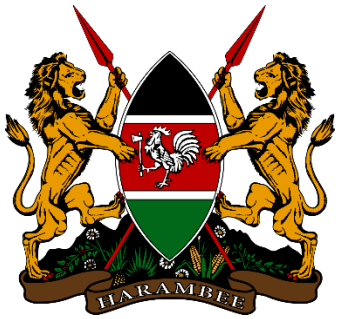
REPUBLIC OF KENYA



THE NATIONAL TREASURY & PLANNING

GAZETTE NOTICE NO XXXXX

PUBLIC SECTOR RISK MANAGEMENT GUIDELINES

November 2022

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 risk management implementation.

The guidelines have been benchmarked with Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management 2017 - Integrating with Strategy and Performance as well as ISO 31000:2018 Risk Management. Guidelines have been done with permission of Kenya Bureau of Standards, the Country's member body of the International Standards Organization.
Risk assessment tools and techniques are beyond the scope of these guidelines and 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 to understand the meaning attributed terms 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, and Code of Governance for State Corporations *(Mwongozo)* place a duty on Accounting Officers of all public sector entities, in both levels of government (national and county) to develop systems of risk and internal controls that build robust business operations.

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.

The effective management of risks assists public sector entities to:

(i.) Set and achieve strategic objectives;

(ii.) Proactively anticipate and manage risks;

(iii.) Comply with legal and policy obligations;

(iv.) Improve decision making; and

(v.) Allocate and utilise resources effectively.

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 strategic planning, decision making and performance management.
4. All public sector entities must ensure that risk management:

(i.) Is an integral and on-going part of its management process.

(ii.) Is as simple and straightforward as possible.

(iii.) That structures and responsibilities are clearly defined.

(iv.) Employees and management partner in risk management processes with clear communication channels.

(v.) 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:

(i.) Continuously identify risks that may affect achievement of their objectives.

(ii.) Evaluate and analyse identified risks in the context of the entity risk criteria.

(iii.) Determine an appropriate method for treatment of identified risks.

(iv.) 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 gazettement. Early adoption is recommended.

PROF. NJUGUNA NDUNG'U, CBS
CABINET SCRETARY/NATIONAL TREASURY AND PLANNING

Acknowledgement

Whilst there are already significant level of disaster reduction, risk management and/or mitigation being practiced within public sector entities, there are no risk management guidelines to guide systematic implementation of integrated risk management by public sector entities.

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 moves the risk management and oversight approach away from just being a reactive response towards a more proactive management approach that is linked intrinsically to performance management.

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 ISO 31000: Risk Management Guidelines and practices in leading countries including South Africa, Australia and the United Kingdom.

These guidelines have been developed by the Public Sector Accounting Standards Board in collaboration with 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. The guidelines were further subjected to stakeholder review in November 2022

I would like to appreciate the very resourceful feedback received through individual and corporate entities including 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 on the exposure draft.

I would also wish to acknowledge the significant contribution of the Steering Committee jointly led by FCPA Fredrick Riaga, the Chief Executive Officer of Public Sector Accounting Standards Board and CPA Ms. Jane Micheni, the Ag. Internal Auditor-General of the National Treasury. Specific recognition goes to the staff of PSASB and Internal Auditor General 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.

DR. CHRIS K. KIPTOO, 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
IRM	-	Integrated 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

Chapter One: Preamble

1.1 Understanding 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 decisions on how to deal 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. All entity's need to set strategy and periodically adjust it, always staying aware of both ever-changing opportunities for creating value and the challenges that will occur in pursuit of that value. To do that, public sector entity's need the best possible framework for optimizing strategy and performance. This places an extra duty of care on public sector governing bodies and senior management 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 Strategy with Performance, 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 helping management to evaluate and treat risks to within acceptable levels 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 because 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 and natural calamities among others create uncertainty.

Risk Management should be embedded into the activities of all public sector entities, including the mission, vision and core values. In developing strategy, business and performance objectives,

entities should consider the implications of the selected strategy; the risks to strategy and performance; and the possibility of the strategy not aligning with core values.

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:

(i.) Improved accountability and better governance;

(ii.) Improved entity performance, growth and resilience;

(iii.) Better management of complex, shared and national critical risks;

(iv.) Improved recognition and seize of opportunities;

(v.) Enabling risk-based decision making and strategy-setting;

(vi.) Optimised resource allocation to match risk exposure;

(vii.) Decreased potential for unacceptable or undesired behaviours such as fraud and other unethical practices;

(viii.) Improved financial management;

(ix.) Improved communication and consultation within the entity and parties sharing risks;

(x.) Fostering risk-informed culture;

(xi.) Improved compliance with laws and regulations; and

(xii.) 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 Ministries, 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 Ministries, Departments and Agencies 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 Code of Governance for State Corporations *(Mwongozo)*, 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.) Article 10 of the Constitution of Kenya (CoK), 2010 which require all entities and citizens to observe National Values and Principles of Governance including public participation; good governance; integrity; accountability; and sustainable development.

(ii.) Article 201 of CoK, 2010 which require all entities and citizens to observe Principles of Public Finance and Values including openness and accountability; prudent and responsible use of public money; and responsible financial management and clear fiscal reporting.

(iii.) Article 232 of CoK, 2010 which require all entities and citizens to observe Principles of Public Service respectively including efficient, effective and economic use of resources; involvement of people in the process of policy making; accountability for administrative acts; and transparency and provision to the public of timely, accurate information.

(iv.) 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.

(v.) Section 138 (4) of the Public Procurement and Asset Disposal Regulations 2020, requires a risk register to be maintained to monitor all identified contract risks.

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 the public sector. The guidelines have been developed to:

(i.) Provide practical guidance in designing a suitable entity specific 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 and application 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' responsibility of managing risks extend beyond the effective management of the entity's specific risks. Arrangements for addressing shared risks and national critical risks must be part of the entities risk management framework.

Public entities should in addition to these guidelines comply with risk management guidelines issued by their respective 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:

(i.) Lack of sustained commitment from the Governing Body and top management in implementing risk management;

(ii.) Risk management not being aligned to strategic objectives;

(iii.) Failure to embed risk management in governance and entity processes;

(iv.) Risk management being treated as an extension of compliance or internal audit function resulting into lack of ownership by risk owners;

(v.) Lack of a clear roadmap and plan for risk management implementation and improvement;

(vi.) Lack of integrated risk management framework resulting in silo approach to risk management;

(vii.) Limitations in the quality and reliability of information used;

(viii.) Past mistakes being overlooked and with no consideration to learn and improve controls;

(ix.) Focus on compliance limiting innovation and change management;

(x.) Unsupportive risk behaviour and culture such as secrecy and fear of retribution ;

(xi.) Entities not keeping abreast with changing business and regulatory environment ;

(xii.) Inadequate risk capacity including skills, experience and resources among others ;

(xiii.) Inadequate risk management governance structure;

(xiv.) Inadequate or lack of risk management infrastructure (tools, data support structures, unreliable data) ;

(xv.) Undefined risk appetite, tolerance levels and associated measurement methodologies or metrics to facilitate effective monitoring.

(xvi.) Complexity of the environment; and

(xvii.) Lack of an open risk culture and lack of risk awareness.

1.8 Where to Start

Public entities that do not have a formal risk management system shall conduct a gap analysis to these guidelines to guide them on areas to prioritise in developing a risk management framework and an implementation plan before implementing risk management processes. An inventory of existing risk management practices, key strategies and related risk strategies shall be conducted, and priority areas identified. To sustain the risk management implementation, the support and commitment of the governing bodies and senior management shall be sought, and resources made available. Head of risk management function shall have knowledge and skills in risk management. The head of the function shall 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 shall 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 the entity's 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 principles of risk management are drawn from ISO 31000: 2018, Risk Management Guidelines and benchmarked with COSO Principles.

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. Entities should leverage on technology to have an effective and robust risk management system.

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 considered 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 behaviour 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 organizational 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 framework 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, risk appetite and organization structure.

(2.) The Risk Management Framework should provide the architecture on which the risk management processes are embedded into the activities and functions of the entity.

(3.) This Framework should provide foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the entity

(4.) The foundations shall include policy, objectives, mandate and commitment to manage risks.

(5.) The organizational arrangements should include plans, relationships, accountabilities, resources, processes and activities for managing risks.

(6.) 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 improved to ensure it continues to be aligned to the entity's mission, vision and strategies.

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

3.1. Leadership and Commitment

(1) Risk management shall be an essential part of leadership and governance, and fundamental on how the entity is directed and controlled at all levels. Top management

is responsible for day-to-day management of risks and the governing body is accountable for overseeing risk management.

(2) The entity shall establish governance arrangements and culture. To support the appropriate risk culture the governing body and management shall ensure that the expected values and behaviours are communicated and embedded at all levels.

(3) The Governing body, shall ensure that risk management is integrated into all organizational activities and shall demonstrate leadership and commitment by:

i.) Ensure that risks are adequately considered when setting the entity's objectives;
ii.) Understand the risks facing the entity in pursuit of its objectives;
iii.) Ensure that systems to manage such risks are implemented and operating effectively;
iv.) Ensure that such risks are appropriate in the context of the entity's objectives;
v.) Ensure that information about such risks and their management is properly communicated.

(4) Management shall be accountable for managing risk and demonstrate leadership and commitment by:

i.) Customizing and implementing all components of the framework.
ii.) Developing a statement or policy that establishes a risk management approach, plan or course of action.
iii.) Ensuring that the necessary resources are allocated to managing risk.
iv.) Assigning authority, responsibility and accountability at appropriate levels within the entity.

3.2 Integration

(1) Integrating risk management into an entity is a dynamic and iterative process and shall be customized to the entity's needs and culture. Risk management shall be an integral part of all entity activities to support decision-making in achieving objectives.

(2) The Accounting Officer shall be responsible for ensuring that risk management is integrated into all aspects of the entity and is not a stand-alone activity.

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

(4) The risk management framework shall 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.

vii.) Embedding management of shared risks and national critical risks into the entity risk management framework and coordinating with the responsible coordinating bodies.

3.3. Design

(1.) Risk Management Framework shall be designed by thorough examination and understanding of its external, internal and risk management context such as contractual relationships, interdependencies, organisational structure and information flow among others.

3.3.1. Understanding the Entity's 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 functional 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

Governing body and senior management shall demonstrate their continual commitment to risk management through a policy, a statement or other forms that clearly convey an entity's objectives and commitment to risk management. An outline Risk Management Policy is attached as **Appendix 1**.

3.3.2.1. Risk Culture

The Governing body and management have a responsibility to set, communicate and enforce a risk culture that consistently influences, directs and aligns with the strategy and objectives of the entity and thereby supports the embedding of its risk management frameworks and processes. This starts with the risk behaviours, attitudes and culture of the governing body and management and reaches down through the whole entity. Senior management defines the characteristics needed to achieve the desired culture overtime, with the Governing bodies providing oversight and focus. An entity can then embrace a risk aware culture by:

(1.) **Maintaining strong leadership:** The Governing body and management places importance on creating the right risk awareness and tone throughout the entity. Culture and risk awareness cannot be charged from second-line team or department functions alone; the entity's leadership must be real driver of change.

(2.) **Employing a participative management style:** Senior management encourages staff to participate in decision making and to discuss risk to the strategy and entity objectives.

(3.) **Enforcing accountabilities for all actions:** Senior management documents policies of accountability and adheres to them, demonstrating to staff that lack of accountability is not tolerated and practicing accountability is appropriately.

(4.) **Aligning risk-aware behaviours and decision-making with performance:** Remuneration and incentive programs are aligned to the core values of the entity including expected behaviours, adherence to codes of conduct, and promoting accountability for risk aware decision -making and judgement.

(5.) **Embedding risk in decision-making:** Senior management addresses risk consistently when making key decisions, which includes discussing and reviewing risk scenarios that can help everyone understand the interrelationship and impacts of risks before finalizing decisions.

(6.) **Having open and honest discussions about risks facing the entity:** Senior management does not view risk as being negative and understands that managing risk is critical to achieving the strategy and entity objectives.

(7.) **Encouraging risk awareness across the entity:** Senior management continually sends messages to staff that managing risk is a part of their daily responsibilities, and that it is not only valued but also critical to the entity's success of survival.

In a risk-aware culture, staff know what the entity stands for and the boundaries within which they can operate. They can openly discuss and debate which risks should be taken to achieve the entity's strategy and objectives, with the result being employee and management behaviours that are more consistently aligned with the entity's risk appetite.

3.3.3. Communication and Consultation

Communication involves sharing information with targeted audiences while consultation involves participants providing feedback with the expectation that it will contribute to and shape decisions or other activities. The entity shall establish an approved approach to communication and consultation to support the framework and facilitate the effective application of risk management.

Senior management shall develop and adopt a Risk Communication and Consultation procedure and reports to ensure timely and relevant risk information collection, collating, synthesized, and shared as appropriate and that feedback is provided, and improvements made.

3.3.4. Allocation of Resources

Governing body and senior management shall ensure allocation of adequate and appropriate resources for risk management, which shall include, but are not limited to:

People, skills, experience and competence as well as professional development.

(1.) The entity's processes, methods and tools to be used for managing risk.

(2.) Documenting processes and procedures.

(3.) Information and Communication Technology tools for managing risk.

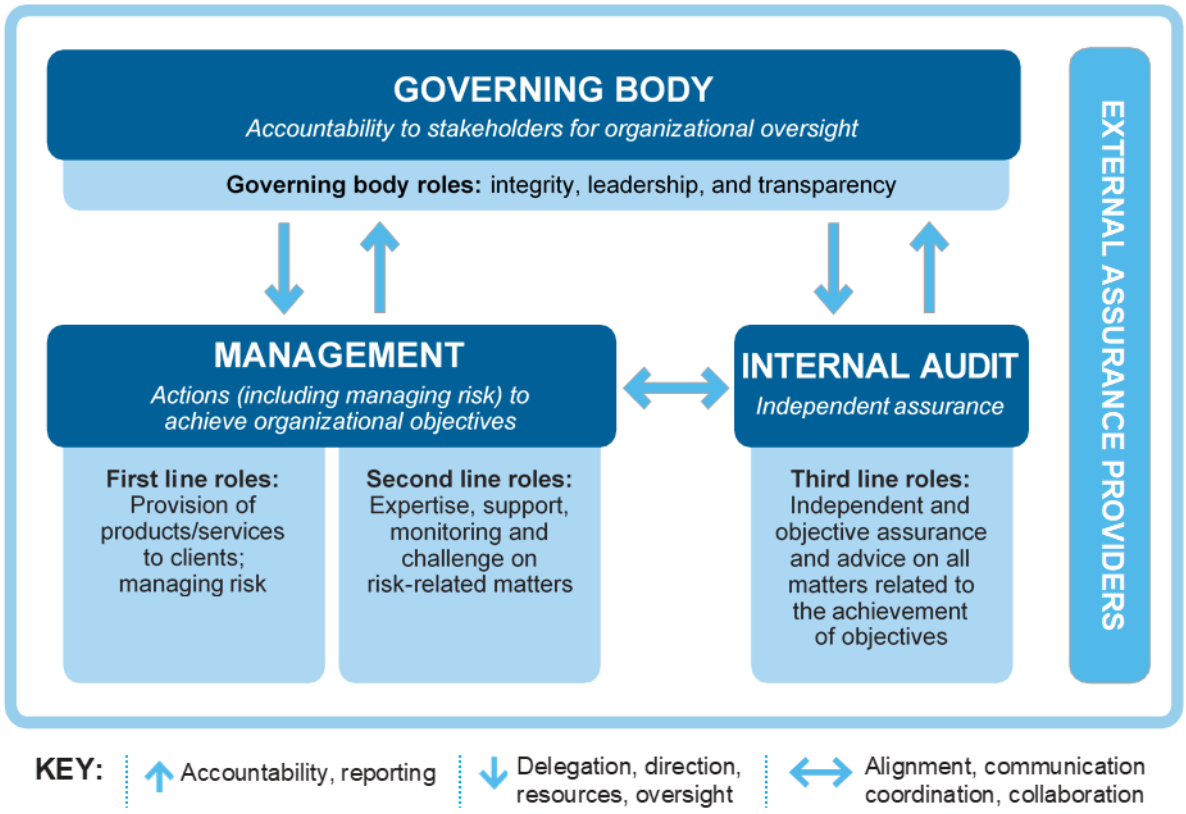
Management shall consider the capabilities of, and constraints on, existing resources.

3.3.5. Organisational Arrangements

(1.) The governing body 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 (Source: The IIA, 2020)



3.3.6. Roles and Responsibilities

The Governing body shall ensure the design of the risk management framework is documented in the risk management policy with clear assigned roles, authorities, responsibilities and accountabilities at all levels of the entity. Detailed roles and responsibilities are shown below;

3.3.6.1. Governing body

(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 appetite.

(ii.) In Counties, the Governor through the County Executive Committee Members exercise executive authority and shall be responsible for risk management policy direction.

(iii.) In National and County Assemblies the Speaker exercises executive authority and shall be responsible for risk management policy direction.

(iv.) In State Corporations and Semi-Autonomous Government Agencies, the Board of Directors have overall responsibility for risk management policy direction as provided in the Code of Governance for State Corporation (*Mwongozo)* Chapter three.

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

(vi.) In Universities, the Council shall have overall responsibilities for risk management policy direction. While the Board of Management have the overall responsibilities of risk management policy direction in Training and Vocational Trainings Institutions.

(2) The Governing Body is responsible for providing oversight over risk management. The Governing body shall:

(i.) Ensure the development of a policy on risk management, which shall take into account sustainability, ethics and compliance risks.

(ii.) Set out its responsibility for risk management in the Board charter.

(iii.) Approve the risk management policy and the risk management framework.

(iv.) Delegate to management the responsibility to implement the risk management plan.

(v.) Monitor that risks taken are within the set tolerance and appetite levels.

(vi.) Review the implementation of the risk management framework on a quarterly basis.

(vii.) Appoint a Committee responsible for risk management in the entity.

(viii.) Ensure that the Committee obtains relevant technical advice where necessary.

(ix.) Evaluate the performance of the Committee once a year.

(x.) Establish a risk management function within the entity.

(xi.) Ensure that risk assessment is carried out on a continuous basis.

(xii.) Receive from the Internal Audit function, a written assessment of the effectiveness of the system of internal controls and risk management.

(xiii.) Receive assurance from Management that the risk management framework is integrated in the daily activities of the entity.

(3) The responsibilities of the Governing Body as captured above shall be specified in the Board Committee Charter handling risk management. The responsibilities of the Board committee responsible for risk management may include, but is not limited to:

(i.) Reviewing, challenging, and concurring with management on:

(a.) Proposed strategy and risk appetite.

(b.) Alignment of strategy and entity objectives with the entity's stated mission, vision, and core values

(c.) Response to significant fluctuations in entity performance or the portfolio view of risk.

(d.) Responses to instances of deviation from core values.

3.3.6.2.Management

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

(1) Management 1st line roles

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

Regulation 158 and 165 of the National and County Public Finance Management 2015 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.) Establishing the necessary structures and reporting lines within the entity to support risk management;

(b.) Influencing entity "risk aware" culture;

(c.) Place the key risks at the forefront of the management agenda and devote personal attention to overseeing their effective management;

(d.) Providing assurance to the Governing Body and other stakeholders that key risks are properly identified, assessed, mitigated and monitored; and

(e.) Hold management accountable for designing, implementing, monitoring and integrating risk management principles into their day-to-day activities.

(ii) Risk Management Committee

The management has delegated responsibility of managing risks to ensure the entity objectives are achieved. Regulation 18 of both the National and County Government PFM, 2015 requires every national and county government entity to establish a Public Finance Management Standing Committee whose responsibility shall include identifying risks and implementation of appropriate measures to manage such risks or anticipated changes impacting on the entity.

The Risk Management Committee made up of all the departmental heads and chaired by the Accounting Officer is responsible for directing and monitoring the implementation, practice and performance of risk management activities. Other responsibilities of the Committee include:

(a.) Review and approve quarterly risk reports from the risk management coordinating function.

(b.) Monitor and review risk management practices, methodologies, tools, risk appetite and related disclosures

(c.) Preparing and recommending changes to the risk management strategy.

(d.) Identifying and assessing risks for all levels of the entity;

(e.) Recommending action to address risks;

(f.) Monitor and evaluate the extent and effectiveness of integration of risk management within the entity;

(g.) Monitor and evaluate the effectiveness of the mitigating strategies implemented to address the material risks of the entity;

(h.) Review the material findings and recommendations by assurance providers on the system of risk management and monitor the implementation of such recommendations;

(i.) Select cost-effective controls and seek input from operational staff on their appropriateness and assign managers to oversee implementation of the controls and to monitor the risks over time.

(j.) Initiate a risk management review when key indicators show entity stress or there have been significant changes/events within the entity.

(k.) Evaluate effectiveness of the entity Business Continuity Management System.

(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.) Implementing the risk management framework;

(b.) Own operational risks and controls in their respective departments/divisions thus ultimately accountable for the management of risk;

(c.) Ensure that all corrective actions against any areas of weakness are effectively and are expeditiously;

(d.) Ensure required risk information is reported and that it meets all established standards for timelines and integrity;

(e.) Ensuring that the risk management processes are followed on a continual and timely basis;

(f.) Ensuring that the entity complies with all external and internal rules, regulations, standards, policies and controls;

(g.) Fostering a risk management culture in their respective departments/divisions;

(h.) Taking appropriate measures to manage risks consistently and proactively;

(i.) Preparing reports on risk management activities in their respective departments and presents them to the Accounting Officer on a monthly basis with copies of the reports to the Head of risk function.

(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; re-organization, entity policies, procedures and code of ethics.

(b.) Contributing to and being responsible for risk management and internal control processes in their respective areas.

(c.) Supporting the development and updating of the documentation of risks,

(d.) Identifying and assessing risks in their areas, and contributing to risk mitigation.

(e.) Effective management of risk including the identification of potential risks.

(f.) Reporting risks and risk incidents from their respective areas and when they come across them in any other place within the entity.

(g.) Embrace and adopt a culture of risk management in execution of their duties.

(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. The function should be assigned to a senior member of staff with appropriate knowledge, experience, skills and professional qualifications in risk management.

The risk management function facilitates the entity's management and coordinates the risk management processes by:

(a.) Providing secretariate service to the Risk Management Committee

(b.) Building the entity's risk capability and defining the entity's risk management practices and framework;

(c.) Developing and implementing the risk management plan;

(d.) Providing guidance and training on risk management processes;

(e.) Supporting management in identifying trends and emerging risks and assessment;

(f.) Assisting management in developing processes and risk treatment action plans;

(g.) Monitoring the adequacy and effectiveness of risk treatment plans, and accuracy and completeness of reporting;

(h.) Escalating identified or emerging risks exposures to the Accounting Officer ;

(i.) Monitoring compliance with the risk management policy;

(j.) Collating risk reports and maintaining risk registers; and

(k.) preparing periodic reports to the Accounting Officer

(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 Management Champions

The Accounting Officer should appoint risk management champions to coordinate the departmental efforts and support the risk management function. Risk Management Champions shall be responsible for the following:

(a.) Managing the risk they have accountability for;
(b.) Reviewing the risk on a regular basis;
(c.) Identifying where current control deficiencies may exist;
(d.) Updating risk information pertaining to the risk;
(e.) Escalating the risk where the risk is increasing in likelihood or consequence;
(f.) Provide information about the risk when it is requested.
(g.) Identify and document emerging risks

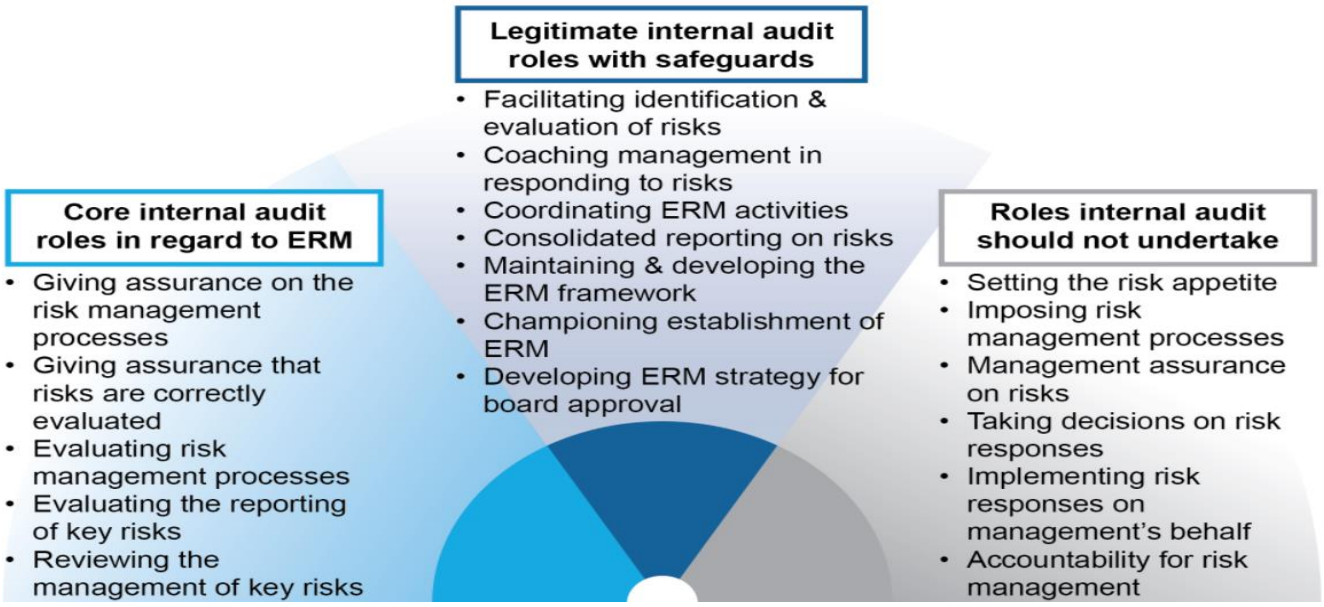
3.3.6.3.Internal audit

Regulations 160 and 153 of the PFM Act, 2015 requires internal auditors to give reasonable assurance through the audit committee on the state of risk management, control and governance within the organization.

The Public Sector Accounting Standards Board (PSASB) through Gazette notice no. 5440 dated 8th August 2014 prescribed the International Standards for the Professional Practice of Internal Auditors issued by the Global Institute of Internal Auditors for use in the public sector. The role of internal audit in risk management must be guided by the International Standards for the Professional Practice of Internal Auditors.

The figure below differentiates between roles the internal audit activity should and, equally important, should not undertake. The internal audit function shall undertake the core roles which entail assurance activities. The consulting and other non-assurance roles should be undertaken with safeguards. The Internal audit function shall not undertake managerial roles on risk management.

Figure 3: The Role of Internal Auditing in Enterprise-Wide Risk Management



(Source: IIA Position Paper: The Role of Internal Auditing in Enterprise-Wide Risk Management January 2009)

NB: The Internal Audit function should ensure entity's high risks are included in the annual risk based audit plan.

3.3.3.1 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 auditors 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**

Section 7 (1) (a) of the Public Audit Act, 2015 requires the Auditor General to give assurance on the effectiveness of internal controls, risk management and overall governance at national and county government.

(2.) **Other government entities and regulatory bodies**

Entities are required to comply with risk management requirements provided by the relevant other government entities and regulatory bodies.

3.3.4 Allocate resources

Governing body and senior management shall ensure allocation of adequate and appropriate resources for risk management, which shall include, but are not limited to:

(1.) People, skills, experience and competence as well as professional development.

(2.) The entity's processes, methods and tools to be used for managing risk.

(3.) Documenting processes and procedures.

(4.) Information and Communication Technology tools for managing risk.

Management shall consider the capabilities of, and constraints on, existing resources.

3.3.5 Establish Communication and Consultation

Communication involves sharing information with targeted audiences while consultation involves participants providing feedback with the expectation that it will contribute to and shape decisions or other activities.

(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

Public entities should implement the risk management framework by developing a risk management implementation plan. The plan should include:

(i.) Identifying intended benefits of the risk management initiative and gaining governing body support

(ii.) Planning the scope of the risk management initiative and developing common language of risk

(iii.) Adopting suitable risk assessment tools and an agreed risk classification system

(iv.) Establishing risk benchmarks (risk criteria) and undertaking risk assessments

(v.) Evaluating effectiveness of existing controls and introduce improvements

(vi.) Embedding risk-awareness culture and aligning risk management with other activities in the entity

(vii.) Monitoring and reviewing risk performance indicators to measure risk management contribution

(viii.) Reporting risk performance in line with obligations and monitor improvement

A sample risk implementation plan is attached as **Appendix 2.**

3.5 Evaluation

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

(2) Each entity should assess the status of its risk management framework and process as follows;

(i.) Self-evaluation annually against the implementation plan and when need arises
(ii.) self-evaluation against a suitable risk management maturity model at least once in three years
(iii.) entities are encouraged to undertake external assessment at least once in five years

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 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.

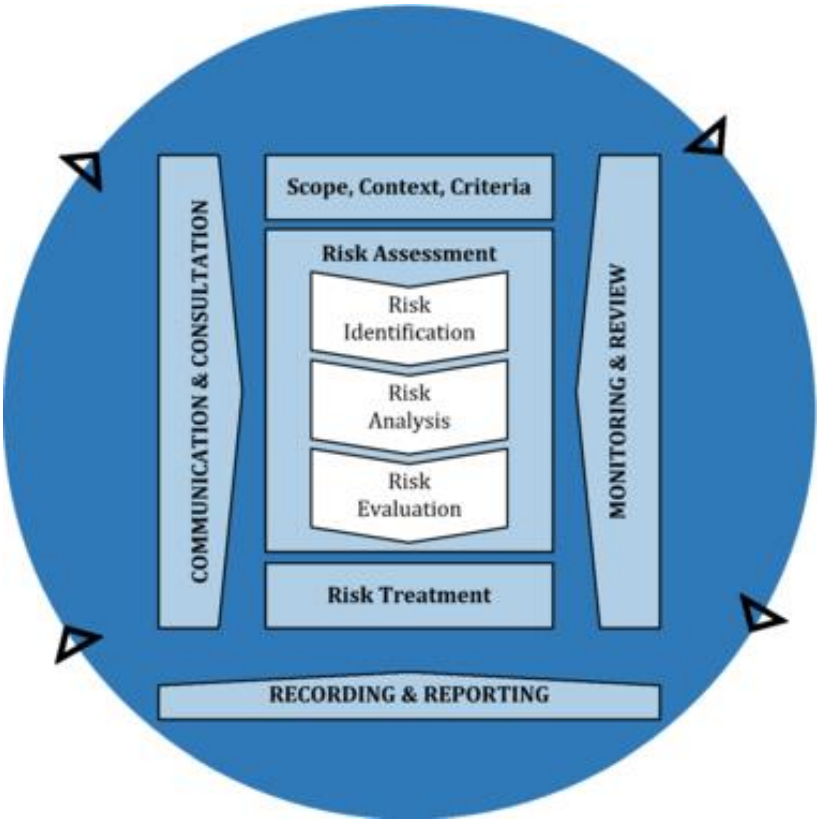
Chapter Four: Risk Management Process

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.) Defining the Scope,
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. Defining the Scope

(1) The entity should define the scope of its risk management activities taking into consideration 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

(2) 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

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

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

4.1.2 External and Internal Context

(1) The external and internal context is the environment in which the entity seeks to define and achieve its objectives.

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

(3) The external context should consider the political, economic, social and cultural, technological, ecological, competitive and legal environment as regards the entity.

(4) 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.

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

(6) 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.

4.1.3 Defining the Risk Criteria (Risk Appetite)

(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 by management and approved by the Governing Body. The statement should clearly articulate the type and degree to which the entity is willing to accept risk. The risk criteria/appetite should be reviewed periodically to align to the entity's operating environment. 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;
vi.) how combinations and sequences of multiple risks will be taken into account: and
vii.) the entity's risk capacity.

Figure 5: Risk profile showing Risk Appetite and Risk Capacity

Source: COSO, 2017

Figure 6: Diagram below explaining risk appetite, tolerance and risk capacity

Source: COSO, 2017

4.2 Risk Assessment

(1) Risk assessment should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiry as necessary.

(2) Risk owners shall have a key role in risk assessment process.

(3) 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.

(4) The entity should take into consideration both the upside (opportunities/events with favourable outcome) and downside risks (those with negative outcomes)

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

4.2.1 Risk Identification

(1) The purpose of risk identification is to find, recognize and describe risks that might help or prevent an entity from achieving its objectives.

(2) Entities should find, recognize and describe risks that may impact the achievement of the entity's objectives. Risk identification requires knowledge of the entity, sector in which it operates, the social political legal, economic, and climatic environment in which it does its business, its financial strengths and weaknesses, its vulnerability and capability to handle unplanned outcomes, significant changes in processes, and the management systems. The entity should consider both tangible and intangible sources of risk.

(3) Entities are encouraged to consider other factors such as the nature and value of assets and resources, consequences and their impact on objectives, limitations of knowledge and reliability of information, time-related factors, biases, assumptions and beliefs of those involved.

(4) 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. Risk identification should consider new and emerging risks relevant to the entity.

(5) The entity can use a range of techniques for identifying uncertainties that may affect one or more objectives. The entity is expected to utilize tools and techniques that are suited to its objectives and capabilities. Some of the techniques that could be used by the entity include interviews, questionnaires, controls self-assessments/process assessments, root cause analysis, desk review, risk workshops, SWOT analysis and recorded in a risk register. A sample **Risk Register Template** is attached in **Appendix 6**.

(6) Identified risks should be grouped into risk categories based on causal factors, both internal and external environment for better understanding the risks and mitigating measures. Sample **Risk Categories** are provided in **Appendix 5**.

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

(8) The entity should identify risks, whether or not their sources are under its control. Consideration should be given that there may be more than one type of outcome, which may result in a variety of tangible or intangible consequences.

(9) The entity should be consistent in risk sentence structure to reduce framing bias.

4.2.2 Risk Analysis

(1) The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect multiple objectives.

(2) Risk analysis should be conducted on identified risks to understand the nature of risk, its characteristics including, where appropriate, and the level of risk. A sample **Risk Register Template** is attached in **Appendix 6**.

(3) Each entity may adopt 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. Where multiple consequences are possible worst case scenario will be considered while determining the overall consequence. A sample **Risk Rating Matrix** is attached as **Appendix 7.**

(4) 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.

(5) 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 analysed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives.

(6) 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.

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

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

(8) Risk analysis provides an input to risk evaluation, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods.

4.2.3 Risk Evaluation

(1.) Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. The purpose of risk evaluation is to assist in making decisions on which risks need treatment and the priority for treatment implementation.

(2.) 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.

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

(4.) 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.

(5.) 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.

(6.) 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.

(7.) The risk action and escalation matrix provide a basis of grouping multiple risk levels into colour codes being high, medium and low 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.

(8.) The outcome of risk evaluation should be recorded, communicated and then validated at appropriate levels of the entity. It should be regularly reviewed and revised based on the dynamic nature and level of risk faced.

4.3 Risk Treatment/ Response

(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 and guided by the risk velocity.

(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.) Risk treatment will be measured in terms of efficiency and effectiveness. Efficiency will measure the cost of implementing risk management responses in terms of time, money and resources, whereas effectiveness will measure the relative degree to which the responses reduce the impact or likelihood of the risk occurring

(5.) Entities should taking into considerations the following factors while considering risk response action or when selecting and deploying Risk Responses

i.) **Business Context:** Risk responses are selected or tailored to the industry, geographical footprint, regulatory environment, operating structure, or other factors

ii.) **Costs and Benefits:** Anticipated costs and benefits are generally commensurate with the severity and prioritization of risks

iii.) **Obligations and Expectations:** Risk response address generally accepted industry standards, stakeholder expectations, and alignment with the mission and vision of the entity.

iv.) **Prioritization of Risk:** The priority assigned to the risk informs the allocation of resources. Risk responses that have large implementation costs (e.g system upgrades, increases in personnel) for lower-priority risks needed to be carefully considered and may not be appropriate given the assessed priority

v.) **Risk Appetite:** Risk response either brings risk within risk appetite of the entity or maintains its current status. Management identifies the response that brings residual risk within the appetite. This may be, for example, a combination of purchasing insurance and implementing internal responses to reduce the risks to a range of tolerance.

vi.) **Risk Severity:** Risk response should reflect the size, the scope, and the nature of the risk and its impact on the entity. For example, in a transaction of production of environment, where risks are driven by changes in volume, the proposed response is scaled to accommodate increased activity

(6.) Depending on the type and nature of the risk, the entity should choose one or several treatment options that modify the downside of risks 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.

Summary of Risk treatment options

Strategy	**Response**	**Additional action**
Target / Exploit/Pursue	Action is taken that accepts increased risk to achieve improved performance.	Convert Risk into Return
Take / Accept	Do nothing since the risk levels are deemed to be within accepted tolerance levels.	Monitor the risk for changes to status
Transfer /Share	Action is taken to reduce the severity of the risk by transferring or otherwise sharing a portion of the risk.	Insurance, work with 3rd parties e.g sub-contractors, etc
Reduce/Mitigate	Action is taken to reduce severity of the risk to tolerable levels	Prevent / detect/ direct
Terminate / Avoid/Eliminate	Discontinue/ disengage operations in cases where able to identify a response that would reduce the risk to an acceptable level of severity.	Divest, close operations, dispose section of the operations/equipment, etc.

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

i.) Exploit it – exploiting a positive risk means acting in ways that will help increase the chances of it occurring. If you're hoping for additional project funding, following up and pleading your case can help exploit the risk.

ii.) Share it– sharing a risk means working with others outside of your project who could also benefit from it to try to exploit it. If other project teams could benefit from new technology, you may work together to speed up the release date.

iii.) Enhance it - Enhancing a positive risk means attempting to increase the opportunity or positive outcome. If you're seeking grant money, you could apply for multiple different grants to increase the total amount you may potentially receive.

iv.) Accept it - Accepting it means you do nothing and wait to see if the event occurs naturally on its own

(8.) 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 Register Template** is attached in **Appendix 6**.

(9.) 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.) The risk management process and its outcomes should be documented in a risk register and reported through appropriate mechanisms as approved by the Governing body. Recording and reporting aims to:

i.) communicate risk management activities and outcomes across the entity;
ii.) provide information for decision-making;
iii.) improve risk management activities;
iv.) assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

(2.) The Governing body should specify the nature, source, format and frequency of the information that it requires. It should ensure that the assumptions and models underlying this information are clear so that they can be understood and, if necessary, challenged. Factors to consider for reporting include, but are not limited to:

i.) differing stakeholders and their specific information needs and requirements;
ii.) cost, frequency and timeliness of reporting;
iii.) method of reporting; and relevance of information to organizational objectives and decision-making.

(3.) A risk register should be developed for each area assessed and the following information included at minimum.

i.) The description of the risk.
ii.) The causes and consequences of the risk.
iii.) The assigned risk owner.
iv.) Details of the existing controls in place to manage the risk.
v.) The inherent risk rating determined from the assessment of the potential consequences and likelihood for the risk.
vi.) Risk tolerance/appetite
vii.) Details of any proposed additional controls, including a due date for implementation.
viii.) The residual risk rating after consideration of the controls in place.

(4.) The risk management process and its outcome should be well documented and reported to Governing Body and Accounting Officer periodically as per the entity's risk management policy to assist them in assessing its effectiveness and making decision.

(5.) 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.

(6.) 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.

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

(8.) Management, staff and stakeholders should immediately report emerging risks to the Risk Management Officer and supervisors and risk management champions in their departments/sections.

(9.) Entities may identify and progressively deploy relevant automated tools that can facilitate efficiency in recording, monitoring and reporting on its risk management activities. A sample **Risk Reporting Schedule** is provided in **Appendix 8**.

4.5 Communication and Consultation

(1.) Communication seeks to promote awareness and understanding of risk, whereas consultation involves obtaining feedback and information to support decision-making

(2.) 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.

(3.) 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.

(4.) 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.

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

(6.) 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.

(7.) 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.

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

4.6 Monitoring and Review

(1) The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes. Ongoing monitoring and periodic review of the risk management process and its outcomes should be a planned part of the risk management process, with responsibilities clearly defined.

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

(3) 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.

(4) Responsibilities for monitoring and review should be clearly defined and at a minimum:

i.) Each entity 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 while managing risks within the established risk appetite levels

iv.) The Internal Audit function should periodically conduct an audit of the risk management systems and advise management and the Governing body on areas that need improvement.

(5) 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.

(6) The results of monitoring and review should be incorporated throughout the entity's performance management, measurements, and reporting activities.

Glossary of Terms

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

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.
Entity specific risks	Risks that can be managed entirely within a single entity's operations and can generally be well understood and effectively managed through straight forward entity risk management processes.
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 multiple objectives.
Enterprise risk management	See risk management
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.
Integrated risk management	Is a set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks
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.
National Critical risks	Strategically significant risks due to their unforeseen pathways resulting in adverse impacts of national significance.
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 audit	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 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. Also referred to as inter-agency 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 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.

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

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	Resources
Scope, context, criteria					
Develop a risk management policy	Board Risk and Compliance Committee (BRC) to review the policy and recommend to the Governing body for approval.	Approved risk management policy	Head of Risk Management Function dd/mm/yy		
Develop/ review risk management strategy	Develop ERM Implementation Framework Develop guidelines on roles and responsibilities for risk management BRC to review the strategy and recommend to the Governing body for approval	Approved risk management strategy	Head of Risk Management Function dd/mm/yy		
Structures and responsibilities	develop/review the risk management unit structure and recommend for approval by the Governing body	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		
Terms of reference for the Risk Management Committees	Develop/Review Terms of Reference for: ▪ Board Risk and Compliance committee Management Committee and align to the RM strategy.	Approved Risk Management Committee charter	Accounting officer dd/mm/yy		

Planned Action	Detailed Actions	Outputs	Due date and responsible person	Progress to date	Resources
Publication of Risk Management Policy	Publicize and communicate the approved policy	Communicated risk management policy to all officials in the entity	Head of Risk Management Function dd/mm/yy		
Raising awareness and risk management training	Develop and formalise detailed training programme/ plan for all officials and any cost implications. Develop risk orientation programme for new employees.	Completed orientation for all officials, RMC and Audit Committee members. All new employees orientated on risk management. Make presentations on risk management at management forums.	Head of Risk Management Function dd/mm/yy		
Develop/ review risk management methodologies and tools s	Development of a risk assessment tool which includes risk quantification and risk ranking. Conduct research and benchmark with latest developments in RM (best practice).	Approved risk assessment methodologies and processes	Head of Risk Management Function dd/mm/yy		
Risk assessment					
Facilitate enterprise-wide risk assessments.	Risk identification Risk analysis Risk evaluation	Risk profile	Head of Risk Management Function dd/mm/yy		
Risk treatment					
Development of risk treatment strategies	Drafting action plans for risks considered unacceptable to the entity (key risks)	Approved risk register Approved risk treatment plan	Risk Owners dd/mm/yy		
Risk monitoring					
Develop key risk indicators	Drafting of individual key risk indicators for key risks	Identified key risk indicators	Risk Owner dd/mm/yy		

Planned Action	Detailed Actions	Outputs	Due date and responsible person	Progress to date	Resources
Incident recording and management	Define and implement an incident recording analysis mechanism	Incident report Incident register	Risk Owner dd/mm/yy		

Appendix 3: Sample Risk Maturity Model

A: IIA Risk Maturity Model

Stage	Culture	Governance	Processes	Risk Based Audit Approach
5 – Risk Enabled	Risk management is a value adding tool and is integrated into all decision-making.	The Governing Body undertakes its risk oversight role. Risk management is embedded at all levels of the entity.	Risk analytics are used to identify and monitor risk. Advanced risk management processes are in use.	Audit risk management processes and uses management's assessment of risk.
4 – Risk Managed	Risk is integrated into strategic planning; risk criteria is stated and communicated. The entity is proactive in risk management.	Top management ensures risk management is structured and consistently implemented across the entity.	Risk management processes are monitored, gaps addressed and continually improved.	Audit risk management processes and uses management's assessment of risk as appropriate.
3 – Risk Defined	Risk management framework is developed and implemented.	Top management take lead in ensuring risk processes are developed and implemented in all key areas.	Formal risk processes are implemented and documented.	Liaise with risk management function and use management's assessment of risk where appropriate.
2 – Risk Aware	Unstructured risk management and limited standardization	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 management and rely on audit's risk assessment.
1 – Risk Naive	The entity has minimal or no awareness of risk management	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 risk management.

B: OECD Risk Management Model

Maturity levels	Emerging	Progressing	Established	Leading	Aspirational
Descriptor	ERM is not well understood or practiced throughout the Entity, although pockets of knowledge and good practice may exist depending on the background and experience of individual staff. While there is acknowledgement that risk assessment and management is important for particular high- profile projects and that at the enterprise level it would bring value to the organization, it is often not delivered consistently or adequately in practice. More generally ERM is undertaken in a reactive and ad hoc manner,	Some ERM capabilities and practices are in place and there is a general understanding in most business areas of the role of risk assessment and risk management at a high level. There is some effort to systematically identify, analyze and treat major risks both at an enterprise level and within large projects, but the extent to which this information informs decision making and resource allocation	ERM capabilities and practices are generally well established in the culture and formal processes of theEntity. ERM and business unit risk management are standardized, coordinated and promoted consistently. Risk information is increasingly taken into account in decision making and resource allocation, particularly for higher risk areas, and reflected in	ERM capabilities and practices are well integratedinto strategic planning and performance management activities and risk appetites are clearly articulated. A strong culture of effective ERM exists across the Entity with a clear understanding of roles and responsibilities. Risk information and outcomes are continuously used to reinforce risk culture, to improve performance and inform decision-making.	ERM capabilities and practices are fully integratedwith strategy and performance management and reinforced through the organizational culture at all levels. Increasing use is made of advanced technology tools, including artificial intelligence, in the identification, monitoring and treatment of risk and risk management processes, including in a dynamic way.
Indicative					
Maturity levels	**Emerging**	**Progressing**	**Established**	**Leading**	**Aspirational**
attributes	Often after risks have materialized.	across the Entity ishighly variable.	performance management processes.		

Strategy	Entity strategy and objective setting usually involvesadjustments to the previous period's strategy/objectives in the light of experience and is generally backward looking as regards to risks (i.e. with a greater focus on previously realised risks rather than an analysis of how future risks might impact the delivery of the Entity's strategy). There is limited consideration ofthe internal and external environments and stakeholders.	Entity strategy andobjective setting involves some analysis of potential delivery risks although this may not be done in a joined-up and systematic process. Some aspects of the internal and external environment and stakeholders are considered.	When Entity strategy is being developed,consideration is given to thepotential effects of major changes in the internal and external environments (such as changes to government policy). Adjustments are made as appropriate in accordance with the Entity's general risk appetite. Thisprocess is supported by structured inputs from business units, risk management experts and governance committees.	Entity strategy is informed by comprehensivehorizon scanning and scenario planning involving a wide range of internal andexternal stakeholders. The detailed objectives for achieving the strategy are adjusted as appropriate in accordance with the Entity's different risk appetites and risk tolerances in specific areas.	The strategic planning process is supported by the use of advanced analytics (e.g. artificial intelligence) using a wide range of inputsto forecast different scenarios and their impacts on the achievement of the strategy. This is done on a continuous basis allowing real-time adjustments to strategy, objectives and/or performance measures, including as a result of changing risk appetites and risk tolerances of the Entity.
	There is a limited understandingof risk appetite by senior leadership	There is a basic understanding of risk appetite but is it not yet interconnected with strategy.	A risk appetite statement, that considers trade-offs, is in place and communicated appropriately.	Risk appetite statements are articulated for key areasof Entity risk. Risk appetite statements are reviewed periodically by the Entity's governance structure in the light of	Risk appetite statements are incorporated into all business objectives and monitored in real-time through advance analytic techniques with suggestions for changes put forward
Maturity levels	**Emerging**	**Progressing**	**Established**	**Leading**	**Aspirational**
				events and appropriate adjustments considered.	automatically for consideration.

Governance	The governance structure for ERM is somewhat unclear and generally uncoordinated between governance bodies.	The Entity governance structure considers ERM and existswith some exchange of information between governance bodies and periodic reporting to the Executive Management Team on major risks and risk management actions.	An Entity-wide governance structure is responsible for the periodicreview and monitoring of key elements of enterprise risk and performance as well as setting general risk appetite.	An Entity-wide governance structure regularly reviews enterpriserisk and performance Entity-wide and approves risk appetite and risk tolerance for major risks.	An Entity-wide governance body engages in proactive and, as necessary, real-time decision-making related to risk and performance to achieve the Entity's strategies and objectives (including supporting objectives of other government agencies).
	Levels of authority and roles and responsibilities are not well documented, understood or applied consistently across the Entity. There is consequently little review and monitoring of many risks and accountability for risk management is unclear.	Levels of authority and roles and responsibilities in some business areas are defined and documented with a focus on reviewing and monitoring major risks and performance indicators. Individual responsibilities as regards to other risks will often not be clear and risk appetite may vary widely across business units.	An operating structure is in place that sets out both levels of authority and individual roles and responsibilities that are consistently applied within most business units.	A comprehensive operating structure is in place to ensure full cooperation between governance bodies. Levels of authority and explicit roles within andacross business units are clearly mapped out in operating plans and individual objectives.	The Entity has well defined and well understooddelineated roles, responsibilities, delegations of authority, and governance structures. These are regularly evaluated by management,including through periodic independent reviews, to determine if they are applied correctly or if changes are needed in the light of changing circumstances.
Maturity levels	**Emerging**	**Progressing**	**Established**	**Leading**	**Aspirational**

Culture	There is a general appreciationat senior level of high-level business risks, but risk management is not promoted across the Entity as a proactive tool and often issues are only addressed after risks materialise.	The need for effective ERMis promoted at the senior management level although with a primary focus on major foreseen risks and high-profile projects with reputational impacts rather than a matter of general Entity culture.	The importance of effective and joined-up ERM across all aspects of the Entity is stressed by senior leadership and generally reflected in training material, performance management processes, including reporting and monitoring, and management objectives.	A strong ERM culture is visibly encouraged, supported through ongoingstructured professional training, and rewarded in performance managementprocesses. This is reinforced by consistent messaging and management behaviours.	ERM is fully integrated into core Entity professional values and is reflected in day-to-day behaviours and an organisational culture focused on innovation. It issupported through a multifaceted approach for continuous training and development.
	The application of ERM in general largely depends on the expertise and risk appetite of individual managers with high variability across the Entity. A number of basic training courses are available although not always ona regular basis and most training is done on the job.	In-house risk management expertise exists (which may be centralised or embeddedin high risk areas). Some core training can be provided on a reactive basisfor those directly accountable for identified high risk projects or issues. ERM in practice may be highly variable across the Entity and often undocumented.	Risk informed decision making by managers is encouraged and supported, including through the provision of general guidance and assistance on demand from risk professionals. Periodic reviews are done as to the ERM culture within the Entity.	There are well communicated expectationsas regards to the incorporation of ERM in decision making at all levelsas well as the involvement of risk management professionals. ERM culture is periodically measured against key performance indicators and qualitative assessments and benchmarked with other organisations.	There is real-time monitoring of behaviours and decisions to ensure alignment with core values and risk appetites, includingthrough the use of automated and embedded advanced technology tools and techniques. This also allows the Entity to make well informed dynamic changes in risk appetites and processes to respond to environmental changes.
Maturity levels	**Emerging**	**Progressing**	**Established**	**Leading**	**Aspirational**
	consistent picture of enterpriserisks.	identify and feedback some common themes and major interrelations between risks for business unit management consideration.	reflected in business unit plans and objectives.	cascaded across the Entity for inclusionin plans at all levels.	Entity wide objectives.

Risk Analysis and Evaluation	Risks are either not analysed formally or risk analysis is done in an inconsistent manner basedon the previous experience and management judgement and without any common format, resulting in an unreliable assessment of enterprise level risk.	Risk analysis is standardised but fairly basic in form, relyingon largely subjective and broad brush judgements which can vary considerably between business units and depend heavily on the engagement of management. There is some analysis for high-level risks that span business units on high-profile projects.	Standardised quantitative risk analysis techniques are increasingly used where appropriate to supplement qualitative analysis in a broadly consistent manner across the Entity. There is increasing use of scenario analysis and/or simulations in high risk areas to test and improve the qualityand reliability of risk analysis.	Quantitative approaches are increasingly used to gain actionable insights into risks. Scenario analysis and simulations are used on a consistent and regular basis. Triggers are identified and deployed to detect a need for risk reassessment and to mitigate for potential biases inassessments.	Risk analysis is carried out using an integrated risk assessment system based ona wide range of real-time qualitative and quantitative data, both internal and external, and using advanced technology tools (such as artificial intelligence) to map cause and effect relationships, including the impacts on interrelated risks.
	Risks are largely prioritised on the basis of high-profile/high budget projects which attract significant reputational risks. Most business areas assume abusiness as usual approach.	A broad measure of the magnitude of risks is derived by the governance structure from high level qualitative judgements of likelihood and impact and is used to assessand prioritise risks at the enterprise level.	The Entity has developed a prioritised portfolio of enterprise risks focused on business objectives and risks to, and opportunities for, those objectives both at the business unit level as well asat the enterprise level.	The Entity maintainsa prioritised portfolio of enterprise risks which are assessed in the context of theoverall organisation objectives. Risks at the program or process level allow decision making based on a thorough understanding of top-down and bottom-up risks and interrelated risks.	The Entitys prioritisedportfolio is updated in real- time and increasingly takes account of risks to other government agencies and government priorities as well as risks for particular taxpayersegments (for example through unforeseen administrative burdens).

	Emerging	Progressing	Established	Leading	Aspirational
	Risk treatment plans are not usually in place although high-level contingency plans may be drawn up for how the business unit or Entity might to react to a few plausible risks if and when they materialise.	Risk treatment plans are developed at the business unit level in a standardised format which requires an assessment of the costs and benefits and an explanation of treatment choices. This will often be done in a subjective manner and will depend heavily on the engagement of senior management. As a result there can be wide variations.	Risk treatments plans are developed in a standardised and data-informed manner at multiple levels of the organisation with some degree of coordination across business units. These treatment plans take account of the business context; cost and benefits; obligations and expectations; prioritisation of risks; risk appetite; risk severity and residual risk.	The full range of potential risk treatment options, including for interrelated risks, are considered and tested in a cross-Entity process. This includes the analysis and treatment of the risks resulting from a chosen risk treatment. Results are measured and triggers are identified and deployed to detect a need for adjustments to risk treatment approaches.	Risk treatment options are identified using an integrated risk assessment system using advanced technology tools (such as artificial intelligence) to calculate cost and benefits against a wide set of risk parameters and data. This system increasingly takes account of risks beyond the Entity, including to other government objectives and taxpayer segments.
	Monitoring is only performed through compliance and internal audit activities and most risk treatment information is only collected by individual areas of responsibility with only risk treatment on high profile areas or projects reported to the governance bodies.	Risk treatments are put in place by each business unit and reported to the appropriate governance committees with periodic updating of the committees. There is limited validation outside of major projects or high-profile risks.	There is regular centralised consideration and challenge of risk treatment proposals by the governance bodies with a focus on the enterprise level and higher risk projects. Risk treatment plans for enterprise risks are collected but may not be routinely shared across the Entity.	The validation of risk treatment plans from across the units, including how they interrelate, is done in a joined-up process by the governance bodies and business units. The effectiveness of risk treatments is periodically tested. Consideration is given to when treatment may require the revision of a strategy or business objective.	Risk treatment options are continuously monitored in the light of new information, including as to their effectiveness, and recommendations for adjustments can be made in real time, including for suggested changes in objectives and strategy and behaviours.

Appendix 4: Risk Criteria/Appetite Sample

Category	Risk Criteria/ appetite Examples
Financial	• Budgetary variations should not exceed XX% of the total expenditure • Zero tolerance to loss of entity's funds as a result of fraud
Strategic	• We will not tolerate performance below …% of the planned strategic initiatives per annum
Health and Safety	• Zero fatalities in our premises • We will not built keep plants/offices/install equipment in flood or earthquake prone areas
Operational	• System failure of not more than xx days/hours in a month/day
Reputational	• Zero tolerance to adverse media coverage
Compliance	• Zero tolerance to noncompliance to the relevant regulatory requirements

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.
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.

Sustainability	Risks arising from uncertain social and environmental event or condition that if it occurs, can impact significantly on the entity
ESG Risks	ESG risks include those related to climate change impacts mitigation and adaptation, environmental, Governance, legal and sustainability.
Business Continuity	Risks impacting unavailability of services and products due to various disruptions

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: Sample Risk Register Template

Combined Risk Register Template **Area/Department:**																
Risk reference	Objective	Risk Description	Date Reported	Risk Category	Possible Causes	Possible Consequences	Inherent Consequence Rating	Inherent Likelihood Rating	Inherent risk rating	Residual Consequence Rating	Residual Likelihood Rating	Residual risk rating	Risk Treatment option	Additional Controls/Actions	Due Date/Timeline	Last Update Date	Risk owner

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

Risk rating (impact x likelihood)

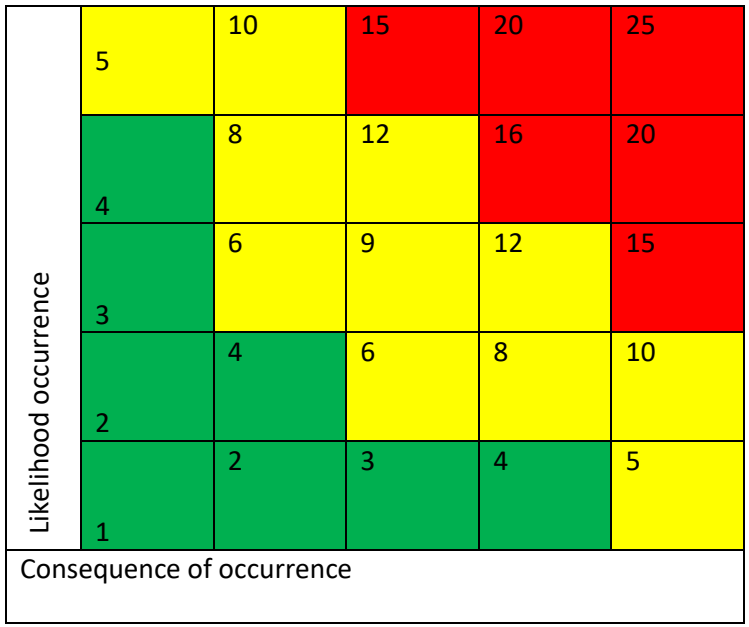
The following is an example of a rating table that can be utilised to categorise the various levels of risk. **Entities are encouraged to customise the rating table to their specific requirements.**

Level of risk	Risk score	Response
High	15 - 25	Unacceptable level of risk – High level of treatment intervention required to achieve an acceptable level of residual risk.
Medium	5 – 12	Unacceptable level of risk, except under unique circumstances or conditions – Moderate level of treatment intervention required to achieve an acceptable level of residual risk
Low	1 - 4	Mostly acceptable – Low level of control intervention required, if any

Note: Entities are encouraged to document risk action and escalation matrix in their respective risk management policy

Note: Entities are encouraged to refer to section 4.3 of the guideline for further information of treatment actions

Appendix 8: Sample Risk Heat Map



Appendix 8: Sample Risk Reporting Schedule

Report Type	Users	Frequency	Purpose & Content
Risk Management Report	1. External and Internal stakeholders 2. Governing Body 3. Board risk assurance committee 4. Risk Management committee 5. Head Internal Audit Unit	Annual /as per the entity risk policy	Annual reports should document risk management activities of the entity and highlight key risks facing the entity and how these are being managed. In addition, the following may be considered: 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 The report to be prepared by the risk management unit.
Risk Management Assurance Report	1. Governing Body 2. Audit committee 3. Board risk assurance committee 4. Risk Management committee	Periodic as per audit plan	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.

	5. External Audit and Other External Review And Regulatory Bodies		The report to be prepared by the Head of Internal Audit
Operational Risk Report	1. Accounting Officer 2. Risk Management committee 3. Head of Risk Management Function 4. Head Internal Audit Unit	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 The report to be prepared by the functional head/risk owner or risk management champion
Incident report	1. Head of Departments/Units. 2. Head of Internal audit. 3. Head of Risk Management Function.	Summary monthly reports	1. Risks realized 2. Failed controls 3. Corrective actions taken and their status The report to be prepared by the risk management champion

Note: The entities are expected to develop templates for risk reporting.

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. Code of governance for state corporations, *(Mwongozo)* 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