seekers and risk takers should be challenged and commitment build to creating and protecting organizational value through risk management.

2.8. **Continuous improvement**

Entities should develop and implement strategies to improve their risk management maturity through review of their framework and application of results of monitoring, external reviews and learning. Monitoring activities such as assurance, routine data collection, incident investigation, root cause analysis and performance reviews should be put in place to identify areas of improvement and to develop an annual risk management improvement plan. This will help the entity not to repeat the same mistakes or fail to seize opportunities.
Chapter Three: Framework

3.0 Introduction

(1.) Each public sector entity should design a cost effective risk management frameworks that is appropriate to its context including the purpose and scope of risk management activities; the external, internal and risk management context; and the risk criteria/appetite and organization structure.

(2.) The Risk Management Framework provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the entity. The entity should set up the foundations including policy, objectives, mandate and commitment to manage risk. The entity should also put in place organizational arrangements including plans, relationships, accountabilities, resources, processes and activities for managing risks. The Risk Management Framework provides the architecture on which the risk management processes are embedded.

(3.) Figure 1 below illustrates how the components of the risk management framework should be developed, embedded into organizational plans and processes and continuously reviewed and improve to ensure it continues to be aligned to the entity’s mission, vision and strategies. These are further described below.

Figure 1: Framework (Source ISO 31000:2018, Risk Management Guidelines)

3.1. Leadership and Commitment

(1) The Governing Body should provide leadership and demonstrate commitment for managing risk by laying the foundations for risk management including:
(i.) Communicating the value of risk management to the entity and its stakeholders;
(ii.) Customizing and implementing all components of the framework;
(iii.) Approving the risk management policy, fraud prevention policy and implementation plan;
(iv.) Including in the risk management policy a risk philosophy statement that conveys to officials the tone for risk management in the entity and intention to embed risk management into decision making and performance management processes;
(v.) Determining the entity’s risk criteria and communicating the amount of risk an entity is willing to accept or retain in order to achieve its objectives;
(vi.) Ensuring there are clear accountabilities for managing risks and that officials are equipped with relevant skills and resources including people, skills, experience and competence; processes, methods and tools; information and knowledge management systems; and professional development for performing their roles efficiently and effectively;
(vii.) Ensuring there are clear procedures for bringing significant issues to its attention with agreed triggers for doing so;
(viii.) Assuring itself of the effectiveness of the entity’s risk management framework;
(ix.) Promoting systematic monitoring of risks; and
(x.) The Board should approve the acceptable level of risk for each risk category.

3.2 Integration

(1) The Accounting Officer is accountable for ensuring that risk management is integrated into all aspects of the entity and is not a standalone activity.

(2) Entities should promote risk–based thinking in processes and quality management systems.

(3) The risk management framework should form an integral part of the entity’s purpose, governance, leadership and commitment, strategy, objectives and operations and help the entity achieve desired levels of sustainable performance and long-term viability through:

(i.) Developing a positive risk management culture characterized by encouraged and acceptable behaviours, discussions, decisions and attitudes toward taking and managing risk;

(ii.) Setting appropriate accountability and oversight roles;

(iii.) Aligning risk management to the entity mission, objectives, strategy and culture;

(iv.) Conducting risk assessment before any major decision;

(v.) Embedding risk management responsibilities in performance management contracts; and
(vi.) Complying with various laws that prescribe specific treatment and reporting of risks within their ambit including prevention of fraud, disaster management, health and safety and others.

3.3. Design

(1.) Before designing the risk management framework each entity should understand the risk management context; the external and internal context; the risk criteria and organizational arrangements that influence the design and implementation of the risk management framework.

(2.) The entity should also:

(i.) Plan the scope of the risk management initiative and develop common language of risk;
(ii.) Establish the risk management strategy, framework and the roles and responsibilities;
(iii.) Assign authorities, responsibilities and accountabilities for risk management; and
(iv.) Put in place appropriate communication protocols to collect, collate, synthesize and share relevant information and feedback provided.

3.3.1 Understanding the Entity and its Context

(1) Define the risk management context
The purpose and scope of risk management activities should be defined. Risk management can be implemented at National, County, Ministry, entity, department, project, product or function level. This will align the risk management framework to the objectives and strategy of the entity and its internal and external context.

(2) Understand the external context
The entity’s external context may include: the social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors; key drivers; external stakeholders’ relationships; and contractual relationships and commitments.

(3) Understand the internal context
The entity’s internal context may include vision, mission and values; governance, organizational structure, roles and accountabilities; strategy, objectives and policies; the organization’s culture; standards, guidelines and models adopted by the entity; capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, intellectual property, processes, systems and technologies); data, information systems and information flows; relationships with internal stakeholders, taking into account their perceptions and values; and contractual relationships and commitments.
3.3.2 Articulate the Risk Management Commitment

(1) Risk management policy

The Accounting Officer should ensure a risk management policy is approved by the Governing Body approval. The risk management policy articulate the entity objectives and commitment for risk management and includes:

(i.) Risk Management Policy Statement
(ii.) Risk Management Policy objectives
(iii.) Purpose & Scope of Risk Management Policy
(iv.) Statement of the attitude of the entity to risk.
(v.) Description of the risk awareness culture or control environment.
(vi.) Level and nature of risk that is acceptable.
(vii.) Details of procedures for risk identification and ranking.
(viii.) List of documentation for analysing and reporting risk.
(ix.) Risk mitigation requirements and control mechanisms.
(x.) Allocation of risk management roles and responsibilities.
(xi.) Risk management training topics and priorities.
(xii.) Criteria for monitoring and benchmarking of risks.
(xiii.) Allocation of appropriate resources to risk management.
(xiv.) Reporting frequencies.
(xv.) Evidence of compliance with the Risk Management Policy
(xvi.) Risk Management Policy Review

An outline Risk Management Policy is attached as Appendix 1.

(2) Articulate the Risk Culture

(i.) The Governing Body and Accounting Officer to promote a risk culture that encourages staff to talk about risk and risk management. The encouraged and acceptable behaviors, discussions, decisions and attitudes toward taking and managing risk within an entity should be determined. This will influence whether employees and managers behavior along the cultural spectrum of risk averse, neutral or aggressive.

(ii.) To embed risk culture the entity should periodically conduct risk management training to different groups.

(iii.) The risk attitude, appetite and tolerance for risk may vary over time, across the entity as a whole and for individual process, program, department or activity and should be monitored through periodic culture reviews.

3.3.3 Organisational Arrangements

(1.) The Governing Organ and senior management should assign authorities, responsibilities and accountabilities for risk management.
(2.) Everyone in an entity has some responsibility for risk management. The “Three Lines Model” developed by the Global Institute of Internal Auditors provides a simple and effective way to help delegate and coordinate risk management roles and responsibilities and set role boundaries within the entity. These guidelines prescribe minimum roles and responsibilities and entities should seek further clarification and direction from the National Treasury on application of this model especially when their structures do not allow the delegation of roles as prescribed below.

Figure 2: Three Lines Model Framework (Source: The IIA)
3.3.3.1 GOVERNING BODY ROLES

(1) The Governing Bodies are not considered to be part of the three lines of defence but are primary stakeholders served by the three lines of defence. The Governing Bodies include the following categories:

(i.) In Ministries, the Cabinet Secretary who are responsible for ensuring departments implement Government policies and operate within their risk criteria.

(ii.) In Counties, the Counties Executive Committee Members under the policy direction of Governors, exercises executive authority and shall be responsible for risk management policy direction.

(iii.) In County Assemblies the County Assembly Service Board under the policy direction of the Speaker exercises executive authority and shall be responsible for risk management policy direction.

(iv.) In State Corporations, the Board of Directors have overall responsibility for risk management policy direction as provided in Mwongozo code of Governance Chapter three.

(v.) In Independent Offices and Commissions, the substantive holders of the Independent Offices and Commissioners (for independent commissions) have overall responsibility for risk management policy direction.

(2) The Governing Body is responsible for providing oversight over risk management and delegates to Audit Committee as stipulated in the Guidelines of Audit Committees for National and County Government and Mwongozo code of Governance and provide feedback. Specific responsibilities for the Governing Body are enumerated in paragraph 3.1 while those of the committees should be specified in committee charters and include:

(i.) reviewing the comprehensiveness and reliability of assurances on risk management;

(ii.) reviewing the entity risk profile quarterly and or annually;

(iii.) Reviewing and recommending disclosure of the top ten risks in the entity’s annual financial statements and the annual governance statement;

(iv.) Reviewing the strategic risk registers and making necessary recommendations to the Governing Body; and

(v.) Assisting the Governing Body in the identification of risks and determination of priorities for action.

(3) Some entities especially those in the Financial Sector may establish Board Risk Management Committee comprising of independent board members to provide oversight over risk management systems.
3.3.3.2 MANAGEMENT ROLES

Management’s responsibility to achieve entity objectives comprises both first and second line roles.

(1) Management. First Line Responsibilities

First line roles are most directly aligned with the delivery of products and/or services to clients of the entity, and include the roles of support functions. The responsibility of managing risk remains within the first line roles. These roles are played mainly by the Accounting Officer, Heads of Departments and Divisions and all entity staff.

(i) Accounting Officer

National and County Public Finance Management Regulations, 2015, Regulation 158 and 165 require all Accounting Officers to develop risk management strategies, which include fraud prevention mechanisms in their entities. To effectively discharge this responsibility in their entities Accounting Officer should set an appropriate tone from the top for risk management by:

(a.) Championing the effective management of risk;
(b.) Articulating risk criteria;
(c.) Assigning responsibilities for risk management and hold management accountable for integrating risk management into operations;
(d.) Evaluating alternative strategies and choosing strategies and set business objectives that consider the entity context and risk criteria;
(e.) Ensuring that the entity develops risk management strategies;
(f.) Maintaining oversight on key risks facing the entity;
(g.) Providing assurance to the Governing Body and other stakeholders that key risks are properly identified, assessed, and treated; and
(h.) Ensuring the risk coordinating function is supported in carrying out its role.

(ii) Risk Management Committee/ Public Finance Management Standing Committee

Management has delegated responsibility of managing risks to ensure the entity objectives are achieved. Public Finance Management Standing Committee which comprises members of senior management and reports to the Accounting Officer, is mandated under regulation 17, 18, 19 of the Public Finance Management Regulations, 2015, to identifying risks and implementation of appropriate measures to manage such risks or anticipated changes impacting on the entity.

In National Government Public Finance Management Standing Committee may double up as the Risk Management Committee made up of all the departmental heads and chaired by the Accounting Officer. The Committee is responsible for directing and
monitoring the implementation, practice and performance of risk management activities. Other responsibilities of the Committee include:

(a.) Reviewing the risk management policy, strategy and implementation plan;
(b.) Reviewing the entity’s risk criteria.
(c.) Ensuring the entity has appropriate risk identification and assessment methodologies, arrangements and tools;
(d.) Developing risk treatment plans to address the significant risks of the entity; and
(e.) Assessing implementation of the risk management policy and strategy and integration of risk management within the entity operations.
(f.) Review and approve quarterly risk reports from the risk management coordinating function.

The Public Finance Management Standing Committee reports to the Governing Body. The head of the risk management function is the Secretary of the Public Finance Management Standing Committee. The specific responsibilities of the Committee should be specific in a charter.

(iii) Heads of Departments and Divisions

Heads of Departments and Divisions have ownership, responsibility and accountability for assessing, controlling and mitigating risks together with maintaining effective internal controls. This level is closest to the activities of the entity and is also primarily responsible for the operation of business activities. As “risk owners” they play a more hands-on role in executing particular, day-to-day, risk and control procedures and are responsible for maintaining effective internal controls on a day-to-day basis.

The specific responsibilities for heads of departments and divisions in relationship to risk management include:

(a.) Identifying and managing risks as part of their everyday business, escalating them promptly as and when necessary;
(b.) Allocating and communicating responsibilities for managing risk;
(c.) Developing and recommending risk tolerance thresholds for processes;
(d.) Developing and maintaining risk registers and profile;
(e.) Embedding risk management practices within the business processes;
(f.) Monitoring risk management against risk criteria;
(g.) Promoting risk awareness within their operations;
(h.) Developing and implementing risk treatment plans;
(i.) Providing risk profile reports and coordinate information sharing; and
(j.) Holding officials responsible for their risk management responsibilities.

(iv) All entity staff
All entity staff have responsibility for risk management and should:

(a.) Diligently identify risks and report them to their supervisor, especially during periods of change to processes or operational practice; organization, entity policies, procedures and code of ethics.

(2). Management 2nd Line Roles

Second line roles provide assistance with managing risk. First and second line roles may be blended or separated.

(i) Risk Management Function

The risk management function coordinates risk management activities across the entity. Depending on the size of the entity, the risk management function may range from a single risk champion, a part time risk management officer (RMO) or a full scale risk management unit. The risk management function should be assigned to a senior member of staff with appropriate knowledge, experience, skills and professional qualifications in risk management.

The RMO should report administratively to the Accounting Officer and functionally to the Governing Body or Board Risk Committee or Audit and Risk Committee. The risk management officer should be independent from line management and the position should be able to provide ‘frank and fearless’ advice about risks and how they are managed.

The risk management function facilitates the entity’s management and oversees the risk management processes by:

(a.) Building the entity’s risk capability and defining the entity’s risk management practices and framework;
(b.) Developing and implementing the risk management plan;
(c.) Providing guidance and training on risk management processes;
(d.) Supporting management in identifying trends and emerging risks and assessment;
(e.) Assisting management in developing processes and risk treatment action plans;
(f.) Monitoring the adequacy and effectiveness of risk treatment plans, and accuracy and completeness of reporting;
(g.) Escalating identified or emerging risks exposures to the Accounting Officer and the Governance body;
(h.) Monitoring compliance with the risk management policy;
(i.) Collating risk reports and maintaining risk registers; and
(j.) Issue a report to the committee of the board that oversights risk on quarterly basis.

(ii) Compliance and Specialised functions
Some entities have compliance and specialised functions that support and monitor the first line roles. The functions vary by entity and industry and include legal, cyber security or environment. These functions should work in an integrated manner to support the first line roles and coordinate with the risk management function.

(iii) Risk Champions

The Accounting Officer should appoint risk champions to coordinate the departmental efforts and support the risk management function.

3.3.3.3 INTERNAL AUDIT

The role of internal audit in risk management must be guided by the International Standards for the Professional Practice of Internal Auditors issued by the Global Institute of Internal Auditors and adopted for use in the Public sector by the Public Sector Accounting standards Board through Gazette notice no. 5440 dated 8th August 2014. Internal audit roles are divided in three categories:

(1) 3rd Line Roles- Core internal audit roles in regard to risk management

(i.) Internal auditors primary responsibility is to provide independent and objective assurance on the effectiveness of the entity’s risk management arrangements including reviewing risk management processes, reviewing the management of key risks; evaluating the reporting of key risks and giving assurance that risks are correctly evaluated.

(ii.) Maintains primary accountability to the Governing Body and independence from the responsibilities of management. Internal audit should report any impairment to its independence to the Governing Body or Audit Committee.

(iii.) Internal audit should use the results of the entity risk assessment in preparing a risk based audit plan and may coordinate work with other assurance providers including business continuity management and compliance under a combined assurance framework.

(2) 2nd Line Roles Internal Audit can perform with safeguards

(i.) The Public Financial management regulations 2015 require the Internal Auditor-General and County Head of Internal Audit Services to promote risk management and provide the management with consulting services to improve the overall operations.

(ii.) Internal audit can provide risk management consulting roles such as facilitating identification and evaluation of risks, coaching management in responding to risks, coordinating risk management activities, consolidating reporting on risks, maintaining and developing risk management framework, championing establishment of risk management frameworks and developing risk management strategy for Governing Body approval. When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility
by actually managing risks. These are roles reserved for the Risk Management function.

(iii.) Internal audit should only be assigned the role of coordinating risk management where the entity’s risk management maturity is at the define level and the role transferred outside internal audit within an agreed transition period. The specific roles should be defined in the internal audit charter and approved by the audit committee.

(iv.) Under such arrangements the internal audit is not independent to provide assurance over risk management system at the entity and the entity should engage external parties to provide assurance over its risk management system.

(ii) 1st Line Roles Internal Audit should not undertake

(i.) Internal Auditors should refrain from assuming any management responsibility by actually managing risks and or being overall responsible for coordinating risk management activities.

(ii.) Internal auditors should not set the risk appetite, impose risk management processes, provide management assurance on risks; take decisions on risk treatment options, implement risk treatment on behalf of management or assume accountability for risk management.

3.3.3.4 EXTERNAL ASSURANCE PROVIDERS

These bodies sit outside the entity’s structure, and also have a role in the overall governance and control structure of the entity. External auditing and/or regulators can be considered as an additional line of defence, providing assurance to the entity’s shareholders, Governing Body and senior management.

(1.) Office of the Auditor General

The Public Audit is applicable to all Entities. Section 7 (1) (a) of the Public Audit Act, requires the Auditor General to give assurance on the effectiveness of internal controls, risk management and overall governance at national and county government. It is therefore an expected of all Entities to have in place a risk management system.

(2.) Other Inspection Bodies

These include Ethics and Anti-Corruption Commission, Public Procurement Regulatory Authority among others.

3.3.3.5 REGULATORY BODIES

(1.) Industry regulatory Bodies

Some sector regulators have established additional risk management regulations that entities operating in these sectors should comply with in addition to these guidelines. These include banking, insurance and pension sectors. Regulators have
powers to inspect entities to establish whether they have complied with set standards.

(2.) **National Government**

The Kenyan Constitution 2010, Public Finance Management Act, 2012, PFM National Government financial regulations mandates:

(i.) The National Government has responsibility for capacity building and technical assistance to the public sector.

(ii.) The National Treasury to:

(a.) monitor the financial aspects of risk management strategies and governance structures for the national government and County government entities;

(b.) design and prescribe an efficient financial management system for the national and county governments;

(c.) monitor and assess the implementation of the Public Finance Management Act and financial regulations;

(d.) Enforce the Public Finance Management Act and financial regulations.

The National Treasury will establish a risk management resource centre. To support public entities in implementing these guidelines and to monitor the maturity of their risk management frameworks and processes.

(3.) **County Governments**

According to the Public Finance Management Act, 2012 and the PFM National Government financial regulations, The County Treasury has powers to carry out its functions and responsibilities to publish and publicize the accounting and financial standards and any directives and guidelines prescribed by the Public Sector Accounting Standards Board.

### 3.3.4 Allocate resources

Top management and oversight bodies, where applicable, should ensure allocation of appropriate resources for risk management, which can include, but are not limited to:

(i.) People, skills, experience and competence;

(ii.) The organization’s processes, methods and tools to be used for managing risk;

(iii.) Documented processes and procedures;

(iv.) Information and knowledge management systems; and

(v.) Professional development and training needs.
3.3.5 Establish Communication and Consultation

(1) Communication protocols should be established to support the risk management framework.

(2) Relevant information should be collected, collated, synthesized and shared as appropriate and feedback provided.

3.4 Implementation

(1) Public entities should develop an appropriate risk management plan which specifies the approach, the management components and resources to be applied to the management of risk. Procedure, practices, assignment of responsibilities, sequence and timing of activities should be specified. The entity should:

(i.) Identify intended benefits of the risk management initiative and gain board support

(ii.) Plan the scope of the risk management initiative and develop common language of risk

(iii.) Establish the risk management strategy, framework and the roles and responsibilities

(iv.) Adopt suitable risk assessment tools and an agreed risk classification system

(v.) Establish risk benchmarks (risk criteria) and undertake risk assessments

(vi.) Determine risk criteria and evaluate the existing controls. Evaluate effectiveness of existing controls and introduce improvements

(vii.) Embed risk-awareness culture and align risk management with other activities in the organization

(viii.) Monitor and review risk performance indicators to measure risk management contribution

(ix.) Report risk performance in line with obligations and monitor improvement

(2) All stakeholders should be involved in the risk management implementation and appropriate capacity building measures should be put in place.

(3) A sample risk implementation plan is attached as Appendix 2.

3.5 Evaluation

(1) Management should periodically evaluate risk management framework performance against its purpose, implementation plans, indicators and expected behaviour to determine whether it remains suitable to support achieving the objectives of the entity.

(2) Each entity should assess the status of its risk management framework and process annually against a risk management maturity to identify, prioritize, implement and monitor improvement opportunities. The entity should also evaluate effectiveness of existing controls, embed risk-awareness culture and align risk management with other activities in the entity.
A sample risk management maturity model is attached as Appendix 3.

3.6 Improvement

(1) Each entity should maintain and improve the suitability, adequacy and effectiveness of its risk management framework and controls in responding to risks facing the entity.

(2) Management should continually monitor and adapt the risk management framework to changing external and internal changes and address any gaps noted. The entity should:

   (i.) Monitor and review risk performance indicators to measure risk management contribution

   (ii.) Report risk performance in line with obligations and monitor improvement

(3) Each entity should provide regular training on risk management to its staff to ensure adequate risk management competency is achieved and maintained.
Chapter Four: Risk Management Process

4.0 Introduction

(1) Public entities should develop and implement risk management policies, procedures and practices to carry out activities to communicate, consult, establish the context, and identify, analyse, evaluate, treat, monitor and review risk. Risk management process should be an integral part of management and decision making and integrated into the structure, operations and processes of the entity.

(2) The risk management process is a set of interactive steps that are undertaken in a coordinated manner, but not necessarily in a sequential manner as illustrated in figure 4 below. Communication and consulting, monitoring and review and recording and reporting activities and performed throughout the risk management process.

Figure 4: Risk Management Process (Source ISO 31000:2018, Risk Management Guidelines)

4.1 Establishing the Scope, Context and Criteria

(1) The management of risk should be undertaken with full consideration of the need to justify the resources used in carrying out risk management. The resources required, responsibilities and authorities, and the records to be kept should also be specified.
(2) An entity should establish the objectives, strategies, scope and parameters of its activities or those parts of the entity where the risk management process is being applied and have regard to any anticipated changes over time.

(3) The following steps should be carried out to establish the risk management context:

(i.) Identify entity objectives,
(ii.) Identify the stakeholders and their objectives.
(iii.) Define the external and internal parameters to be considered when managing risk.
(iv.) Define the risk criteria

4.1.1. Identifying Entity Objectives

(1) Risks are reviewed in the context of entity objectives. For public entities these are set by the relevant enabling legislation and periodic plans. These are explicit and implicit goals, values and imperatives and should be expressed clearly and unambiguously.

(2) The objectives should not be confused with the plans (strategic, project or operational) through which the entity pursues its purpose.

(3) Entities should assess the alignment between the entity strategic objectives with mission and vision and core values should be considered.

(4) Entities should assess the relevant objectives and decisions that have to be made, expected outcomes, time, location, risk assessment tools and techniques, resources required and relationships with other activities and processes.

4.1.2 Identify Stakeholders and their objectives

(1) To achieve an inclusive process, identify the areas that are, or might be, impacted and seek relevant stakeholders input including.

(i.) Internal stakeholders such as Heads of Departments, staff at all levels and relevant Governing Body.

(ii.) External stakeholders such as Legislators, regulators, community in which the entity operates, clients, vendors, funding bodies and media.

(2) Internal and external stakeholders should be identified through systematic brainstorming sessions that employs knowledge and experience of the public sector entity.

(3) The communication needs of each stakeholder should be identified and communication and consultation steps planned.

4.1.3 Defining the External and Internal parameters considered when managing risks

Entities should identify the external and internal environment factors that can affect the achievement of objectives in the area within which the risk management process will be undertaken.

4.1.4 Defining the Risk Criteria
(1) Entities should determine the amount and type of risks that they may or may not take relative to its objectives and develop a risk criteria approved by the Governing Body. Risk criteria can be developed through stating the entity’s approach to assess and eventually pursue, retain, take or turn away from risk.

(2) The risk criteria should be established at the beginning of the risk management process and used to evaluate the significance of different types of risks to support decision making processes.

(3) The risk criteria should be aligned with the entity’s risk management framework, risk capacity and attitude. The criteria should be customized to the specific purpose and scope of the activity being assessed.

(4) In determining the risk criteria, the entity should consider the applicable laws and regulations and government policies governing the entity and stakeholders views. The risk criteria should be drafted and approved by the Governing Board. The statement should clearly articulate the type and degree to which the Department is willing to accept risk. A sample risk appetite statement is attached as Appendix 4.

(5) Entities should also consider:
   (i.) the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible);
   (ii.) how consequences (both positive and negative) and likelihood will be defined and measured;
   (iii.) time-related factors;
   (iv.) consistency in the use of measurements;
   (v.) how the level of risk is to be determined; and
   (vi.) How combinations and sequences of multiple risks will be taken into account.

4.2 Risk Assessment

(1) Entities should undertake and document risk assessment at every level of the entity and for any proposed program, project or initiative at least once annually and when circumstances change as risks are dynamic.

(2) Risk assessment involves risk identification, risk analysis and risk evaluation steps described below.

4.2.1 Risk Identification

(1) Entities should find, recognize and describe risks that may impact the achievement of the entity objectives. Risk identification requires knowledge of the entity, sector in which it operates, the legal, social, economic, political, and climatic environment in which it does its business, its financial strengths and weaknesses, its vulnerability to unplanned losses, the processes, and the management systems and business mechanism by which it operates.
(2) Events and their causes and potential consequence, whether negative or positive should be considered for each strategy, activity or function, division, location, project, program or major decision within the risk assessment scope. Issues associated with not pursuing an opportunity; that is, the risk of doing nothing and missing an opportunity is also considered.

(3) Risks that have been identified by reviewing possible sources of risk information and by apply suitable risk identification tools and techniques including interviews, desk review, risk workshops and recorded in a risk register. A sample Risk Register Template is attached in Appendix 6A.

(4) Identified risks should be grouped into risk categories based on causal factors including internal sources such as human resources and external such as the social environment for better understanding the risks and mitigating measures. Sample Risk Categories are provided in Appendix 5.

(5) A risk universe listing all possible risks should be developed for risk analysis.

### 4.2.2 Risk Analysis

(1) Risk analysis should be conducted on identified risks to understand the nature of risk, its characteristics including, where appropriate, and the level of risk. This process is important to making decisions on whether to treat the risks and on the most appropriate risk treatment options. A sample Risk Analysis Documentation Template is attached in Appendix 6B.

(2) Each entity should adapt a qualitative, quantitative or quasi –quantitative risk matrix to assess level or the magnitude of risk to its objectives based on likelihood and consequences criteria. A matrix with combinations of likelihood and consequences can be adopted to rank risks low, medium or high depending on their severity as demonstrated in the appendices. A sample 5X5 Risk Matrix is attached as Appendix 7.

(3) Other risk criteria as velocity, the speed of onset of risk; volatility, the predictability of risks changing over time; and interdependence, the possibility of some events triggering other events leading to domino effect.

(4) 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.

(5) Risk analysis should be undertaken based on likelihood of events, complexity and connectivity; time related factors and volatility; effectiveness of existing controls; the consequences once it occurs; and the sensitivity and confidence levels.

(6) Risk analysis is a two-step process that involves:

   (i.) Inherent risk assessment to establish the level of exposure in the absence of deliberate management actions to influence the risk; and
(ii.) Residual risk assessment to determine the actual remaining level of risk after considering the effectiveness of risk treatment implemented to influence the risk.

(4.) A risk inventory consisting of risks requiring an evaluation of treatment options should be developed.

4.2.3 Risk Evaluation

(1.) Risk evaluation should be conducted to assist in making decisions on which risks need treatment and the priority for treatment implementation.

(2.) Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.

(3.) The results of the risk evaluation should be compared with the risk criteria / risk appetite to determine whether the risk and/or its magnitude is acceptable or tolerable or whether additional action is required. The risk criteria should include associated costs and benefits, legal requirements, socio-economic and environmental factors, concerns of stakeholders, etc.

(4.) Interdependencies between risks or possible combination of events should be identified and assessed.

(5.) The entity should use the results of the evaluation to decided either to do nothing further; consider risk treatment options, undertake further risk analysis to better understand the risk, maintain existing controls, or to reconsider objectives.

(6.) A decision should be made as to whether a risk is acceptable or unacceptable depending on the willingness to tolerate the risk; that is, the willingness to bear the risk after it is treated in order to achieve the desired objectives.

(7.) A risk may be regarded as acceptable or tolerable if the decision has been made not to treat it. A risk may be acceptable or tolerable if no treatment is available, treatment costs are prohibitive, the level of risk is low and does not warrant using resources to treat it; or the opportunities involved significantly outweigh the threats. Significant risks that are considered acceptable or tolerable should be monitored.

(8.) Risk owners should lead the evaluation process and involve all stakeholders who will be affected by the decision.

(9.) The risk action and escalation matrix provide a basis of grouping multiple risk levels into colour codes being catastrophic, major, moderate and minor categories. Each grouping is associated with a decision rule, such as treat the risk to bring it to an acceptable level, treat the risk only under certain circumstances or accept the risk. These groupings can also provide escalation points for risk management decisions, ensuring that risks are visible to, and managed at, the appropriate level. A sample risk action and escalation matrix is attached as Appendix 8.
4.3 Risk Treatment

(1.) The entity should select, design and implement the most appropriate risk treatment options that support achievement of intended outcomes and manage risks to an acceptable level.

(2.) The entity should develop a range of options for mitigating the risk, assessing those options, and then preparing and implementing action plans. The highest rated risks should be addressed as a matter of urgency.

(3.) The most appropriate risk treatment should be selected balancing the costs of implementing each activity against the benefits derived. In general, the cost of managing the risks needs to be commensurate with the benefits obtained. When making cost versus benefit judgments the wider context should also be taken into account.

(4.) Depending on the type and nature of the risk, the entity should choose one or several treatment options that modify the risk by:

(i.) Accepting (Tolerate/Retain): No action is taken to change the severity of the risk. This risk treatment option is appropriate when the risk to strategy and business objectives is already within the risk criteria. Risk that is outside the entity’s risk criteria and that management seeks to accept will generally require approval from the Governing Body.

(ii.) Avoiding (Terminate/Eliminate): Action is taken to remove the risk, which may mean ceasing a product line, declining to expand to a new geographical market, abandoning a project/programme, or selling a division. Choosing avoidance suggests that the entity was not able to identify a response that would reduce the risk to an acceptable level of severity.

(iii.) Exploiting (Pursue): Action is taken that accepts increased risk to achieve improved performance. This may involve adopting more aggressive growth strategies, expanding operations, or developing new products and services. When choosing to pursue risk, management should understand the nature and extent of any changes required to achieve desired performance while not exceeding the boundaries of acceptable tolerance.

(iv.) Mitigating (Reduce): Action is taken to reduce severity of the risk. This involves any of myriad everyday business decisions that reduces risk to an amount of severity aligned with the target residual risk profile and risk criteria.

(v.) Sharing (Transfer): Action is taken to reduce the severity of the risk by transferring or otherwise sharing a portion of the risk. Common techniques include outsourcing to specialist service provider, purchasing insurance products and engaging in hedging transactions. As with reduce risk treatment, sharing risks lower residual risk in alignment with risk criteria.

(5.) The risk treatment plans should identify those responsible for action, time frames for implementation, budget requirements or resource implications, performance
measures and review process where appropriate. Progress of treatments against critical implementation milestones should be monitored. A sample Risk Treatment Template is attached in Appendix 6C.

(6.) Contingency arrangements for high impact risks should be designed and tested to support continuity, incidence and crisis management and resilience.

4.4 Recording and Reporting

(1.) A risk register should be developed for each area assessed and the following information included in the risk register as a minimum.

(i.) The description of the risk.
(ii.) The causes and implications of the risk.
(iii.) The assigned risk owner.

(2.) In addition, the following information if known, should be included.

(i.) Details of the existing controls in place to manage the risk.
(ii.) The inherent risk rating determined from the assessment of the potential consequences and likelihood for the risk.
(iii.) Details of any proposed controls, including a due date for implementation.
(iv.) The residual risk rating after consideration of the controls in place.

(3.) The risk management process and its outcome should be well documented and reported to Governing Body and Accounting Officer at least once annually to assist them in assessing its effectiveness and making decision.

(4.) The Governing Body, Audit Committee should review the risk profile at least once annually. The Accounting Officer and Risk Management Committee should review the risk profile on a quarterly basis while extreme and high risks will be escalated immediately to the Governing Body for consideration and direction.

(5.) Entities should share risk information on shared risks with other entities involved in the management of the risk for planning and action while complying with confidentiality and privacy requirements.

(6.) Regulated entities should comply with the reporting requirements set out by the sector regulator.

(7.) Management, staff and stakeholders should immediately report emerging risks to the Risk Management Officer and supervisors immediately.

(8.) A sample Risk Reporting Guide is provided in Appendix 9.

4.5 Communication and Consultation

(1.) Each entity should 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 risk management process to inform decision making.

(2.) Relevant, accurate, complete and timely information about the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of risk should
be shared with stakeholders to promote their understanding of risks, the basis on which some decision are made and the reason why certain actions and accountabilities are required.

(3.) 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 decision while making appropriate measures to protect the confidentiality and integrity of information.

(4.) As part of a risk management process, all agencies should maintain communication among team members, analysts, stakeholders, partners, and customers to keep a project or decision moving through the risk management process.

(5.) Providers of outsourced services and partners in public private partnerships 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 supporting risk mitigation strategies.

(6.) Each entity should 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.

(7.) Entities should make appropriate disclosures on risk management and internal control to contribute to fair balanced and understandable annual reports.

4.6 Monitoring and Review

(1) Each entity should review its risks, its risk management framework and the application of its risk management practices on a regular basis, to identify change from the required or expected performance level, provide assurance and implement improvements arising out of such reviews.

(2) The entity’s monitoring and review processes should encompass all aspects of the risk management process for the purposes of:

(i.) The risk owners ensuring that controls are effective and efficient in both design and operation

(ii.) Obtaining further information to improve risk assessment

(iii.) Analysing and learning lessons from risk events, including near-misses, changes, trends, successes and failures. As a tool for risk management, incident management involves all risk incidents be recorded, analyzed and more important, actions taken and tracked for implementation.

(iv.) Detecting changes in the external and internal context, including changes to risk criteria and to the risks, which may require revision of risk treatments and priorities

(v.) Identifying emerging risks.

(3) Responsibilities for monitoring and review should be clearly defined and at a minimum:
(i.) Each Department develop a structured review process for all key risks within their area to be monitored in the risk treatment plans and report on progress.

(ii.) The Risk Management Officer and Risk Management Committee should confirm on a quarterly basis that key risks on the corporate risk register are managed and that the risk management framework, risk management process, risk or control remain appropriate and the register is updated.

(iii.) The Accounting Officer should continuously monitor key risk indicators (KRI) to determine if the risk is likely to materialize and ensure full compliance with the entity’s policies and procedures.

(iv.) The Internal Audit Unit should conduct a risk management audit of the risk management systems and advise management and Audit Committee on areas that need improvement.

(4) The performance of entity risk management systems will be measured by implementation and documentation of risk management, identification and successful treatment of risks, mitigation and control of losses, reduction in costs of risks and achievement of objectives among others.
**Glossary of Terms**

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

| Term                  | Definition                                                                                                                                 |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Assurance             | A general term for confidence that can be derived from objective information over the successful conduct of activities, the efficient and effective design and operation of internal control, compliance with internal and external requirements and the produce of credible information to support decision making. |
| Business Objectives   | Specific and measurable results entities want to achieve their strategy. They can be defined at different levels.                           |
| Cause                 | An element which alone or in combination has potential to give rise to a risk.                                                             |
| Communication and consultation | A continual and iterative processes that an entity conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk prior to making a decision. The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of the management of risk. |
| Consequence           | The outcome of an event affecting objectives should the risk occur. (A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives. Consequences can be expressed quantitatively or qualitatively. A consequence can escalate through cascading and cumulative effects.) |
| Control               | A measure that maintains and / modifies risk. Controls include, but are not limited to, any process, policy, device, practice, or other conditions and /or actions which maintain and /or modify risk. Controls may not always exert the intended or assumed modifying effects. |
| Core values           | The entity’s beliefs and ideals about what is good or bad, acceptable or unacceptable which influence the behaviour of the entity.          |
| Data                  | Raw facts that can be collected together to be analysed, used, or referenced.                                                            |
| Entity objectives     | The measurable steps that an entity takes to achieve its strategy.                                                                      |
| Establishing the context | Defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy |
| Event                 | An occurrence or change of a particular set of circumstances and can be something that is expected which does not happen, or something that is not expected which does happen. Events can have multiple causes and consequences and can affect |
| **Enterprise risk management** | multiple objectives. |
|-------------------------------|---------------------|
| **External context** | External environment in which the entity seeks to achieve its objectives. External context can include the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local and trends that having impact on the objectives of the entity. |
| **Exposure** | Extent to which an entity and/or stakeholder is subject to an event. |
| **Frequency** | The number of events or outcomes per defined unit of time. It can be applied to past events or to potential future events, where it can be used as a measure of likelihood/probability. |
| **Governing Body** | Refers to Board of Directors, Supervisory Board, Board of Governors or Trustees, Commissioners, or any other designated body of the entity who are accountable to stakeholders for the success of the entity and to whom the Accounting Officer functionally reports to. |
| **Governance** | The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the entity toward the achievement of its objectives. |
| **Information** | Processed, organized, and structured data concerning a particular fact or circumstances. |
| **Inherent risk** | The level of risk associated with the entity as a whole, or the individual system being examined before considering the effectiveness of controls. |
| **Internal context** | Internal environment in which the entity seeks to achieve its objectives. Internal context can include governance, organizational structure, roles and accountabilities; policies, objectives, and the strategies that are in place to achieve them. |
| **Internal control** | It is a process effected by an entity’s Governing Body, management and other personnel designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance. |
| **Level of risk** | The magnitude of a risk or combination of risks expressed in terms of the combination of consequences and their likelihood. |
| **Likelihood** | Chances of something happening. Likelihood can be defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically. |
| **Key risk** | A Key risk is a risk or combination of risks that can seriously affect the performance, future prospects or reputation of the entity. These should include those risks that would threaten its business model, future performance, solvency or liquidity. The term can be used interchangeably principal risk. |
| **Mission** | The entity’s core purpose, which establishes what it wants to accomplish and why it exists. |
| **Monitoring** | Continuous 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. |
| **Opportunity** | An action or potential action that creates or alters goals or approaches for creating, preserving, and realizing value. |
| **Probability** | The measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty. |
| **Resilience** | It is the adaptive capacity of an entity in a complex and changing environment. |
| **Residual risk** | The level of risk associated with the entity as a whole, or the individual system being examined after considering the effectiveness of controls. |
| **Risk** | The effect of uncertainty on objectives. An effect is a deviation from the expected. It can be positive, negative or both, and create or result in opportunities and threats. Objectives can have different aspects and categories, and can be applied at different levels. Risk is usually described in terms of risk sources, potential events, their consequences and their likelihood. |
| **Risk acceptance** | It is an informed decision to take a particular risk. Accepted risks are subject to monitoring and review. |
| **Risk aggregation** | The combination of a number of risks into one risk to develop a more complete understanding of the overall risk. |
| **Risk analysis** | The process to comprehend the nature of risk and to determine the level of risk based on the assessment of the likelihood of the risk occurring and the consequences should it occur. The velocity, proximity, and frequency of risk should also be considered if they are relevant to assessing the risk. |
| **Risk assessment** | The overall process of risk identification, risk analysis and risk evaluation. |
| **Risk appetite** | The amount of risk, on a broad level, an entity is willing to accept in pursuit of value. See risk criteria. |
| **Risk attitude** | An entity’s approach to assess and eventually pursue, retain, take or turn away from risk. This term can be used interchangeably with the term risk philosophy. |
| **Risk avoidance** | Informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk. |
| **Risk aversion** | It is the attitude to turn away from risk. |
| **Risk capacity** | The maximum amount of risk that an entity is able to absorb in the pursuit of strategy and business objectives. |
| **Risk criteria** | A set of terms of reference against which the significance of risk is evaluated. It can be derived from standards, laws, policies and other requirements. Risk appetite and risk tolerance are terms also used to describe risk criteria. |
| **Risk culture** | The attitudes, behaviours and understanding about risk, both positive and negative that influence the decisions of management and personnel and reflect the mission, vision and core values of the entity. |
| **Risk champion** | A person who by virtue of his/her expertise or authority champions a particular aspect of risk management process but is not the risk owner. |
| **Risk description** | A structured statement of risk usually containing four elements: sources, events, causes and consequences. |
| **Risk drivers** | A factor that has a major influence on risk. |
| **Risk evaluation** | Is the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. |
| **Risk governance** | Is the participation in the risk management process throughout the entire organization by personnel that are knowledgeable, skilled and competent in risk management. |
| **Risk identification** | Is the process of finding, recognizing and describing risks. It involves the identification of risk sources, events, their causes and their potential consequences. |
| **Risk inventory** | Stock-take on all the risks that can impact an entity. This term can be used interchangeably with risk universe. |
| **Risk management** | Coordinated activities to direct and control an entity with regard to risk. The term enterprise risk management can be used interchangeably. This term can be used interchangeably with enterprise risk management. |
| **Risk management** | It is the systematic, independent and documented process for obtaining evidence and evaluating it objectively in order to determine the extent to which the risk |
| Term                      | Definition                                                                                                                                 |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| audit                     | management framework, or any selected part of it, is adequate and effective.                                                             |
| Risk Management Committee | A committee appointed by the accounting officer to manage the entity support of risk management.                                         |
| Risk management framework | A set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the entity. Foundations include policy, objectives, mandate and commitment to manage risk. Organizational arrangements include plans, relationships, accountabilities, resources, processes and activities. The risk management framework is embedded within the entity’s overall strategic and operational policies and practices. |
| Risk Management Officer   | An officer or unit responsible for co-ordinating and supporting the overall risk management process but who does not assume the responsibilities of management for identifying, assessing and managing risk. |
| Risk management plan      | A scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk. Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities. The risk management plan can be applied to a particular product, service, process and project, and part or whole of the entity. |
| Risk management policy    | A statement of the overall intentions and direction of an entity related to risk management                                                    |
| Risk management process   | The systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating and reviewing risk. |
| Risk matrix               | The tool for ranking and displaying risks by defining ranges for consequence and likelihood.                                            |
| Risk owner                | The person accountable for managing a particular risk within an entity.                                                                      |
| Risk oversight            | The supervision of the risk management framework and process.                                                                                |
| Risk perception           | It reflects the stakeholder’s needs, issues, knowledge, belief and values.                                                                 |
| Risk portfolio            | Risk requiring an evaluation of risk treatment options.                                                                                     |
| Risk profile       | The description of any set of risk. It can relate to the whole entity or a part of an entity or as otherwise defined. |
|--------------------|-------------------------------------------------------------------------------------------------------------|
| Risk register      | A record of information about identified risks related to a specific entity activity.                             |
| Risk reporting     | The form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management. |
| Risk sharing       | It is a form of risk treatment involving the agreed distribution of risk with other parties. Risk sharing can be carried out through insurance or other forms of contract. |
| Risk source        | An element which alone or in combination has the potential to give rise to risk.                                |
| Risk strategy      | The specific management activities that are aimed at dealing with various risks associated with the business. It includes decision on risk tolerance levels and acceptance, avoidance or transfer of risks faced. |
| Risk tolerance     | Means the boundaries of acceptable variation in performance related to objectives.                               |
| Risk treatment     | The process to modify risk.                                                                                  |
| Risk universe      | All the possible risks that an entity is exposed to.                                                          |
| Severity           | Measurement consideration such as likelihood and impact of events or the time it takes to recover from events. |
| Shared risk        | A risk with no single owner, where more than one entity is exposed to or can significantly influence the risk. |
| Stakeholder        | A person or entity that can affect, be affected by, or perceive themselves to be affected by a decision or activity. |
| Strategy           | The entity plan to achieve its mission and vision and apply its core values.                                   |
| Threat             | Potential source of dangers, harm or undesirable outcome. A threat is a negative situation in which loss is likely to occur and over which one has relatively little control. A threat to one party may pose an opportunity to another. |
| Uncertainty        | It is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood. |
| Vulnerability      | The intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence. |
Appendices
Appendix 1: Sample Risk Management Policy Outline

The Policy outline developed by each public sector entity should incorporate:

**Purpose**-Outline the purpose of the risk management policy.

**Scope**-Specify who this policy applies to.

**Risk Governance**-Provide an overview of the risk governance structure of the organisation. Indicate who is involved in risk management and what their responsibilities are, from the Cabinet Secretary, to the Principal Secretary, the Board, Audit Committees, the Chief Executive Officer/Accounting Officer, line Managers, Risk Managers, Internal Audit, and the staff & contractors. Make reference to the risk management guidelines for practical guidance on the process.

**Risk Management Process**-Outline the steps involved in the risk management process. Make reference to the risk management guidelines for practical guidance on the process.

**Integration with other systems and processes**-Describe how risk management is integrated and embedded into organisational processes.

**Risk Categories**-Specify risk categories to be included in the risk register and in risk reporting.

**Risk registers**-Include details on the types of risks to be included on the risk register (e.g. operational or strategic), the criterion for adding and removing risks from the register, who will review the risk register and how often it will be reviewed.

**Risk Reporting**-Outline the risk reporting requirements. The purpose of risk reporting is to create awareness of key risks, improve accountability for the management of risk and the timely completion of risk treatment plans. Details as to who prepares reports, who reviews reports and how often reports are reviewed should be included.

**Risk Management Performance**-Outline how the performance of risk management will be measured. Measuring performance is a key monitoring activity to assess how effective risk management is at supporting corporate objectives.

**Risk Appetite**-Articulate the entities risk criteria - a statement that influences and guides decision making, clarifies strategic intent and ensures choices align with the capacities and capabilities of the entity.

**Interagency and State Significant Risks**-State the entities approach to identifying and managing interagency and state significant risks.

**Review and approval**-State how often and who will review the risk management policy. Review of the risk management policy should take into the account progress made against the risk management improvement plan, which is a blueprint for how the risk management policy is implemented across the organisation.
Appendix 2: Sample Risk Management Implementation Plan

The entity risk management implementation plan sets out all risk management activities planned for the XXX financial year to guide the implementation of the risk management policy and strategy.

| Planned Action | Detailed Actions | Outputs | Due date and responsible person | Progress to date |
|----------------|------------------|---------|---------------------------------|------------------|
| Develop a risk management policy | Risk Management Committee (RMC) to review the policy and recommend to the Accounting Officer / Authority for approval. | Approved risk management policy | Risk Officer dd/mm/yy | |
| **Risk orientation** | | | | |
| Develop/ review risk management strategy | Develop ERM Implementation Framework  Develop guidelines on roles and responsibilities for risk management  Review Fraud Prevention Plan  RMC to review the strategy and recommend to the Accounting Officer for approval | Approved risk management strategy | Risk Officer dd/mm/yy | |
| Structures and responsibilities | The RO to develop the risk management unit structure and present it to the RMC to review and recommend for approval by the Accounting Officer | Additional structure created and approved as required  Appointment into approved positions and structure  Formal delegation of responsibilities to existing personnel (via appointment letters and performance agreements) and structures (via charters) | Accounting Officer dd/mm/yy | |
| Publication of Risk Management Policy | Publicize the policy on the intranet | Communicated risk management policy to all officials in the entity | Risk Officer dd/mm/yy | |
| Raising awareness and risk management training | Develop and formalise detailed training programme/ plan for all officials and any cost | Completed orientation for all officials, RMC and Audit Committee members. | Risk Officer dd/mm/yy | |
| Planned Action | Detailed Actions | Outputs | Due date and responsible person | Progress to date |
|----------------|------------------|---------|---------------------------------|------------------|
|                | Implications.    | All new employees orientated on risk management. | Risk Officer | |
|                | Develop risk orientation programme for new employees. | Make presentations on risk management at management forums. | dd/mm/yy | |
| Terms of reference for the Risk Management Committee | Review existing RMC’s Terms of Reference and align to the RM strategy. | Approved Risk Management Committee charter | Risk Officer | |
|                | Approved risk assessment methodologies and processes | | dd/mm/yy | |

**Risk assessment**

| Planned Action | Detailed Actions | Outputs | Due date and responsible person | Progress to date |
|----------------|------------------|---------|---------------------------------|------------------|
|                | Development of a risk assessment protocol which includes risk quantification and risk ranking. Conduct research and benchmark with latest developments in RM (best practice). | Approved risk assessment methodologies and processes | Risk Officer | |
| Develop/ review risk management methodologies and processes | | | dd/mm/yy | |
| Facilitate enterprise-wide risk assessments. | Information gathering Facilitate risk identification and assessment sessions Analyse information and develop risk assessment reports. | Approved strategic risk register | Risk Officer | |
| | | | dd/mm/yy | |
| | | | dd/mm/yy | |
| | | | dd/mm/yy | |

**Risk response**

| Planned Action | Detailed Actions | Outputs | Due date and responsible person | Progress to date |
|----------------|------------------|---------|---------------------------------|------------------|
|                | Drafting action plans for all gaps identified in addressing the top risks. | Action plans implemented per agreed milestone | Risk Owner | |
| Development of risk response strategies | | | dd/mm/yy | |
| Drafting of individual key risk indicators for the top risks | Analysis report of key risk indicators per agreed frequency | | Risk Owner | |
| | | | dd/mm/yy | |
| Planned Action                                                                 | Detailed Actions                                                                 | Outputs                                                                 | Due date and responsible person | Progress to date |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------|----------------------------------|------------------|
| Risk monitoring                                                                |                                                                                  |                                                                        |                                  |                  |
| Assess risks controls effectiveness                                            | Assign assurance providers to assess the controls of medium and low risks identified (monitored risks). | Combined assurance plan Report on risks controls assessed              | Internal Audit                   |                  |
|                                                                                  |                                                                                  |                                                                        | dd/mm/yy                          |                  |
| Ensure risk management processes and methodologies are reviewed independently.   | Audit of risk management effectiveness                                            | Performance audit report Status reports on risk management implementation. | Internal / External Audits       |                  |
|                                                                                  |                                                                                  |                                                                        | dd/mm/yy                          |                  |
| Facilitate the execution of RM processes and infrastructure.                   | Implement appropriate risk reporting to the Accounting Officer, Governing Body, Audit Committee, RMC and Senior Management. | Approved progress reports: present progress reports to various stakeholders at various intervals. | Risk Officer                    |                  |
|                                                                                  |                                                                                  |                                                                        | dd/mm/yy                          |                  |
|                                                                                  |                                                                                  |                                                                        |                                  |                  |
## Appendix 3: Sample Risk Maturity Model

| Stage       | Culture                                      | Governance                                                                                     | Processes                                                                                                           | Risk Based Audit Approach                      |
|-------------|----------------------------------------------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| 5 – Risk    | Risk management is a value adding tool and   | The Governing Body undertakes its risk oversight role. Risk management is embedded at all       | Risk analytics are used to identify and monitor risk. Advanced risk management processes are in use.               | Audit risk management processes and uses      |
| Enabled     | is integrated into all decision-making.      | levels of the entity.                                                                         |                                                                                                                    | management’s assessment of risk.               |
| 4 – Risk    | Risk is integrated into strategic planning;   | Top management ensures risk management is structured and consistently implemented across the   | Risk management processes are monitored, gaps addressed and continually improved.                                 | Audit risk management processes and uses      |
| Managed     | risk criteria is stated and communicated.    | entity.                                                                                        |                                                                                                                    | management’s assessment of risk as            |
|             | The entity is proactive in risk management.  |                                                                                               |                                                                                                                    | appropriate.                                  |
| 3 – Risk    | Risk management framework is developed and   | Top management take lead in ensuring risk processes are developed and implemented in all key  | Formal risk processes are implemented and documented.                                                              | Liaise with risk management function and use |
| Defined     | implemented.                                 | areas.                                                                                         |                                                                                                                    | management’s assessment of risk where         |
|             |                                              |                                                                                               |                                                                                                                    | appropriate.                                  |
| 2 – Risk    | Unstructured risk management and limited     | Risk management initiatives are supported by top management on a need basis.                  | As needed risk and control self-assessment process are implemented. Scattered silos approach to risk management. | Promote entity wide approach to risk          |
| Aware       | standardization                              |                                                                                               |                                                                                                                    | management and rely on audit’s risk assessment.| |
| 1 – Risk    | The entity has minimal or no awareness of    | The Governing Body and Management is not committed in establishing risk management framework. | Processes are performed on an ad hoc basis by individuals.                                                          | Promote risk management and rely on audit’s   |
| Naive       | risk management                              |                                                                                               |                                                                                                                    | risk management.                              |
## Appendix 4: Risk Criteria Sample

| Category   | Item                                                                 | Green (Appetite)                                      | Amber (Tolerance)                                  | Red (Limit)                                   | Internal Monitoring & Reporting                                                                 | External Monitoring & Reporting                                                                 |
|------------|----------------------------------------------------------------------|------------------------------------------------------|---------------------------------------------------|-----------------------------------------------|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Financial  | Monetary value of financial impact of identified risks, after mitigation | 2.5% of budget or ≤Kshs----                         | Between 2.5 and 5% budget or between xxx and xxx Kshs | >5% of the budget or xxx Kshs                 | Relevant committee: > Kshs xxx or 4% of budget                                                   | if deemed appropriate by Governing Body                                                              |
|            |                                                                      |                                                      |                                                   |                                               | Governing Body: >Kshs or 10% of budget                                                       |                                                                                                   |
| Strategic  | Strategic impact on Department measured against set KPIs             | No appetite-KPI targets are met                      | Minor KPI target(s) are not met                   | we will not meet key strategic objective(s) as per legislation | Relevant committee: Minor KPI target not met.                                                   | if deemed appropriate by Governing Body                                                              |
|            |                                                                      |                                                      |                                                   |                                               | Governing Body: Will not meet a strategic objective                                          |                                                                                                   |
| Operational| Lack of quality in response to stakeholder requirement                | 0 complaints from individual stakeholders            | < 2 complaints from individual stakeholder        | > 2 complaints from individual stakeholder    | Relevant committee: if >2 working days or >2 complaints from individual stakeholder            | if deemed appropriate by Governing Body                                                              |
|            | Unavailability and/or system(s) failure                              | 1 working day                                        | < 2 working days                                  | >2 working days                               | Governing Body: if deemed appropriate by committee                                           |                                                                                                   |
|            | Unable to provide core services                                      | 1 working day                                        | < 2 working days                                  | >2 working days                               |                                                                                                 |                                                                                                   |
| Reputation | Adverse media coverage and/or public attitude                        | No media coverage                                    | critical articles in press and/or public criticism form regulatory body | Ministerial concern or comparable political repaccussions | Relevant committee: Critical article in press or criticism from regulatory body or <2 concurrent complaints from individual stakeholder | if deemed appropriate by Governing Body                                                              |
|            | Loss of stakeholder confidence                                       | 0 complaints from individual stakeholders            | < 2 complaints from individual stakeholder        | > 2 complaints from individual stakeholder    | Governing Body: Anything involving political repercussion or >2 concurrent complaints         |                                                                                                   |
| Compliance | Confirmed and qualified breaches of compliance and/or regulatory requirements | Compliance with all standards internal and external | Minor non-compliance with internal standards or protocols | Non-compliance with regulatory and/or other compliance requirements | Governing Body: if deemed material by committee                                                  | if deemed appropriate by Governing Body                                                              |
### Appendix 5: Sample Risk Categories

| Category       | Description                                                                                                                                 |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Strategy risks | Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment (e.g. political, economic, social, technological, environment and legislative change). |
| Governance risks | Risks arising from unclear plans, priorities, authorities and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance. |
| Operations risks | Risks arising from inadequate, poorly designed or ineffective/inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money. |
| Legal risks    | Risks arising from a defective transaction, a claim being made (including a defense to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets (for example, intellectual property). |
| Property risks | Risks arising from property deficiencies or poorly designed or ineffective/inefficient safety management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public. |
| Financial risks | Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting. |
| Commercial risks | Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and/or failure to meet business requirements/objectives. |
| People risks   | Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviour, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance. |
| Category               | Description                                                                                                                                                                                                 |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Technology risks       | Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.                                                                 |
| Information risks      | Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.                                                                 |
| Security risks         | Risks arising from a failure to prevent unauthorized and/or inappropriate access to the estate and information, including cyber security and non-compliance with General Data Protection Regulation requirements.              |
| Project/Programme risks| Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.                                                                       |
| Reputational risks     | Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations. |

Failure to manage risks in any of these categories may lead to financial, reputational, legal, regulatory, safety, security, environmental, employee, customer and operational consequences.
Appendix 6: Risk Assessment Templates

A: Sample Risk Register Template

| Area/Department: | Date of Risk Identification |
|------------------|-----------------------------|
|                  |                             |

| Risk reference | Objective | Risk Description | Risk Category | Consequence | Likelihood | Inherent risk rating | Current Controls | Effectiveness of existing controls | Suggestions on Additional Actions | Risk Owner |
|----------------|-----------|------------------|---------------|-------------|------------|---------------------|-----------------|-----------------------------------|----------------------------------|------------|
|                |           |                  |               |             |            |                     |                 |                                   |                                   |            |

B: Sample Risk Analysis Documentation

| Risk events | Possible Outcomes | Effect on objectives | Possible Causes | Possible Sources | Risk Interdependencies | Impact types and ranges | Likelihood |
|-------------|-------------------|----------------------|-----------------|-------------------|------------------------|------------------------|------------|
|             |                   |                      |                 |                   |                        |                        |            |


| Risk Register ID | Risk category | Risk Description | Control Effectiveness | Risk Treatment option | Cost benefit analysis | Is the treatment to be implemented or not | Monitor & Review | Implementation Status | Risk owner | Risk Treatment Owner |
|------------------|---------------|------------------|-----------------------|-----------------------|----------------------|----------------------------------------|-----------------|----------------------|-------------|---------------------|
|                  |               |                  |                       |                       |                      |                                        |                 |                      |             |                     |
|                  |               |                  |                       |                       |                      |                                        |                 |                      |             |                     |
|                  |               |                  |                       |                       |                      |                                        |                 |                      |             |                     |
|                  |               |                  |                       |                       |                      |                                        |                 |                      |             |                     |

C: Sample Risk Treatment Plan

Area/Department:

Date Treatment developed:
Appendix 7: Sample Risk Rating Matrix

Impact
The following is an example of a rating table that can be utilised to assess the potential impact of risks. Entities are encouraged to customise the rating table to their specific requirements.

| Rating | Description          | Impact on the achievement of Objectives                                                                 | Financial loss       | Public sector entity’s Reputation                      |
|--------|----------------------|---------------------------------------------------------------------------------------------------------|----------------------|-------------------------------------------------------|
| 1      | Insignificant        | Negative outcomes or missed opportunities that are likely to have a negligible impact on ability to meet objectives. | Minimum financial loss-less than Kshs 100,000 | Negligible impact                                    |
| 2      | Minor                | Negative outcomes or missed opportunities that are likely to have a relatively low impact on ability to meet objectives. | Between Kshs 100,000 and 1 million | Adverse local media only                             |
| 3      | Moderate             | Negative outcomes or missed opportunities that are likely to have a relatively moderate impact on ability to meet objectives. | Between Kshs 1 million and Kshs 50 million | Adverse print media coverage but not Headlines         |
| 4      | Major                | Negative outcomes or missed opportunities that are likely to have a relatively substantial impact on ability to meet objectives. | Between Kshs 50 million to Kshs 100 million | Adverse and extended national electronic and print media and social media |
| 5      | Catastrophic         | Negative outcomes or missed opportunities that are of critical importance to the achievement of objectives. | Over Kshs 100 million | Demand for Government inquiry                         |

Likelihood
The following is an example of a rating table that can be utilised to assess the likelihood of risks. Entities are encouraged to customise the rating table to their specific requirements.

| Rating | Description  | Frequency                                                                                                           | Probability of occurring in % |
|--------|--------------|---------------------------------------------------------------------------------------------------------------------|-------------------------------|
| 1      | Rare         | The risk is conceivable but is only likely to occur in extreme circumstances.                                        | 0-20                          |
| 2      | Unlikely     | The risk occurs infrequently and is unlikely to occur within the next 3 years.                                       | 20-40                         |
| 3      | Possible     | There is an above average chance that the risk will occur at least once in the next 3 years.                           | 40-60                         |
| 4      | Likely       | The risk could easily occur, and is likely to occur at least once within the next 12 months.                           | 60-80                         |
| 5      | Almost certain| The risk is already occurring, or is likely to occur more than once within the next 12 months.                       | 80-100                        |
**Inherent risk exposure (impact x likelihood)**

The following is an example of a rating table that can be utilised to categorise the various levels of inherent risk. Entities are encouraged to customise the rating table to their specific requirements.

| Inherent risk magnitude | Risk rating | Response                                                                 |
|-------------------------|-------------|--------------------------------------------------------------------------|
| High                    | 15 - 25     | Unacceptable level of risk – High level of control intervention required to achieve an acceptable level of residual risk |
| Medium                  | 8 – 14      | Unacceptable level of risk, except under unique circumstances or conditions – Moderate level of control intervention required to achieve an acceptable level of residual risk |
| Low                     | 1 - 7       | Mostly acceptable – Low level of control intervention required, if any    |

**Residual risk exposure (inherent risk x control effectiveness)**

The following is an example of a rating table that can be utilised to categorise the various levels of residual risk. Entities are encouraged to customise the rating table to their specific requirements.

| Residual risk magnitude | Risk rating | Response                                                                 |
|-------------------------|-------------|--------------------------------------------------------------------------|
| High                    | 15 - 25     | Unacceptable level of residual risk – Implies that the controls are either fundamentally inadequate (poor design) or ineffective (poor implementation). Controls require substantial redesign, or a greater emphasis on proper implementation. |
| Medium                  | 8 – 14      | Unacceptable level of residual risk – Implies that the controls are either inadequate (poor design) or ineffective (poor implementation). Controls require some redesign, or a more emphasis on proper implementation. |
| Low                     | 1 - 7       | Mostly acceptable level of residual risk – Requires minimal control improvements. |
## Appendix 8 : Risk Action and Escalation Matrix

| Risk Zone                  | Meaning                                                                 | Action Required for Risk                                                                 | Risk Escalation                                                                 |
|----------------------------|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Unacceptable/Catastrophic  | Risks that require urgent attention. Not permitted unless approved by the Governing Body | Urgent action required. Reduce the level of risk to major or below. Investigate and take steps to mitigate or avoid within a specified short term (1 month) period. | Escalated to the Cabinet Secretary and County Executive Committee Members/Governing Body |
| Significant/Major Risks    | that require prompt action. Only acceptable if it is not practicable or efficient to reduce the level of risk. | Reduce the level of risk to medium or below. **Prompt action** required, complete within three (3) months. | Accounting Officer                                                               |
| Tolerable/Moderate Risks   | Are acceptable to a limited period of time to allow treatment to be in keeping with the entity/project objectives. | Treat as soon as possible but within one year. **Weighted action** required - Risks will be treated as long as the costs do not outweigh the benefits. | Heads of Directorate/Departments/General manager                                  |
| Acceptable/Minor risks.    | Plan to treat in keeping with other priorities.                         | **Periodic monitoring.** Ongoing controls as part of general or routine management activates. | Heads of Sections/managers                                                        |
| Insignificant              | Risks to be monitored and managed with existing controls                | Can be dealt with internally                                                              | No escalation required                                                            |
## Appendix 9: Sample Risk Reporting Schedule

| Report Type                          | Users                                                                 | Frequency | Purpose & Content                                                                                                                                                                                                 |
|-------------------------------------|----------------------------------------------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| **Annual Report**                   | 1. External and Internal stakeholders  
2. Governing Body  
3. The Board risk management committee  
4. Risk Management committee  
5. Head Internal Audit Unit         | Annual    | Annual reports should document risk management activities of the entity and highlight key risks facing the entity and how these are being managed.                                                                 |
| **Risk Management Assurance Report**| 1. Governing Body  
2. Audit committee  
3. The Board risk management committee  
4. Risk Management committee  
5. Head Internal Audit Unit  
6. External Audit and Other External Review And Regulatory Bodies | Annual    | 1. Provide independent and objective assurance on the effectiveness of the entity's risk management arrangements including reviewing risk management processes, the management and reporting of key risks and giving assurance that risks are correctly evaluated.  
2. Provide assurance on the effectiveness of the system of internal control and risk assessment.  
3. Providing assurance to the Governing Body and other stakeholders that key risks are properly identified, assessed, and treated. |
| **Board Audit/Risk Management Committee report** | 1. The Board risk management committee  
2. Risk Management committee  
3. Head Internal Audit Unit          | Quarterly | The report can include:  
1. Risk register  
2. Significant risks: information provided on these risks include risk owner, risk treatment, additional treatments and timeframes and any other information  
3. Risk trends: trend analysis can only occur where there is frequent and regular assessment of risks. Trend reports can cover movements in risks, identifying those which are getting worse or better; show the effect of treatments on risk; identify risks that need further treatment.  
4. New or emerging risks: by conducting regular assessments, reports on new or emerging risks should be able to be compiled  
5. Risks with ineffective controls: the provision of this information will allow the Board and the Accounting Officer to identify potential points of business failure requiring urgent |
response or action
6. Risk categories: generic risk categories are strategic, operational, compliance and reporting (both financial and management) etc

| Operational Risk Report | 1. Risk Management committee | Quarterly | 1. The risk management process and its outcome.  
2. Assessing the effectiveness of the risk management system and developing an improvement plan.  
3. Top risks at functional level |
|-------------------------|-----------------------------|-----------|----------------------------------|
|                         | 2. Head of Risk Management Function |           |                                  |
|                         | 3. Head Internal Audit Unit   |           |                                  |

| Incident report         | 1. Head of Departments/Units. | Summary monthly reports | 1. Risks realized  
2. Failed controls  
3. Corrective actions taken and their status |
|-------------------------|-------------------------------|-------------------------|----------------------------------|
|                         | 2. Head of Internal audit.    |                         |                                  |
|                         | 3. Head of Risk Management Function. |                   |                                  |
References
1. A Risk Management Standard, 2002, Institute of Risk Management
2. International Standards for the Professional Practice of Internal Audit
3. ISO 31000:2018, Risk Management Guidelines
4. ISO 9001:2015, Risk –based thinking
5. ISO Guide 73, Risk Management – Vocabulary
6. COSO Enterprise Risk Management- Integrating with Strategy and Performance, 2017
7. Kenya Gazette Notice No.2690 of 15th April 2016 Audit Committee Guidelines for National Government and County Governments entities.
8. Mwongozo code of governance for state corporations, 2015
9. The Constitution of Kenya, 2010
10. The Public Finance Management Act, 2012
11. Risk Management- Risk Assessment Techniques, IEC/FDIS 31010
12. Public Finance Management Regulations, National Government, 2015
13. Public Finance Management Regulations, County Government, 2015