Republic of Uganda

Ministry of Water and Environment

Administrative Guidelines on the Internal Control Framework and Internal Audit Standards

Integrated Internal Controls System (COSO)
Fraud Risk Management
Risk Management Plan

2018

Contents

Forward ……......…………………………………………………………………………ii
List of Abbreviations ………………………………………………………………………iii
Introduction ……………………………………………………………………………….. 1

Public Accountability …………………………..……………………………………..5

Internal Control Framework ……………………………………………………………..6

Definition of Internal Control 6
Internal Control is a process 7
Internal control is Geared to the Achievement of Objectives 7
Internal Control is Effected by People...8
Internal Control Provides Reasonable Assurance 8
Internal Control is Adaptable to the Entity Structure 9

Relevance of internal control ……………....……………………………….…………9

Internal Control Objectives…………………………………………………………….9

Objectives Setting and Internal Control..10
Components/Elements of Internal Control 10
Control Environment – 11
Risk Assessment 12
Control Activities 12
Information and Communication...13
Monitoring 13
Relationship of Objectives, Components, and MWE: 14
Objectives 15
Internal Control Activities 15
Roles and Responsibilities of Internal Control 16
Responsible Parties...16
The TPC/TPM and Its Committees 17
The Permanent Secretary (PS)...17
Other Members of Senior Management...18
Other MWE Personnel..19

Assessing Internal Controls…………………………………………………………...19

Establish scope and accountability: 20
Identify and document risks and controls: 20
Evaluate effectiveness of controls: 20
Identify control gaps and deficiencies; develop remediation plan(s):...21
Monitor and report on issues and report to management:..21
Internal Control Review 21

Internal Control Self-Assessment Checklist……………………………………………..22

Forward

In the past, management of risk in the public service has not received adequate attention. With the enactment of the Public Financial Management Act (PFMA) 2015, the foundation has been laid for a more effective corporate governance framework as well as an accountable financial management system for the public sector. The Act has also established the legal framework for risk management in the public sector.

Today, more than ever, all the officials in the employment of Ministry of Water and Environment (MWE) should be taking a long, hard look at risk – the threats to success and the possible consequences if they materialize. The importance of looking at risk comes in the wake of a more demanding society, bold initiatives and more challenge when things go wrong. Public sector risk management and control should be firm on the agenda for every official involved in MWE. Effective risk management processes in this Ministry will ultimately help achieve:

- Clarity of the Ministry's purpose by clearly identifying policy needs and actions required to meet its strategic objectives,
- More cohesiveness of effort through organizational consistency and clear role definition,
- Better decisions making through consideration of issues,
- Faster reactions through concentration on key performance trends, and
- Promotion of integrity, transparency and accountability by recording decisions in context and allocating responsibility for action.

As a good practice, risk management processes and responsibilities are incorporated in the list of responsibilities allocated to Ministry's Top Management, Accounting Officer and Audit Committees. However, these responsibilities are extended to all Managers as per the provisions of the PFMA-2015. The PFMA establishes responsibility for Risk Management at all levels of management including project/programme managers and thus becomes everybody's responsibility. This should be seen as a medium term vision and to be successful it must assist in organizational and individual behavioral change and therefore of benefit to the individual as well as the entire Ministry of Water and Environment.

The development of this Risk Management Framework has been aligned to the Integrated Internal Controls System (COSO-2013), to ensure a consistent approach to risk management in organizations. We therefore endorse the adoption of this risk management framework as a fundamental step towards an outward looking, accountability and innovative risk control process in this Ministry.

I therefore on behalf of the Ministry of Water and Environment wish to express our appreciation to all our stakeholders who contributed to the formulation of this Integrated Internal Control Framework.

Alfred Okot Okidi
Permanent Secretary

List of Abbreviations

CFO	Chief Financial Officer
COSO	Committee of Sponsoring Organizations
DEA	Directorate of Environmental Affairs
DWD	Directorate of Water Development
DWRM	Directorate of Water Resources Management
ENR-SWG	Environment and Natural Resources Sub-Sector Working Group
ERM	Enterprise Risk Management
GoU	Government of Uganda
LANs	Local Area Networks
MWE	Ministry of Water and Environment
NEMA	National Environment and Management Authority
NFA	National Forestry Authority
NWSC	National Water and Sewerage Corporation
PFMA	Public Finance Management Act
PS	Permanent Secretary
TPC	Top Policy Committee
TPM	Top Policy Management
WESWG	Water and Environment Sector Working Group
WSSWG	Water and Sanitation Sub-Sector Working Group
UNMA	Uganda National Meteorological Authority

1.0 Introduction

The Ministry of Water and Environment (MWE) was established following the Cabinet decision in 2007. The Ministry is a lead institution in the Water and Environment Sector. It is responsible for overall coordination, policy formulation, setting standards, inspection, monitoring, technical back-up and initiating legislation. It also monitors and evaluates sector development programmes to keep track of their performance, efficiency and effectiveness in service delivery.

The **Vision** of the Ministry of Water and Environment is '*Sound management and sustainable utilisation of Water and Environment resources for the betterment of the population of Uganda.'*

Its' **Mission** *is 'To promote and ensure the rational and sustainable utilisation, development and effective management of water and environment resources for socio-economic development of the country'*

The **Mandate** of the Ministry is derived from the Constitution of the Republic of Uganda (1995) and the Local Governments Act, CAP 243 and includes initiating *legislation, policy formulation, setting standards, inspections, monitoring, and coordination and back up technical support in relation to water and environment sub sectors*.

1.1 Institutional Framework

The Ministry is comprised of three directorates of Directorate of Water Resources Management (DWRM), Directorate of Water Development (DWD) and Directorate of Environmental Affairs (DEA). In addition the Ministry is supported by stand-alone departments in support to the technical departments such as Finance and Administration Department, Water and Environment Sector Liaison Department and Policy and Planning Department responsible for the strategic planning, budgeting and monitoring and Climate Change Department. The detailed structure is provided under figure 1.

The ministry is guided by the Top Policy Management (TPM) headed by the Senior Minister and assisted by two Ministers of State for Water and Environment respectively. In addition is the Water and Environment Sector Working Group (WESWG) is chaired by the Permanent Secretary and assisted by two co-chairs persons representing Water and Sanitation donor group and Environment and Natural Resources donor group. The WESWG is responsible for the overall sector coordination, resource mobilization and allocation as well as review of progress. The Water and Sanitation Sub-Sector Working Group (WSSWG) and the Environment and Natural Resources Subsector Working Group (ENR-SWG) are responsible for the sector planning and priority setting, implementation, monitoring, supervision and management of their respective subsector in support to the WESWG.

Other key stakeholders include all Heads of Semi-Autonomous Institutions i.e. National Environment Management Authority (NEMA), National Forestry Authority (NFA), National Water and Sewerage Corporation (NWSC) and Uganda National Meteorological Authority (UNMA), Local Government, Donors, Civil Society Organisations and Private Sector.

1.2 Policy, Legal and Regulatory Framework

The key policy, legal and regulatory framework which guide the operations of the Water and Environment Sector includes the following:

The Uganda Constitution (1995), Internal Audit Charter, Public Procurement and Disposal of Public Assets Act 2003 and Public Procurement and Disposal of Public Assets Regulations 2014, the Public Finance Management Act (PFMA-2015), Staff Code of Conduct and Ethics for the Uganda Public Service, MWE Clients Charter 2011-2014, **The** Audit Act, 2008, The Anti-Corruption Act-2011, Zero Tolerance to Corruption Policy (2009), IGG Act 2002. Other legislations include; Uganda Water Action Plan (1995), National Environment Management Policy (1994), National Gender Policy (1997), Water Policy (1999), Uganda Forestry Policy (2001) National Forest Plan, 2002 and Uganda Climate Change Policy (2014), The Local Governments Act Cap (1987) 243, The Water Act (1995), The National Environment Management Authority Act (1995).

Overall purpose of the Enterprise Risk Management Policy and Framework

Institutions operate in environments where factors such as technology, regulation, restructuring, changing service requirements and political influence create uncertainty. Uncertainty emanates from an inability to precisely determine the likelihood that potential events will occur and the associated outcomes.

Enterprise Risk Management (ERM) forms a critical part of any institution's strategic management. It is the process whereby an institution both methodically and intuitively addresses the risk attached to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of activities. ERM is therefore recognized as an integral part of sound organizational management and is being promoted internationally and in Uganda as good practice applicable to the public and private sectors.

Public sector institutions are bound by constitutional mandates to provide products or services in the interest of the public good. As no institution has the luxury of functioning in a risk-free environment, public sector institutions also encounter risks inherent in producing and delivering such goods and services.

All institutions face uncertainty, and the challenge for management is to determine how much uncertainty the institution is prepared to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. The framework provides a basis for management to effectively deal with uncertainty of associated risk and opportunity, thereby enhancing its capacity to build value. Value is maximized when management sets objectives to strike an optimal balance between growth and related risks, and effectively deploys resources in pursuit of the institution's objectives. It is accordingly accepted by all stakeholders that MWE will manage risks faced in an appropriate manner.

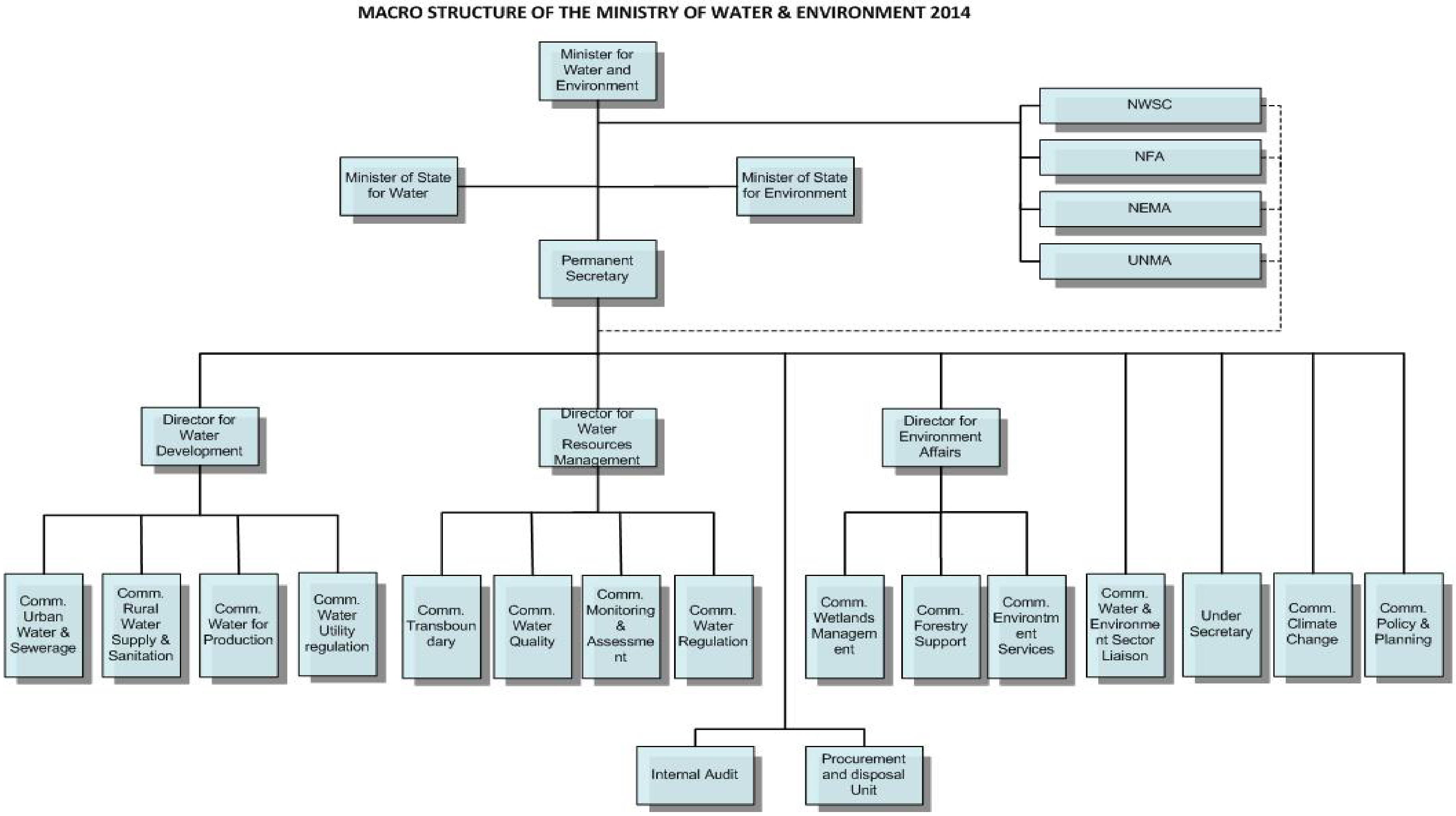
The *Enterprise Risk Management Policy* provides a framework within which management can operate to enforce the pro-active ERM process and to inculcate the risk management culture throughout MWE and to further ensure that the risk management efforts of MWE are optimized. It describes MWE's ERM processes and sets out the requirements for management in generating risk management action, together with furthering risk management assurance. This document further sets out MWE’s policy on the management of risk at all levels of the organization.

The *Enterprise Risk Management Framework* specifically addresses the structures, processes and standards implemented to manage risks on an enterprise-wide basis in a consistent manner.

MWE is not homogenous and therefore, this framework sets out the principles to support effective risk management. MWE is expected to apply these principles in developing systems that are tailored to their specific environments. As the field of risk management is dynamic, this framework document is expected to change from time to time.

Current trends in good corporate governance, most notably the King Report on Corporate Governance (King III), have given special prominence to the process of ERM and reputable organizations are required to demonstrate that they comply with expected risk management standards. This means that MWE must ensure that the process of risk management receives special attention throughout the organization and that *all levels of management know, understand and comply with the framework document.*

Figure 1: Macro Structure of Ministry Water and Environment


MACRO STRUCTURE OF THE MINISTRY OF WATER & ENVIRONMENT 2014
Minister for Water and Environment
Minister of State for Water
Minister of State for Environment
Permanent Secretary
NWSC
NFA
NEMA
UNMA
Director for Water Development
Director for Water Resources Management
Director for Environment Affairs
Comm. Urban Water & Sewerage
Comm. Rural Water Supply & Sanitation
Comm. Water for Production
Comm. Water Utility regulation
Comm. Transboundary
Comm. Water Quality
Comm. Monitoring & Assessment
Comm. Water Regulation
Comm. Wetlands Management
Comm. Forestry Support
Comm. Environtment Services
Comm. Water & Environment Sector Liaison
Under Secretary
Comm. Climate Change
Comm. Policy & Planning
Internal Audit
Procurement and disposal Unit

1.3 Justification of MWE Internal Control Framework

In the exercise of the duties under the Public Finance Act (PFA) 2015, Section 45(2) states provides the basis for Accounting officers to put in place an effective system of controls. It states, “An Accounting Officer shall, in respect of all resources and transactions of a vote, put in place effective systems of risk management, internal control and internal audit”.

The primary purpose of establishing internal controls is to mitigate risks which could prevent the MWE from achieving its strategic objectives. Consequently, the Top Policy Committee (TPC) of MWE has used the mandate granted in the PFA 2015 to establish an internal control framework for the ministry of Water and Environment (MWE) to:

a) Provide the MWE with a systematic approach to implementing a system of internal controls over its processes and activities;

b) Help to provide internal and external stakeholders with the assurance that the MWE’s financial and operational processes are managed in a manner that supports the achievement of its strategic plans and priorities as set out by the TPC;

c) Identify the requirements for establishing an effective internal control system for the MWE, with the requisite objectives, components and concepts;

d) Provide a mechanism for identifying and managing systemic risks that could affect the achievement of its business objectives and/or expose the MWE to financial risk and potential loss;

e) Set a baseline for establishing a system of control activities that is proportionate to the level of risk required to safeguard the MWE’s assets, taking into account the MWE’s risk profile, including its risk appetite; and

f) Establish MWE climate and enabling culture within the MWE that will enhance its mission based on ethical values and a well-defined code of conduct.

The secondary purpose is to provide the tools for the ministry and departments to establish and maintain these internal controls.

1.4 Public Accountability

The TPC and Permanent Secretary (PS) of MWE are accountable to the GOU, funding partners and the public at large in conducting the affairs of the ministry. MWE Commissioners and other senior management including appointed department heads are also accountable to the public.

Their role is to ensure that their decisions and actions while executing their mandate meet four basic elements, which form the essence of public accountability:

a) Effectiveness: achieving the MWE’s goals
b) Efficiency: making optimal use of scarce resources
c) Compliance: observing restrictions on the use of resources and complying with mandates

d) Reporting: periodically demonstrating accountability for the stewardship of resources placed in their care.

The TPC and department heads are responsible for maintaining sufficient internal controls to obtain reasonable assurance that the ministry and department goals are achieved efficiently and in compliance with established laws. Reasonable assurance of public accountability is achieved by maintaining strong internal controls within the MWE, at least equivalent to the *Internal Control recommendations* issued by the GOU in the various public financial management frameworks.

Therefore, implementing internal controls that conform to the *Internal Control – Integrated Framework* (2013) issued by the Committee on Sponsoring Organization of the Treadway Commission (COSO) will go a long way in helping MWE to achieve adequate public accountability.

1.5 Internal Control Framework

Section 45 (2) requires accounting officers in the exercise of their duties under this Act, in respect of all resources and transactions of a vote, to put in place effective systems of risk management, internal control and internal audit.

A system of internal control allows MWE management to stay focused on the MWE's pursuit of its operations and financial performance goals, while operating within the confines of relevant laws and minimizing surprises along the way. Internal control enables MWE to deal more effectively with changing economic and competitive environments, leadership, priorities, and evolving business models.

The purpose of MWE adopting the COSO Internal Control - Integrated Framework (Framework) is to help MWE management better control MWE and to provide the TPC with an added ability to oversee internal control.

MWE's implementation of controls under this COSO framework will take into consideration the following:

a) Design of any controls or control processes will be adaptable to the structure of the MWE and the dynamic nature of the risk environment within which the MWE operates;

b) New measures or changes to controls will be reviewed as part of a process, taking into consideration any compensating controls to ensure there is an optimum balance between control and efficiency; and

c) Costs incurred for the implementation of a control will not ordinarily outweigh its benefits, although exceptions could occur where the cost of a key control is not a factor for consideration.

Definition of Internal Control

Internal control is ***a process***, ***effected by MWE's TPC***, management, and other personnel, ***designed to provide reasonable assurance*** regarding the ***achievement of objectives*** relating to operations, reporting and compliance.

This definition emphasizes that internal control is:

- *Geared to the achievement of objective*s in one or more separate but overlapping categories - operations, reporting and compliance
- *A process* consisting of ongoing tasks and activities - it is a means to an end, not an end in itself
- *Effected by people* - not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of MWE to effect internal control
- Able to *provide reasonable assurance* - but not absolute assurance, to MWE's senior management and the TPC.
- *Adaptable to the ministry structure* - flexible in application for the entire MWE or for a particular division, operating unit, or business process

Internal control is therefore a process effected by MWE management and staff that is designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- *Effectiveness and efficiency of operations*
- *Reliability of financial reporting*
- *Compliance with applicable laws and regulations*

All levels of MWE management are responsible for establishing internal control processes to help the Ministry achieve its mission, to stay on course toward meeting financial goals, to minimize risk, and to more effectively deal with change.

Internal Control is a process

Internal control is not one event or circumstance, but a dynamic and iterative process - actions that permeate MWE's activities and that are inherent in the way management runs the ministry. Embedded within this process are controls consisting of policies and procedures. These policies reflect management or TPC statements of what should be done to effect internal control. Such statements may be documented, explicitly stated in other management communications, or implied through management actions and decisions. Procedures consist of actions that implement a policy.

Business processes, which are conducted within or across operating units or functional areas, are managed through the fundamental management activities, such as planning, executing, and checking. Internal control is integrated with these processes. Internal control embedded within these business processes and activities are likely more effective and efficient than stand-alone controls.

Internal control is geared to the Achievement of Objectives

The Framework sets forth three categories of objectives, which allow MWE to focus on separate aspects of internal control:

- *Operations Objectives* - These pertain to effectiveness and efficiency of the ministry's operations, including operational and financial performance goals, and safeguarding assets against loss.
- *Reporting Objectives* - These pertain to internal and external financial and non-financial reporting and may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, standard setters, or the ministry's policies.
- *Compliance Objectives* - These pertain to adherence to laws and regulations to which the ministry is subject.

These distinct but overlapping categories - a particular objective can fall under more than one category - address different needs and may be the direct responsibility of different individuals. The three categories also indicate what can be expected from internal control.

A system of internal control is expected to provide MWE with reasonable assurance that those objectives relating to external reporting and compliance with laws and regulations will be achieved. Achieving those objectives, which are based largely on laws, rules, regulations, or standards established by legislators, regulators, and standard setters, depends on how activities within the ministry's control are performed. Generally, management and/or the TPC have greater discretion in setting internal reporting objectives that are not driven primarily by such external parties. However, MWE may choose to align its internal and external reporting objectives to allow internal reporting to better support the ministry's external reporting.

Internal Control is effected by People

Internal control is effected by the TPC, management, and other personnel. It is accomplished by the people of MWE, by what they do and say. People establish the ministry's objectives and put actions in place to achieve specified objectives.

The TPC's oversight responsibilities include providing advice and direction to management, constructively challenging management, approving policies and transactions, and monitoring management's activities. Consequently, the TPC is an important element of internal control. The TPC and senior management establish the tone for MWE concerning the importance of internal control and the expected standards of conduct across the ministry.

People must know their responsibilities and limits of authority. Accordingly, a clear and close linkage needs to exist between people's roles and responsibilities and the way in which these duties are communicated, carried out, and aligned with the ministry's objectives.

Internal Control Provides Reasonable Assurance

Reasonable assurance does not imply that MWE will always achieve its objectives. Effective internal control increases the likelihood of MWE achieving its objectives. However, the likelihood of achievement is affected by limitations inherent in all systems of internal control, such as human error, the uncertainty inherent in judgment, and the potential impact of external events outside management's control. Additionally, a system of internal control can be circumvented if people collude. Further, if management is able to override controls, the entire system may fail. Even though MWE’s system of internal control should be designed to prevent and detect collusion, human error, and management override, an effective system of internal control can experience a failure.

Internal Control is Adaptable to the Entity Structure

The legal entity structure of MWE is typically designed to follow regulatory reporting requirements, limit risk, or provide tax benefits. Often MWE of legal entities is quite different from the management operating model used to manage operations, allocate resources, measure performance, and report results.

Internal control can be applied, based on management’s decisions and in the context of legal or regulatory requirements, to the management operating model, legal entity structure, or a combination of these.

Relevance of internal control

Internal controls are used to manage risks and as a result are fundamental to how the MWE operates. They are designed, implemented and continuously adapted to the MWE’s systems and processes. In particular:

a) Internal controls are an inseparable part of the day-to-day activities of the MWE, from information technology and travel to hiring and processing transactions. Internal controls create an environment that helps management to efficiently manage resources and achieve operational goals and objectives;

b) Internal controls are designed to assist managers and MWE staff with the effective discharge of their responsibilities; and

c) Controls are embedded within the internal control processes, which consist of guidelines and procedures.

Internal Control
Effectiveness and Efficiency of Operations
Compliance with applicable Laws and Regulations
Reliability of Financial and Non-Financial Reporting

Internal Control Objectives

The TPC at MWE must establish internal control objectives to effectively assess areas of potential risk. The following key internal control objectives apply to Ministry department heads and managers:

- Accuracy of financial statements – sound information systems
- Validity of transactions, timeliness and completeness in processing transactions
- Compliance with applicable regulations and internal policy frameworks
- Economy, efficiency, and effectiveness

- Economy is getting inputs that can do the job at the best price
- Efficiency is getting the best results from inputs, fine tuning processes so that they work well and are up to date
- Effectiveness is getting the right results, achieving Ministry objectives

Objectives Setting and Internal Control

MWE has a strategic plan that sets out its mission and vision. It also sets out strategies, and the objectives MWE wants to achieve. To support MWE in its efforts to achieve objectives the COSO framework has five components/elements of internal control:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring Activities

Components/Elements of MWE's Internal Control

The following five elements of control standards and 17 principles shall be considered and adopted by all MWE management and staff in its operations.

Component/Element	Principle
Control Environment	1. MWE demonstrates a commitment to integrity and ethical values
	2. The TPC demonstrates independence from management and exercises oversight of the development and performance of internal control.
	3. Management establishes, with TPC oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
	4. MWE demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
	5. MWE holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
Risk Assessment	6. MWE specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
	7. MWE identifies risks to the achievement of its objectives across the ministry and analyzes risks as a basis for determining how the risks should be managed.
	8. MWE considers the potential for fraud in assessing risks to the achievement of objectives.
	9. MWE identifies and assesses changes that could significantly impact the system of internal control.
Control Activities	10. MWE selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
	11. MWE selects and develops general control activities over technology to support the achievement of objectives.
	12. MWE deploys control activities through policies that establish what is expected and procedures that put policies into place.

Component/Element	Principle
Information and Communication	13. MWE obtains or generates and uses relevant, quality information to support the functioning of internal control.
	14. MWE internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
	15. MWE communicates with external parties regarding matters affecting the functioning of internal control.
Monitoring Activities	16. MWE selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
	17. MWE evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the TPC, as appropriate.

Control Environment

The control environment sets the tone for MWE. It provides discipline and structure and strongly influences the control consciousness of the people within MWE. The control environment at MWE begins with the administration's philosophy and operating style as well as the priorities and direction provided by the STP. Key factors in the control environment include the integrity, ethical values, and competence of personnel. MWE's philosophy regarding integrity and ethical values are reflected in the Code of Ethics for Public Servants. A confidential avenue of communication is available in the ministry for reporting Financial Irregularities and documented in the whistle blowing policy. Competency of MWE personnel is ensured through a systematic hiring process, periodic evaluations that include performance and ethical standards, ongoing training, and professional development programs.

In addition to each of the principles set out above, COSO develops these further into points of focus to help management consider how the principle can be successful and that the component is addressed in MWE's system of control.

Control Environment	
Principle	**Point Of Focus**
1. MWE demonstrates a commitment to integrity and ethical values.	Sets the tone at the top
	Establishes standards of conduct
	Evaluates adherence to standards of conduct
	Addresses deviations in a timely manner
2. The TPC demonstrates independence from management and exercises oversight of the development and performance of internal control.	Establishes oversight responsibilities
	Operates independently
	Applies relevant expertise
	Provides oversight for the system of internal control
3. Management establishes, with TPC oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Considers all structures of the ministry
	Establishes reporting lines
	Defines, assigns, and limits authorities and responsibilities
4. MWE demonstrates a commitment to attract,	Establishes policies and practices

develop, and retain competent individuals in alignment with objectives.	Evaluates competence and addresses shortcomings
	Attracts, develops, and retains individuals
	Plans and prepares for succession
5. MWE holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Enforces accountability through structures, authorities, and responsibilities
	Establishes performance measures, incentives, and rewards
	Evaluates performance measures, incentives, and rewards for ongoing relevance
	Considers excessive pressures
	Evaluates performance and rewards or disciplines individuals

Risk Assessment

Risk assessment is the identification and analysis of relevant risks which may prevent the Ministry or a department from meeting its operational, financial, and compliance objectives. MWE management should assess risk based on the types of activities performed, organizational structure, staffing levels, and attitudes within the department. Internal Control Guides and risk matrixes are available to assists departments in assessing and analyzing risks.

Risk Management	
Principle	**Point Of Focus**
6. MWE specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Define objectives
	Define Risk Tolerance
7. MWE identifies risks to the achievement of its objectives across the ministry and analyzes risks as a basis for determining how the risks should be managed.	Risk identification
	Risk Analysis
	Risk Response
8. MWE considers the potential for fraud in assessing risks to the achievement of objectives.	Fraud Risk factors and response
9. MWE identifies and assesses changes that could significantly impact the system of internal control.	Identification of Change
	Analysis and response to change.

Control Activities

Control activities are the policies and procedures established to ensure that management's directives are implemented. MWE managers must be cognizant of the Ministry policies and procedures and supplement these procedures with department level guidance when necessary. MWE being a government entity uses the GOU public financial management Policy frameworks In addition, MWE recommends specific control activities in its Internal Control Guides to mitigate its sector specific risks.

Control Activities	
Principle	**Point Of Focus**
10. MWE selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Design of control activities
	Segregation of Duties
11. MWE selects and develops general control activities	Design of information control activities

over technology to support the achievement of objectives.	Design of information technology infrastructure
12. MWE deploys control activities through policies that establish what is expected and procedures that put policies into place.	Documentation of policies
	Periodic review of policies

Information and Communication

Pertinent information must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems produce reports containing operational, financial and compliance-related information that make it possible to run and control the Ministry business. The reports deal not only with internally generated data, but also information about external events, activities and conditions necessary to informed business decision-making and external reporting.

All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. MWE managers need solid lines of communication between the department and central functions as well as between department management and staff. MWE communication channels are used to ensure communication effectively flows down, across, and up MWE.

Information Communication	
Principle	**Point Of Focus**
13. MWE obtains or generates and uses relevant, quality information to support the functioning of internal control.	Data is processed into relevant and reliable information
14. MWE internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Communications by Management reach all levels of MWE.
	Communications flow up to Management.
15. MWE communicates with external parties regarding matters affecting the functioning of internal control.	Public Information Office is the designated focal point for external communications.
	Appropriate communication methods are utilized.

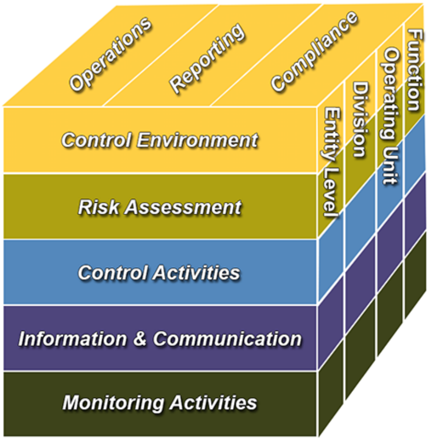
Monitoring

Monitoring is a process that assesses the quality of the internal control process over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the course of operations and includes regular management and supervisory activities such as reviewing reconciliations and summary reports. MWE managers are responsible for monitoring the activities performed within their department; central administration is responsible for evaluating internal controls within each department and monitoring activities within a department when deemed necessary.

Monitoring	
Principle	**Point Of Focus**
16. MWE selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Establish a baseline between the internal control design and current state
	Monitoring activities are performed to evaluate effectiveness of the internal control system.
	Evaluation of the monitoring results are performed to continually improve the system.
17. MWE evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the TPC of directors, as appropriate.	Issues are evaluated for deficiency in design or operating effectiveness.
	Corrective action is completed on a timely basis by the control owner.

Relationship of Objectives, Components, and MWE:

A direct relationship exists between *objectives*, which are what MWE strives to achieve, *components*, which represent what is required to achieve the objectives, and *entity structure* (the operating units, legal entities, and other structures). The relationship can be depicted in the form of a cube.



- The three categories of objectives operations, reporting, and compliance are represented by the columns.
- The five components/elements of internal control are represented by the rows.
- The entity structure, which represents the overall MWE, divisions, subsidiaries, operating units, or functions, including business processes such as Procurement, Engineering, etc. and to which internal control relates, are depicted by the third dimension of the cube.

Each component cuts across and applies to all three categories of objectives. For example, attracting, developing, and retaining competent people who are able to conduct internal control - part of the control environment component - is relevant to all three objectives categories.

The three categories of objectives are not parts or units of the ministry. For instance, operations objectives relate to the efficiency and effectiveness of operations, not specific operating units or functions such as Procurement, Engineering, or human resources.

Accordingly, when considering the category of objectives related to reporting, for example, knowledge of a wide array of information about the ministry's operations is needed. In that case, focus is on the middle column of the model—reporting objectives—rather than on the operations objectives category.

Internal control is a dynamic, iterative, and integrated process. For example, risk assessment not only influences the control environment and control activities, but also may highlight a need to reconsider the ministry's requirements for information and communication, or for its monitoring activities. Thus, internal control is not a linear process where one component affects only the next. It is an integrated process in which components can and will impact another.

Objectives

Management, with TPC oversight, sets objectives that align with the ministry's mission, vision, and strategies. These high-level objectives reflect choices made by management and TPC about how MWE seeks to create, preserve, and realize value for its stakeholders. Such objectives may focus on the ministry's unique operation needs, or align with laws, rules, regulations, and standards imposed by legislators, regulators, and standard setters, or some combination of the two. Setting objectives is a prerequisite to internal control and a key part of the management process relating to strategic planning.

Individuals who are part of the system of internal control need to understand the overall strategies and objectives set by MWE. As part of internal control, management specifies suitable objectives so that risks to the achievement of such objectives can be identified, assessed and managed. Specifying objectives includes the articulation of specific, measurable or observable, attainable, relevant, and time-bound objectives.

Internal Control Activities

The following internal control activities are tools used in accomplishing the objective of setting up an internal control system:

Establishing a Control Conscious Environment – Setting the tone at the top within the Ministry and each department is essential in developing sound internal controls. Ensuring MWE staff are properly trained, are knowledgeable of Ministry policies and procedures, and receive feedback on a regular basis are key factors to a good control conscious environment.

Segregation of Duties – The separation of certain functions such as initiating, authorizing, recording and reconciling transactions is an important control activity. The amount of segregation possible within a function depends on the size and structure of the department. However, every effort should be made by MWE managers to ensure that one person does not have control over all parts of a transaction or process. Guidance for segregation within established Ministry processes is provided through segregation of duties matrixes.

Authorization/Approval Processes – Approving and authorizing responsibilities within MWE departments should be limited to as few people as possible. Any delegated purchasing authority should be clearly documented on the MWE annual statement of delegated authority. System passwords are used as an integral part of the MWE approval process and must be kept confidential. Supportive documentation should be reviewed for each transaction to verify business purpose, budgetary constraints and compliance.

Physical Control of Assets – MWE business managers are responsible for the physical control of assets within the department. Safeguards should be implemented to ensure proper accountability of assets.

Monitoring – Monitoring activities by MWE managers would include such things as monthly financial statement review (ie, budget to actual reports), departmental feedback sessions, and internal control self-assessments. The MWE Quality Assurance Support Team performs central monitoring functions. The ministry's Internal Audit Division provides independent monitoring through internal audits.

Roles and Responsibilities of Internal Control

Internal control is effected by personnel internal to the ministry, including the TPC and its committees, management and personnel, business-enabling functions, and internal auditors. Collectively, they contribute to providing reasonable assurance that specified objectives are achieved.

MWE views internal control through the following three lines of defense:

- Management and other personnel on the front line provide the first line of defense as they are responsible for maintaining effective internal control day to day; they are compensated based on performance in relation to all applicable objectives.
- Business-enabling functions such as risk, control, legal, and compliance provide the second line of defense as they clarify internal control requirements and evaluate adherence to defined standards. While they are functionally aligned to the business, their compensation is not directly tied to performance of the area to which they render expert advice.
- Internal audit provides the third line of defense it assesses and reports on internal control and recommend corrective actions or enhancements for management to consider and implement;

Responsible Parties

Every individual within MWE has a role in effecting internal control. Roles vary in responsibility and level of involvement, as discussed below.

The TPC and Its Committees

The TPC is responsible for overseeing the system of internal control. The TPC has a key role in defining expectations about integrity and ethical values, transparency, and accountability for the performance of internal control responsibilities. TPC members are objective, capable, and inquisitive. They have a working knowledge of the ministry's activities and environment, and they commit the time necessary to fulfill their governance responsibilities. They utilize resources as needed to investigate any issues, and they have an open and unrestricted communications channel with all MWE personnel, the internal auditors, independent auditors, external reviewers, and legal counsel.

As part of its governance, risk and compliance oversight responsibilities, the TPC has a critical role in ensuring the effectiveness of internal controls by:

- Setting the "tone at the top" and organizational climate for the MWE;
- Providing oversight for the system of internal control;
- Overseeing the adequacy of the MWE's system of internal controls; and
- Being informed of any significant control deficiencies or breakdowns in the MWE.

The Permanent Secretary (PS)

The PS is accountable to the TPC and is responsible for designing, implementing, and conducting an effective system of internal control. More than any other individual, the PS sets the tone at the top that affects the control environment and all other components of internal control.

The PS's responsibilities relating to internal control include:

- With the support of management, providing leadership and direction to senior management, shaping MWE values, standards, expectations of competence, organizational structure, and accountability that form the foundation of the ministry's internal control system (e.g. specifying MWE objectives and policies)
- Maintaining oversight and control over the risks facing the ministry (e.g., directing all management and other personnel to proactively identify risks to the system of internal control, considering the ever-increasing pace of change and networked interactions of business partners, outsourced service providers, customers, employees, and others and resulting risk factors)
- Guiding the development and performance of control activities at the ministry level, and delegating to various levels of management the design, implementation, conduct, and assessment of internal control at different levels of the ministry (e.g., processes and controls to be established)
- Communicating expectations (e.g., integrity, competence, key policies) and information requirements (e.g., the type of planning and reporting systems the ministry will use)
- Evaluating control deficiencies and the impact on the ongoing and long-term effectiveness of the system of internal control (e.g., meeting regularly with senior management from each of the operating units such as research and development,

production, marketing, sales, and major business-enabling functions such as finance, human resources, legal, compliance, risk management to evaluate how they are carrying out their internal control responsibilities)

Other Members of Senior Management

Senior management comprises not only the PS but also the other senior executives leading the key operating units and business-enabling functions. Examples include:

- Commissioners
- Chief Internal auditor
- Financial officer
- Information officer
- Legal officer
- Risk officer
- Other senior leadership roles, depending on the nature of the ministry

Senior management guides the development and implementation of internal control policies and procedures that address the objectives of their functional or operating unit and verify that they are consistent with the ministry-wide objectives. They provide direction, for example, on a unit's organizational structure and personnel hiring and training practices, as well as budgeting and other information systems that promote control over the unit's activities. As such, through a cascading responsibility structure, each executive is a PS for his or her sphere of responsibility.

Senior management roles support the PS with respect to internal control, specifically by:

- Providing leadership and direction to management in terms of shaping MWE values, standards, expectations of competence, organizational structure, and accountability that form the foundation of the ministry's internal control system (e.g. specifying MWE objectives and policies)
- Maintaining oversight over the risks facing the ministry (e.g., directing all management and other personnel to proactively identify risks to the system of internal control, considering the ever-increasing pace of change and networked interactions of business partners, outsourced service providers, customers, employees, and others and resulting risk factors)
- Guiding the development and performance of controls at the ministry level, and delegating to various levels of management the design, implementation, conduct, and assessment of internal control at different levels of the ministry (e.g., processes and controls to be established)
- Communicating expectations (e.g., integrity, competence, key policies) and information requirements (e.g., the type of planning and reporting systems the ministry will use)
- Evaluating internal control deficiencies and the impact on the ongoing and long-term effectiveness of the system of internal control (e.g., meeting regularly with finance, controllership, risk management, information technology, human resources, and business management from each of the operating units to evaluate how they are carrying out their internal control responsibilities)

The chief financial officer (CFO) supports the PS in front-line responsibilities, including internal control over financial reporting. The CFO may at times be required by law to certify to the effectiveness of internal control over financial reporting, alongside the PS.

Other MWE Personnel

Internal control is the responsibility of everyone in the ministry and therefore constitutes an explicit or implicit part of everyone's job description. Front-line personnel constitute the first line of defense in the performance of internal control responsibilities. Examples include:

- Control Environment - Reading, understanding, and applying the standards of conduct of MWE
- Risk Assessment - Identifying and evaluating risks to the achievement of objectives and understanding established risk tolerances relating to their areas of responsibility
- Control Activities - Performing reconciliations, following up on exception reports, performing physical inspections, and investigating reasons for cost variances or other performance indicators
- Information and Communication - Producing and sharing information used in the internal control system (e.g., inventory records, work-in-process data, expense reports) or taking other actions needed to effect control
- Monitoring Activities - Supporting efforts to identify and communicate to higher-level management issues in operations, non-compliance with the code of conduct, or other violations of policy or illegal actions.

The care with which those activities are performed directly affects the effectiveness of the internal control system. Internal control relies on checks and balances, including segregation of duties, and on employees not "looking the other way." Personnel must understand the need to resist pressure from superiors to participate in improper activities, and channels outside normal reporting lines are available to permit reporting of such circumstances.

Assessing Internal Controls

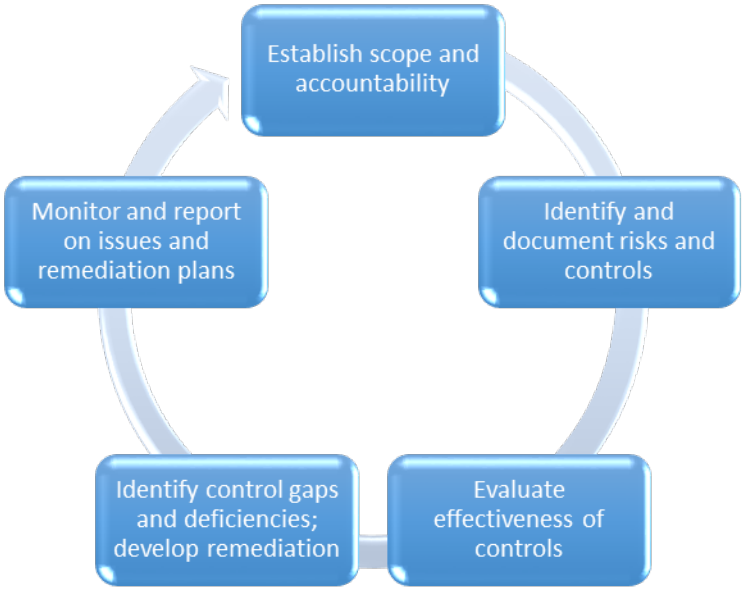
The criteria for determining the effectiveness of internal controls are based on the presence and complete integration of the five components of control indicated above to ensure that risk mitigation is sufficient to allow achievement of the objectives. In order to determine if the components in each category are jointly effective, each component must be individually assessed using the principles and points of focus herein included the accompanying spreadsheet.

When assessing the effectiveness of internal controls, MWE should;

- consider what are the significant risks and assess how they have been identified, evaluated and managed;
- assess the effectiveness of the related system of internal control in managing the significant risks, having regard, in particular, to any significant failings or weaknesses that have been reported;

- consider whether necessary actions are being taken promptly to remedy any significant failings or weaknesses; and
- consider whether the findings indicate a need for more extensive monitoring of the system of internal control.

There are five steps to assessing the effectiveness of internal controls based on the COSO framework.


Establish scope and accountability
Identify and document risks and controls
Evaluate effectiveness of controls
Identify control gaps and deficiencies; develop remediation
Monitor and report on issues and remediation plans

Establish scope and accountability:

- Gain an understanding of the key activities that support the objectives and deliverables of the ministry or business unit;
- Determine the relevant processes and systems linked to the key activities; and
- Determine the business owner accountable for the activity and related internal controls.

Identify and document risks and controls:

- Document the relevant business processes in flowcharts or narratives;
- Identify the risks and controls in the business unit's processes and systems across various risk categories;
- Map specific control activities to control objectives and risks; and
- Classify controls as key controls, secondary controls or compensating controls.

Evaluate effectiveness of controls:

- Rank and prioritize risks based on financial impact and likelihood of occurrence;
- Evaluate the mitigating controls for effectiveness by reviewing the control's design and operating effectiveness; and
- Rate controls as effective or ineffective based on their ability to mitigate the relevant risks.

Identify control gaps and deficiencies; develop remediation plan(s):

- Review the ineffective controls to determine the nature of the control deficiencies (a deficiency is defined as a shortcoming in some aspect of the system of internal control that has the potential to adversely affect the ability of the ministry to achieve its objectives);
- Assess the impact and severity of the deficiency;
- Evaluate the deficiency as to its materiality; and
- Develop a remediation plan for the identified deficiencies.

Monitor and report on issues and report to management:

- Monitor and track control issues and remediation plans;
- Report to management highlighting the key risks faced by the unit, the status of remediation plans and the areas requiring management attention; and
- Ensure regular status reports to management until remediation is complete.

Internal Control Review

Reviewing the effectiveness of internal control is an essential part of the TPC's responsibilities while management is accountable to the TPC for developing, operating and monitoring the system of internal control and for providing assurance to the TPC that it has done so.
Aspects of the review work may be delegated to the Audit Committee and other appropriate TPC committees such as a Risk Committee or Health and Safety Committee. However, the TPC as a whole should form its own view on the adequacy of the review after due and careful enquiry by it or its committees.

When reviewing the system of internal controls during the year, the TPC should:

- consider what are the significant risks and assess how they have been identified, evaluated and managed;
- assess the effectiveness of the related system of internal control in managing the significant risks, having regard, in particular, to any significant failings or weaknesses that have been reported;
- consider whether necessary actions are being taken promptly to remedy any significant failings or weaknesses; and
- consider whether the findings indicate a need for more extensive monitoring of the system of internal control.

In addition to the regular review process, the TPC is required to undertake a specific annual assessment for the purpose of making its public statement on internal control. The assessment should consider issues dealt with in reports reviewed by it during the year together with any additional information necessary to ensure that the TPC has taken account of all significant aspects of internal control. This assessment should cover not only the accounting period, but also the period up to the date of approval of the annual report and accounts.

The TPC's annual assessment should, in particular, consider:

- changes since the last review in the nature and extent of significant risks and MWE's ability to respond effectively to changes in its business and external environment;

- the scope and quality of management’s ongoing monitoring of risks and the system of internal control, and, where applicable, the work of its internal audit function and other providers of assurance;
- the extent and frequency of the communication of the results of the monitoring to the TPC - or TPC committees - which enables it to build up a cumulative assessment of the state of control in MWE and the effectiveness with which risk is being managed;
- the incidence of significant control failings or weaknesses that have been identified at any time during the period and the extent to which they have resulted in unforeseen outcomes or contingencies that have had, could have had, or may in the future have, a material impact on MWE’s financial performance or condition; and the effectiveness of MWE’s reporting process.

Internal Control Self-Assessment Checklist

Management is responsible to establish internal controls to keep their MWE on course toward its financial goals, to help it achieve its mission, to minimize surprises and risks, and to allow the organization to successfully deal with change. Internal controls are defined as activities undertaken to increase the likelihood of achieving management objectives in three areas:

- Efficiency and effectiveness of operations
- Reliability of financial reporting
- Compliance with laws and regulations

Some internal controls are established at the institutional level; others are established by MWE management. To achieve success, MWE management needs to (1) be knowledgeable about, and support, institutional controls, and (2) implement practical and effective internal controls specific to the particular MWE. The following checklist is provided to facilitate a self-assessment of internal controls by MWE management of individual departments. It is intended to address general aspects of internal controls, and does not include specific controls applicable to individual MWEs.

Organization of the checklist is consistent with the five interrelated components of internal control defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). The ministry encourages department heads and other MWE management to use this self-assessment checklist to evaluate internal controls in their areas of responsibility. Management should also add to the checklist other controls that apply specifically their MWEs. Internal Audit would be pleased to consult on methods to improve your internal controls.

Index

1. **Control Environment**
   - Integrity and Ethical Values
   - Commitment to Competence
   - Management's Philosophy and Operating Style
   - Organizational Structure
   - Assignment of Authority and Responsibility
   - Human Resource Policies and Practices
2. **Risk Assessment**
3. **Control Activities**
   - Written Policies and Procedures
   - Control Procedures
   - Controls over Information Systems
4. **Information and Communication**
   - Access to Information
   - Communication Patterns
5. **Monitoring**

• Organizational Goals and Objectives • Risk Identification and Prioritization • Managing Change	• Management Supervision • Outside Sources • Response Mechanisms • Self-Assessment Mechanisms

Assessment Factor	**Indication of strong Controls**	**Indication of weak Controls**	**Assessment**				
Strong - Weak							
			1	**2**	**3**	**4**	**5**
Section 1 – Control Environment							
1 - Integrity and Ethical Values							
1.1 Acceptable business practices.	MWE management (department and supervisory staff) understand MWE's policies covering matters such as legitimate use of MWE resources.	Policies are poorly understood					
1.2 Codes of conduct.	MWE management understand MWE's policies governing relationships with sponsors, suppliers, creditors, regulators, the community, and the public at large.	Policies are poorly understood.					
1.3 Conflicts of interests.	MWE management understand MWE's policies regarding potential conflicts of interest.	Policies are poorly understood.					
1.4 Integrity.	MWE management sets a good example and regularly communicates high expectations regarding integrity and ethical values.	Management does not set a good example and/or does not communicate high expectations regarding integrity and ethical values.					
2 – Commitment to Competence							
2.1 Job descriptions.	Responsibilities are clearly defined in writing and communicated as appropriate.	Responsibilities are poorly defined or poorly communicated.					
2.2 Knowledge and Skills.	MWE management (department and supervisory staff) understand the knowledge and skills required to accomplish tasks.	Management does not adequately consider knowledge and skill requirements.					
2.3 Employee competence.	MWE management is aware of competency levels, and is involved in training and increased supervision when competency is low.	Management is not adequately aware of competency levels, or does not actively address problems.					
3 – Management's Philosophy and Operating Style							

Assessment Factor	Indication of strong Controls	Indication of weak Controls	Assessment				
Strong - Weak							
			1	2	3	4	5
3.1 Communication within MWE.	MWE management insists on full and open disclosure of financial or business issues with appropriate department and MWE personnel.	Management is secretive and reluctant to conduct business or deal with issues in an open manner.					
3.2 Laws and regulations.	There is active concern and effort to ensure compliance with the letter and intent of laws and regulations.	Management is willing to risk the consequences of noncompliance.					
3.3 Getting the job done.	Management is concerned with and exerts effort to get the job done right the first time.	Management is willing to get the job done without adequate regard to quality.					
3.4 Exceptions to policy.	Exceptions to policy are infrequent. When they occur they must be approved and well documented.	Exceptions to policy are the norm and are rarely documented.					
3.5 Approach to financial accountability.	Management's approach shows concern and appreciation for accurate and timely reporting. Budgeting and other financial estimates are generally conservative.	Financial accountability is given low priority.					
3.6 Emphasis on meeting budget and other financial and operating goals.	Realistic budgets are established and results are actively monitored. Corrective action is taken as necessary. The MWE learns from, and does not repeat, mistakes.	Management either shows little concern (climate of laxness), or makes unreasonable demands (climate of fear).					
3.7 Approach to decision making.	Decision-making processes are deliberate and consistent. Decisions are made after careful consideration of relevant facts. Policies and procedures are in place to ensure appropriate levels of management are involved.	Decision making is nearly always informal. Management makes arbitrary decisions with inadequate discussion and analysis of the facts.					
4 – Organizational Structure							
4.1 Complexity of the organizational structure.	Complexity of the structure is commensurate with the organization. Lines of reporting are clear and documentation is up-to-date.	Lines of responsibility are unclear or unnecessarily complicated for the size and activities of the entity.					
4.2 Organization charts.	Documentation exists and is up to date.	Documentation does not exist or is out-of-date. The documented structure does not correspond with actual responsibilities.					

Assessment Factor	Indication of strong Controls	Indication of weak Controls	Assessment				
Strong - Weak							
			1	**2**	**3**	**4**	**5**
4.3 Size of the management group.	Size is commensurate with the complexity of the MWE and its growth.	Size is not appropriate (e.g., too many levels, too dispersed, or too "thin").					
4.4 Stability of the management group.	Low turnover.	High turnover.					
5 – Assignment of Authority and Responsibility							
5.1 Delegation of authority and assignment of responsibility for operating and financial functions.	Delegation of authority and assignment of responsibility is clearly defined. Individuals are held accountable for results.	Decisions are dominated by one or a few individuals. Roles and responsibilities of middle management are unclear.					
5.2 Authority limits.	Authority limits are clearly defined in writing and communicated as appropriate.	Policies and procedures covering authority limits are informal or poorly communicated.					
5.3 Delegated signature authority.	Appropriate limits have been placed on each delegation of signature authority. Management reviews and updates signature records as turnover occurs.	Signature authority is delegated without adequate consideration. Delegated authority is not in line with employee knowledge, training, or competence.					
5.4 Knowledge and experience.	Key personnel are knowledgeable and experienced. Management does not delegate authority to inexperienced individuals.	Key personnel are inexperienced. Management delegates authority without regard to knowledge and experience.					
5.5 Resources.	Management provides the resources needed for employees to carry out their duties.	Management does not provide necessary resources.					
6 – Human Resource Policies and Practices							
6.1 Selection of personnel.	A careful hiring process is in place. The Human Resources Department is involved in identifying potential employees based on job requirements.	The hiring process is informal, and sometimes proceeds without adequate involvement by higher-level supervisors.					
6.2 Training.	On-the-job and other training programs have defined objectives. They are effective and important.	Training programs are inconsistent, ineffective, or are given low priority.					

Assessment Factor	**Indication of strong Controls**	**Indication of weak Controls**	**Assessment**				
Strong - Weak							
			1	**2**	**3**	**4**	**5**
6.3 Supervision policies.	Personnel are adequately supervised. They have a regular resource for resolving problems.	Regular supervision does not exist or is ineffective. Employees are frustrated and feel they ‘have nowhere to go’ with issues.					
6.4 Inappropriate behavior.	Inappropriate behavior is consistently reprimanded in a timely and direct manner, regardless of the individual's position or status.	Reprimands are not timely, direct, or are not consistently applied (climate of favoritism).					
6.5 Evaluation of personnel.	An organized evaluation process exists.	The evaluation process is ad hoc and inconsistent. Performance issues are not formally addressed.					
6.6 Methods to compensate personnel.	Compensation decisions are based on a formal process with meaningful involvement of more than one level of management. The effect of performance evaluations on compensation decisions is defined and communicated.	Compensation decisions are ad hoc, inconsistent, or inadequately reviewed by management.					
6.7 Staffing of critical functions.	Critical functions are adequately staffed, with reasonable workloads.	There is inadequate staffing and frequent periods of overwork and "organizational stress."					
6.8 Turnover. Particularly turnover in financially responsible positions.	Low turnover. Management understands root causes of turnover.	High turnover. Management does not understand root causes.					
Section 2 – Risk Assessment							
7 – Organizational Goals and Objectives							
7.1 MWE-wide objectives.	A formal MWE-wide mission or value statement is established and communicated throughout the MWE.	A MWE-wide mission or value statement does not exist.					
7.2 Critical success factors.	Factors that are critical to achievement of MWE-wide objectives are identified. Resources are appropriately allocated between critical success factors and objectives of lesser importance.	Success factors are not identified or prioritized.					
7.3 Activity-level objectives.	Realistic objectives are established for all key activities including operations, financial reporting and compliance considerations.	Activity-level objectives do not exist.					

Assessment Factor	**Indication of strong Controls**	**Indication of weak Controls**	**Assessment**				
Strong - Weak							
			1	**2**	**3**	**4**	**5**
7.4 Measurement of objectives.	MWE-wide and activity level objectives include measurement criteria and are periodically evaluated.	Performance regarding objectives is not measured. Targets are not set.					
7.5 Employee involvement.	Employees at all levels are represented in establishing the objectives.	Management dictates objectives without adequate employee involvement.					
7.6 Long and short-range planning.	Long and short-range plans are developed and are written. Changes in direction are made only after sufficient study is performed.	No organized planning process exists. There are frequent shifts in direction or emphasis.					
7.7 Budgeting system.	Detailed budgets are developed by area of responsibility following prescribed procedures and realistic expectations. Plans and budgets support achievement of MWE-wide action steps.	Budgets do not exist or are "backed into" depending on desired outcome.					
7.8 Strategic planning for information systems.	Planning for future needs is done well in advance of expected needs and considers various scenarios.	The information system lags significantly behind the needs of the business.					
8 – Risk Identification and Prioritization							
8.1 Identification and consideration of external risk factors.	A process exists to identify and consider the implications of external risk factors (economic changes, changing sponsor, student and community needs or expectations, new or changed legislation or regulations, technological developments, etc.) on MWE-wide objectives and plans.	Potential or actual external risk factors are not effectively identified or evaluated.					
8.2 Identification and consideration of internal risk factors.	A process exists to identify and consider the implications of internal risk factors (new personnel, new information systems, changes in management responsibilities, new or changed educational or research programs, etc.) on MWE-wide objectives and plans.	Potential or actual internal risk factors are not effectively identified or evaluated.					
8.3 Prioritization of risks.	The likelihood of occurrence and potential impact (monetary and otherwise) have been evaluated. Risks have been categorized as tolerable or requiring action.	Risks have not been prioritized.					

Assessment Factor	Indication of strong Controls	Indication of weak Controls	Assessment				
Strong - Weak							
			1	**2**	**3**	**4**	**5**
8.4 Approach to studying risks.	In-depth, cost / benefit studies are performed before committing significant MWE resources.	Risks are accepted with little or no study.					
8.5 Process for monitoring risks.	A risk management program is in place to monitor and help mitigate exposures.	Exposure is dealt with on a case by case basis. Regular efforts or programs to manage risks do not exist.					
8.6 Consultation with external advisors.	External advisors are consulted as needed to supplement internal expertise.	Internal expertise regarding risk and control issues is inadequate. Assistance is never sought from outside sources.					
9 – Managing Change							
9.1 Commitment to change.	Management promotes continuous improvement and solicits input and feedback on the implications of significant change.	Management promotes the status quo, even when changes are needed to meet important business needs.					
9.2 Support of change.	Management is willing to commit resources to achieve positive change.	Management offers no resources to facilitate change.					
9.3 Routine change.	Mechanisms exist to identify, prioritize, and react to routine events (i.e., turnover) that affect achievement of MWE-wide objectives or action steps.	Procedures are not present or are ineffective.					
9.4 Economic change.	Mechanisms exist to identify and react to economic changes.	Procedures are not present or are ineffective.					
9.5 Regulatory change.	Mechanisms exist to identify and react to regulatory changes (maintain membership in associations that monitor laws and regulations, participate in MWE forums, etc.).	Procedures are not present or are ineffective.					
9.6 Technological change.	Mechanisms exist to identify and react to technological changes and changes in the functional requirements of the MWE.	Procedures are not present or are ineffective.					
Section 3 – Control Activities							
10 – Written Policies and Procedures							

Assessment Factor	Indication of strong Controls	Indication of weak Controls	Assessment				
Strong - Weak							
			1	**2**	**3**	**4**	**5**
10.1 Access to MWE policies and procedures.	MWE staff have available up to date MWE policy and procedures and know how to use them.	MWE policy and procedures are not available or are rarely used.					
10.2 MWE policies and procedures.	The MWE has documented its own policies and procedures. They are well understood by MWE staff.	MWE policies and procedures do not exist.					
11 – Control Procedures							
11.1 Senior management reviews.	Senior management monitors the MWE's performance against objectives and budget.	Senior management does not monitor MWE performance.					
11.2 Top level (MWE-wide) objective performance reviews by MWE management.	Reviews are made of actual performance compared to objectives and previous periods for all major initiatives. Management analyzes and follows up as needed.	Analyses are not performed or management does not follow up on significant deviations.					
11.3 Top level (MWE-wide) financial performance reviews by MWE management.	Reviews are made of actual performance versus budgets, forecasts, and performance in prior periods for all major initiatives. Management analyzes and follows up as needed.	Analyses are not performed or management does not follow up on significant deviations.					
11.4 Direct functional or activity management by MWE management.	Performance reviews are made of specific functions or activities, focusing on compliance, financial or operational issues.	No performance reviews occur.					
11.5 Performance indicators.	Unexpected operating results or unusual trends are investigated.	Operating results and trends are not monitored.					
11.6 Accounting statements and key reconciliations.	Accounting statements and key reconciliations are completed timely. Management performs a diligent review and signifies approval by signature and date.	Reconciliations are not performed timely or regularly. Management does not carefully review or formally approve statements or reconciliations.					
11.7 Sponsored project account management.	Sponsored project accounts are reviewed and reconciled. PIs certify the expenditures timely. MWE management monitors the portfolio of sponsored accounts for compliance and fiscal responsibility.	Sponsored project accounts are not monitored; reconciliations and certifications are not timely.					

Assessment Factor	Indication of strong Controls	Indication of weak Controls	Assessment				
Strong - Weak							
			1	**2**	**3**	**4**	**5**
11.8 Use of restricted funds (gifts).	Restrictions on use are well documented, and are understood by employees who administer the funds. Usage is monitored by management, accounts are reconciled.	Restrictions are not clearly documented. Restricted fund accounts are not monitored; usage may not match restrictions.					
11.9 Information processing.	Controls exist to monitor the accuracy and completeness of information as well as authorization of transactions.	No information processing controls are in place.					
11.10 Physical controls.	Equipment, supplies, inventory, cash and other assets are physically secured and periodically counted and compared to the amounts shown on control records.	Equipment, supplies, inventory, cash and other assets are not protected. Control records do not exist or are not up to date.					
11.11 Training and guidance for asset custodians.	Adequate guidance and training are provided to personnel responsible for cash or similar assets.	No training or guidance is provided.					
11.12 Separation of duties.	Financial duties are divided among different people (responsibilities for authorizing transactions, recording them and handling the asset are separated).	No significant separation of financial duties among different employees.					
11.13 Record retention.	MWE employees understand which records they are responsible to maintain and the required retention period. Records are appropriately filed.	MWE employees do not understand which records they are responsible for maintaining. The filing system is inadequate.					
11.14 Disaster response plan.	A disaster response and recovery plan has been developed and is understood by key personnel.	No disaster response or recovery plan exists.					
12 – Controls over Information Systems							
12.1 Local information systems and LANs.	System operations are documented; software is appropriately acquired and maintained; access to the system, programs and data is controlled; the system is maintained in a secure environment; applications are appropriately developed and maintained.	Inadequate controls over local information systems or LANs.					

Assessment Factor	**Indication of strong Controls**	**Indication of weak Controls**	**Assessment**				
Strong - Weak							
			1	**2**	**3**	**4**	**5**
12.2 Application controls.	The MWE controls its computer applications by diligent and timely response to edit lists, rejected transactions and other control and balancing reports. Controls ensure a high level of data integrity including completeness, accuracy, and validity of all information in the system.	Application controls are not used.					
12.3 Back Up.	Key data and programs on LANs or desktop computers are appropriately backed up and maintained. Off-site storage is adequate considering possible risks of loss.	No formal back up procedures exist. Management has not informed staff of back up requirements.					

Assessment Factor	Indication of strong Controls	Indication of weak Controls	Assessment				
Strong - Weak							
			1	**2**	**3**	**4**	**5**
Section 4 – Information and Communication							
13 – Access to Information							
13.1 Relevant external information.	MWE members receive relevant information regarding legislation, regulatory developments, economic changes or other external factors that affect the MWE.	Relevant information is not available.					
13.2 Management reporting system.	An executive information system exists. Information and reports are provided timely. Report detail is appropriate for the level of management. Data is summarized to facilitate decision making.	A formal reporting system does not exist. Reports are not timely or are not at appropriate levels of detail.					
13.3 Management of information security.	Information is evaluated and classified based on level of integrity, confidentiality and availability. Individuals with access to information are trained to understand their responsibilities related to the information.	Information used by the MWE has not been evaluated and classified. Employees are not trained with respect to information security.					
14 – Communication Patterns							
14.1 Trust.	Management promotes and fosters trust between employees, supervisors and other MWEs.	Interactions among department, staff and/or with other MWEs is characterized by low levels of trust.					
14.2 Policy enforcement and discipline.	Employees who violate an important policy are disciplined. Management's communications and actions are consistent with policies.	Violations, while not condoned officially, are often overlooked. Management's actions are inconsistent with official policies.					

Assessment Factor	Indication of strong Controls	Indication of weak Controls	Assessment				
Strong - Weak							
			1	**2**	**3**	**4**	**5**
14.3 Recommendations for improvement.	Employees are encouraged to provide recommendations for improvement. Ideas are recognized and rewarded.	Employees' ideas are not welcomed.					
14.4 Formal communications.	Formal methods are used to communicate MWE policies and procedures (e.g., manuals, training programs, written codes of conduct, and acceptable business practices).	To the extent that they exist, policies are buried in unused manuals and documents.					
14.5 External communications.	Standards and expectations are communicated to key outside groups or individuals (e.g., vendors, consultants, donors, sponsors, subcontractors, sub-recipients).	No external communication of standards and expectations.					
14.6 Informal communications.	Employees are kept informed of important matters (downward communication) and are able to communicate problems to persons with authority (upward communication). There is effective functional coordination within the MWE (lateral communication).	Most information is received by the "grapevine."					
14.7 Communication with evaluators.	Information is openly shared with outside evaluators.	Information is kept secret from outside evaluators.					
Section 5 – Monitoring							
15 – Management Supervision							
15.1 Effectiveness of key control activities.	Management routinely spot-checks transactions, records and reconciliations to ensure expectations are met.	Management never performs spot-checks.					

Assessment Factor	Indication of strong Controls	Indication of weak Controls	Assessment				
Strong - Weak							
			1	**2**	**3**	**4**	**5**
15.2 Management supervision of accounting function.	Accounting policies are defined and adopted after appropriate consideration. Policies are effectively communicated (in writing).	Policies are ad hoc or poorly communicated.					
15.3 Management supervision of new systems development.	Policies are defined for developing new systems or changes to existing systems (cost/benefit analysis, team composition, user specifications, documentation, acceptance testing, and user approval).	Policies and procedures are ad hoc, poorly communicated, or ineffective.					
15.4 Budget analysis.	Budgets are compared to actual results and deviations are followed up on a timely basis. Adequate consideration is given to commitments.	An analysis of actual versus budgeted results is not performed, or management does not follow up on deviations.					
16 – Outside Sources							
16.1 Industry and professional associations.	Data is used to compare the MWE's performance with peers or industry standards.	Comparative data is not regularly monitored.					
16.2 Regulatory authorities.	Reports from regulatory bodies are considered for their internal control implications.	Response is limited to what is necessary to "get by" the regulators.					
16.3 Sponsors, students, suppliers, creditors, and other third parties.	Root causes of inquiries or complaints are investigated and considered for internal control implications.	Inquiries or complaints are dealt with case-by-case, with little or no follow-up.					
16.4 External auditors.	Information provided by external auditors about control-related matters are considered and acted on at high levels.	Findings are referred to lower levels or are explained away.					
17 – Response Mechanisms							
17.1 Management follow-up of violations of policies.	Timely corrective action is taken.	Follow-up is sporadic.					

Assessment Factor	**Indication of strong Controls**	**Indication of weak Controls**	**Assessment**				
Strong - Weak							
			1	**2**	**3**	**4**	**5**
17.2 External or internal audit findings.	Findings are considered and immediately acted upon at appropriate levels.	Consideration of findings is delegated to lower levels or is given low priority.					
17.3 Changes in conditions (e.g., economic, regulatory, technological, or competitive).	Changes are anticipated and routinely integrated into ongoing long- and short-range planning.	Responses are reactive rather than proactive.					
18 – Self-Assessment Mechanisms							
18.1 Monitoring of control environment.	Management periodically assesses employee attitudes, reviews the effectiveness of the organization structure, and evaluates the appropriateness of policies and procedures.	Assessment processes do not exist.					
18.2 Evaluation of risk assessment process.	Management periodically evaluates the effectiveness of its risk assessment process.	Assessment processes do not exist.					
18.3 Assessment of design and effectiveness of internal controls.	Internal controls are subject to a formal and continuous internal assessment process.	Assessment processes do not exist.					
18.4 Evaluation of information and communication systems.	Management periodically evaluates the accuracy, timeliness and relevance of its information and communication systems. Management questions information on management reports that appears unusual or inconsistent.	Assessment process does not exist.					

Republic of Uganda

MINISTRY OF WATER AND ENVIRONMENT

RISK MANAGEMENT FRAMEWORK

2018

Table of contents

Background

Introduction ....
Overall purpose of the Enterprise Risk Management Policy and Framework .... **Error! Bookmark not defined.**
Key definitions 41
Risk 41
Enterprise Risk Management 41
Basic Principles of Governance 42

The purpose of the Enterprise Risk Management (ERM) Framework

Purpose of the ERM framework 43
Benefits of the ERM policy and framework 43
Legal mandate 44
Accounting Officer 44
Management, other personnel and Risk Champions 44
Internal Auditors 44
Audit Committee 45
Enterprise Risk Management Framework Guidelines 45
Corporate governance guidelines 45
Roles, responsibilities and governance 46
Introduction 46
Members of the Top Policy Committee (TPC) 46
Accounting Officer (MWE Permanent Secretary) 46
MWE Risk Committee 47
Management 48
Audit Committee 49
The Audit Committee further: 50
Departmental Heads 50
Chief Risk Officer (CRO) 51
Internal Audit 52
Internal Audit is responsible for: 52
The Auditor-General's Office – External Audit 52
Enterprise Risk Management (ERM) Approach 53
Introduction 53
internal EnvironmenT 53
Objective Setting 53
Risk Identification And Assessment 54
Step One: Identify Risks 54
Purpose 54
Step Two: Identify Existing Controls 59
Step Three: Assess Control Performance and Level of Risk Exposure 60

Step Four: Identifying Risk Treatments 64
1.1 66
1.2 66
1.3 66
Step 6. Identifying Actions to Mitigate Risk Exposure 68
Communication and Reporting 68
Combined Assurance 69
Monitoring 70
Embedding Risk Management 70
Annexure A Integration with strategy 71
Annexure B: Glossary of Terms 72
Annexure C: Project - Risk Management Cheat Sheet 75
Appendix 6: Glossary of Risk Management Terms

List of Abbreviations

AO	Accounting Officer
COSO	Committee of Sponsoring Organizations
CRO	Chief Risk Officer
ERM	Enterprise Risk Management
IT	Information Technology
MWE	Ministry of Water and Environment
PFMA	Public Finance Management Act
SAI	Supreme Audit Institution
TPC	Top Policy Committee

Key definitions

Risk

The Institute of Risk Management defines risk as "*…the uncertainty of an event occurring that could have an impact on the achievement of objectives.* Risk not only manifests as negative impacts on the achievement of goals and objectives, but also as a missed opportunity to enhance organizational performance. Risk is measured in terms of consequences of impact and likelihood."

This definition applies to each and every level of the enterprise and the overriding policy and philosophy is that the management of risk is the responsibility of management at each and every level in MWE. The management of risk is no more or less important than the management of organizational resources and opportunities and it simply forms an integral part of the process of managing those resources and opportunities.

Enterprise Risk Management

Enterprise Risk Management (ERM) is the application of risk management throughout the institution rather than only in selected business areas or disciplines. ERM recognizes that risks (including opportunities) are dynamic, often highly interdependent and ought not to be considered and managed in isolation. ERM responds to this challenge by providing a methodology for managing institution-wide risks in a comprehensive and integrated way.

ERM deals with risks and opportunities affecting value creation or preservation and is defined as follows with reference to COSO (The Committee of Sponsoring Organizations of the Treadway Commission):

"a continuous, proactive and systematic process, effected by an institution's executive authority, executive TPC, accounting authority, accounting officer, management and other personnel, applied in strategic planning and across the institution, designed to identify potential events that may affect the institution, and manage risks to be within its risk tolerance, to provide reasonable assurance regarding the achievement of institution's objectives."

The Public Sector Risk Management Framework guideline provided by the Office of the Accountant General at National Treasury defines risk management as "a systematic process to identify, evaluate and address risks on a continuous basis before such risks can impact negatively on the institutions service delivery capacity. When properly executed risks management provides reasonable, but not absolute assurance, that the institution will be successful in achieving its goals and objectives."

A full glossary of terms is included in Annexure A.

Basic Principles of Governance

First line of defense	**Second line of defense**	**Third line of defense**
Primary risk and control responsibility	Oversight	Independent assurance
Business line management	Risk management	Internal and external audit
● Promotes strong risk culture ● Sets risk appetite; creates risk definitions ● Owner of risk management process ● Implements controls ● Day-to-day risk management by risk takers	● Develops centralised risk management policies and standards ● Develops risk management processes and controls ● Monitors and reports on risk	● Provides independent and objective challenge to the levels of assurance provided by business operations and oversight ● Validates processes in the risk management framework ● External audit gives assurance on the financial Statements

Purpose of the ERM framework

The purpose of the ERM framework is to provide a comprehensive approach to better integrate risk management into strategic decision-making; and

- Provide guidance for the accounting officer, managers and staff when overseeing or implementing the development of processes, systems and techniques for managing risk, which are appropriate to the context of MWE.
- Advance the development and implementation of modern management practices and to support innovation throughout the Public Sector;
- Contribute to building a risk-smart workforce and environment that allows for innovation and responsible risk-taking while ensuring legitimate precautions are taken to protect the public interest, maintain public trust, and ensure due diligence;

It is anticipated that the implementation of the Enterprise Risk Management Framework will:

- Support MWE's governance responsibilities by ensuring that significant risk areas associated with policies, plans, programs and operations are identified and assessed, and that appropriate measures are in place to address unfavorable impacts;
- Improve results through more informed decision-making, by ensuring that values, competencies, tools and the supportive environment form the foundation for innovation and responsible risk- taking, and by encouraging learning from experience;
- Strengthen accountability by demonstrating that levels of risk associated with policies, plans, programs and operations are explicitly understood and that investment in risk management measures and stakeholder interests are optimally balanced; and
- Enhance stewardship and transparency by strengthening MWE's capacity to safeguard human resources, property and interests.

Benefits of the ERM policy and framework

The benefits of the Enterprise Risk Management Policy and Framework are as follows:

- **Aligning risk appetite and strategy** – MWE's management considers their risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.
- **Pursuing institutional objectives through transparent identification and management of acceptable risk –** There is a direct relationship between objectives, which are what MWE strives to achieve and the ERM components, which represent what is needed to achieve the objectives.
- **Providing an ability to priorities the risk management activity –** Risk quantification techniques assist management in prioritizing risks to ensure that resources and capital are focused on high priority risks faced by MWE.
- **Enhancing risk response decisions –** ERM provides the rigor for management to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.
- **Reducing operational surprises and losses –** MWE gains enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.
- **Identifying and managing multiple and cross-enterprise risks** – MWE faces a myriad of risks affecting different parts of MWE and ERM facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.
- **Seizing opportunities** – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.

- **Improving deployment of capital –** Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.
- **Ensuring compliance with laws and regulations –** ERM helps ensure effective reporting and compliance with laws and regulations, and helps avoid damage to MWE reputation and associated consequences.
- **Increasing probability of achieving objectives –** ERM assists management in achieving the organization's performance and profitability targets and prevents loss of resources. Controls and risk interventions will be chosen on the basis that they increase the likelihood that MWE will fulfill its intentions to stakeholders.

Legal mandate

The Public Finance Management Act, 2015 has legislated key governance best practices.

Accounting Officer

Section 45(2) of the Public Finance Management Act, 20015 requires that an Accounting Officer, in respect of all resources and transactions of a vote, to put in place effective systems of risk management, internal control and internal audit.

Management, other personnel and Risk Champions

The accounting officer may delegate the risk management function under Section 45(6) of the Public Finance Management Act 2015 "An Accounting Officer may delegate a function or responsibility of Accounting Officer specified in this Act, to a public officer under the control of the Accounting Officer". This implies that responsibility for risk management vests at all levels of management and that it is not limited to only the accounting officer and internal audit.

Internal Auditors

Section 48(2) (b) and (c) of the Public Finance Management Act 2015 require Internal Auditors to;

(b) Evaluate the effectiveness and contribute to the improvement of risk management processes of a vote; and

(c) Provide assurance on the efficiency, and the effectiveness of the economy in the administration of the programmes and operations of a vote.

Section 48(4) of the same Act states requires an internal auditor to prepare an annual work plan of the activities to be performed by the internal auditor in a financial year which shall be determined by the **fiscal risk** of the vote.

Section 2110 – Risk Management of the International Standards for the Professional Practice of Internal Auditing States:

"The internal audit activity should assist the organization by identifying and evaluating significant exposures to risk and contributing to the improvements of the risk management and control systems –

> *A1 -The internal audit activity should monitor and evaluate the effectiveness of the organization's risk management system.*
>
> *A2 -The internal audit activity should evaluate risk exposures relating to the organization's governance, operations and information systems regarding the:*

- *Reliability and integrity of financial and operational information;*
- *Effectiveness and efficiency of operations;*

- *Safeguarding of assets; and*
- *Compliance with laws, regulations and contracts.*

  C1 -During consulting engagements, internal auditors should address risk consistent with the engagement's objectives and be alert to the existence of other significant risks.

  C2 -Internal auditors should incorporate knowledge of risks gained from consulting engagements into the process of identifying and evaluating significant risk exposures of the organization."

Audit Committee

Section 49 (i) of the Public Finance Management Act, 2015 requires that the Minister to establish an audit committee for each sector of Government and audit committees for a number of votes in local governments.

Section 49(5) (d) requires (d) Audit Committees to facilitate risk assessment to determine the amount of risk exposure of the assets of the vote and the possibility of loss that may occur, with a view to mitigating risks.

Risk Management Framework Guidelines

The Enterprise Risk Management Framework ensures that key risks are identified, measured and managed. The Enterprise Risk Management Framework provides management with proven risk management tools that support their decision-making responsibilities and processes, together with managing risks (threats and opportunities), which impact on the objectives and key value drivers. The ERM is everyone's responsibility and must be embedded into the everyday activities of MWE. This implies that ERM must be part of every decision that is made, every objective that is set and every process that is designed. Detailed ERM responsibilities for key risk management role players are listed below.

Corporate governance guidelines

Institutions are encouraged to adhere to the principles espoused in the King Report on Corporate Governance (King III). King III discusses the following principles, which have been incorporated in this framework:

- Responsibility for the governance of risk;
- The determination of risk tolerance;
- The establishment of a risk committee;
- The responsibility of management to design, implement and monitor the risk management plan;
- The performance on continuous risk assessments;
- The implementation of frameworks and methodologies;
- The implementation of appropriate risk responses by management;
- The implementation of continuous risk monitoring by management; and
- Assurance to be provided on the effectiveness of the risk management process.

Roles, Responsibilities And Governance

Introduction

- The Accounting Officer of is ultimately responsible for ERM and should assume overall ownership.
- All managers and employees have some responsibility for ERM.
- Managers support the risk management philosophy, promote compliance with the risk appetite and manage risks within their spheres of responsibility consistent with risk tolerances.
- Personnel are responsible for executing ERM in accordance with established directives and protocols.
- A number of external parties often provide information useful in effecting ERM, but they are not responsible for the effectiveness of MWE's ERM processes and activities.

Members of the Top Policy Committee (TPC)

TPC is collectively accountable for the achievement of the goals and objectives of MWE. As risk management is an important tool to support the achievement of this goal, it is important that TPC should provide leadership to governance and risk management. TPC may delegate this responsibility to an Executive Committee of the TPC. High level responsibilities of the TPC for risk management include**:**

- Providing ***oversight and direction*** to the institution on the risk management related strategy and policies;
- Having knowledge of the extent to which the institution and management has established effective risk management in their respective institutions and ***assign responsibility and authority***;
- Awareness of and concurring with the institution's ***risk appetite and tolerance levels;***
- Reviewing the institution's ***portfolio view of risks*** and considering it against the risk tolerance;
- ***Influencing*** how ***strategy and objectives*** are established, institutional activities are structured, and risks are identified, assessed and acted upon;
- Requiring that management should have an established set of ***values by which every employee should abide by;***
- Insist on the ***achievement of objectives***, effective performance management, accountability and value for money.
- Consideration of:
  - ✓ The design and functioning of ***control activities***, information and communication systems, and monitoring activities;
  - ✓ The quality and frequency of ***reporting;***
  - ✓ The ***way the institution is managed*** including the type of risks accepted;
  - ✓ The appropriateness of the **reporting lines**.

In addition the TPC should:

- ✓ Assign responsibility and authority;
- ✓ Insist on accountability.

Accounting Officer (MWE Permanent Secretary)

The PFMA 2015 makes it clear that Accounting Officer (AO) is responsible for implementing effective, efficient and transparent systems of risk management within the institutions under their control. The Accounting Officer is therefore accountable for the institution's risk management in terms of legislation. It is important that the AO sets the right tone for risk management in the institution, this will ensure that the institution operates in a conducive control environment where the overall attitude, awareness, and actions of management regarding internal controls and their importance to the institution is at par with the stated vision, values and culture of the institution.

The Accounting Officer is responsible for:

- the ***identification of key risks*** facing their respective institution;
- the total process of risk management, which includes a related system of internal control;
- for forming its own opinion on the effectiveness of the process;
- providing ***monitoring, guidance and direction*** in respect of ERM;
- ascertaining the status of ERM within their respective institution, by discussion with senior management and providing ***oversight*** with regard to ERM by:
  - ✓ Knowing the extent to which management has established effective ERM;
  - ✓ Being aware of and concurring with the set risk appetite;
  - ✓ Reviewing the institution's portfolios view of risk and considering it against respective risk appetite; and
  - ✓ Considering the most significant risks and whether management is responding appropriately
- Identifying and fully appreciating the risk issues and key risk indicators affecting the ability of the institution to achieve its strategic purpose and objectives;
- ensuring that appropriate systems are implemented to manage the identified risks, by measuring the risks in terms of impact and probability, together with proactively managing the mitigating actions to ensure that the institutions assets and reputation are suitably protected;
- ensuring that the institutions ERM mechanisms provides an assessment of the most significant risks relative to strategy and objectives;
- considering input from the internal auditors, external auditors, auditor general, risk committee and subject matter advisors regarding ERM;
- utilizing resources as needed to conduct special investigations and having open and unrestricted communications with internal auditors, external auditors, the auditor general and legal TPC;
- for disclosures in the annual report regarding ERM;
- Provide stakeholder's with assurance that key risks are properly identified, assessed, mitigated and monitored through receiving credible and accurate information regarding the risk management processes. The reports must provide an evaluation of the performance of risk management and internal control;
- Hold management accountable for designing, implementing, monitoring and integrating risk management principles into their day-to-day activities.

Ministry of water and Environment Risk Committee

The MWE Risk Committee is an oversight committee responsible to the Accounting Officer for the monitoring of risk management. It is responsible for assisting the Accounting Officer in addressing its oversight requirements of risk management and evaluating the institution's performance with regard to risk management. Management is accountable to the MWE Risk Committee for *designing, implementing and monitoring* the process of risk management and *integrating it into the day-to-day activities* of the institution. The responsibilities of the Risk Management Committee may include:

- Review the risk management policy and strategy, and recommend for approval by the Accounting Officer;

- Review and assess the integrity of the risk control systems and ensure that the risk policies and strategies are effectively managed;
- Set out the nature, role, responsibility and authority of the risk management / risk officer function within the institution and outline the scope of risk management work;
- Monitor the management of significant risks to the institution, including emerging and prospective impacts;
- Review any legal matters, together with the legal advisor, that could have a significant impact on the institution;
- Review management and internal audit reports detailing the adequacy and overall effectiveness of the institution's risk management function and its implementation by management, and reports on internal control and any recommendations, and confirm that appropriate action has been taken;
- Review risk identification and assessment methodologies to obtain reasonable assurance of the completeness and accuracy of the risk register;
- Review and approve the risk tolerance for the institution;
- Evaluate the effectiveness of mitigating strategies to address the material risks of the Institution;
- Report to the Accounting Officer any material changes to the risk profile of the Institution;
- Review and approve any risk disclosures in the Annual Financial Statements;
- Monitor the reporting of risk by management with particular emphasis on significant risks or exposures and the appropriateness of the steps management has taken to reduce the risk to an acceptable level;
- Monitor progress on action plans developed as part of the risk management process;
- Review reports of significant incidents and major frauds (both potential and actual) including the evaluation of the effectiveness of the response in investigating any loss and preventing future occurrences;
- Significant incidents are defined as any event which results in, or has the potential to result in serious personal injury (to the public, staff or third parties) or serious physical damage to property, plant, equipment, fixtures or stock;
- Significant frauds are defined as any fraud which results in, or has the potential to result in the loss of assets with a value exceeding 10% of the institution' budget allocation;
- Providing feedback to the audit committee on the effectiveness of risk management;
- Develop goals, objectives and key performance indicators for the Committee for approval by the Accounting Officer;
- Develop goals, objectives and key performance indicators to measure the effectiveness of the risk management activity;
- Set out the nature, role, responsibility and authority of the risk management function within the Institution for approval by the Accounting Officer, and oversee the performance of the risk management function;
- Provide proper and timely reports to the Accounting Officer on the state of risk management, together with aspects requiring improvement accompanied by the Committee's recommendations to address such issues.

Senior Management

Management is accountable to the Accounting Officer for designing, implementing and monitoring risk management, and integrating it into the day-to-day activities of the institution. This needs to be done in such a manner as to ensure that risk management becomes a valuable strategic management tool for underpinning the efficacy of service delivery and value for money. Management is responsible for:

- designing an ERM programme in conjunction with the Chief Risk Officer;
- deciding on the manner in which risk mitigation will be embedded into management processes;
- ***inculcating a culture of risk management*** in the institution ;
- providing risk registers and risk management reports to the Chief Risk Officer pertaining to risk and control;
- identifying positive aspects of risk that could evolve into potential opportunities for the institution by viewing risk as an opportunity by applying the risk/reward principle in all decisions impacting upon the institution;
- assigning a manager to every key risk for appropriate mitigating action and determining an action date;
- holds official accountable for their specific risk management responsibilities;
- utilizing available resources to compile, develop and implement plans, procedures and controls within the framework of the institution's Enterprise Risk Management Policy to effectively manage the risks within the institution;
- ensuring that adequate and cost effective risk management structures are in place;
- identifying, evaluating and measuring risks and where possible quantifying and linking each identified risk to key risk indicators;
- developing and implementing risk management plans including:
- actions to optimize risk/ reward profile, maximize reward with risk contained within the approved risk appetite and tolerance limits;
- implementation of cost effective preventative and contingent control measures
- implementation of procedures to ensure adherence to legal and regulatory requirements;
- monitoring of the ERM processes on both a detailed and macro basis by evaluating changes, or potential changes to risk profiles;
- implementing and maintaining adequate internal controls and monitoring the continued effectiveness thereof;
- implementing those measures as recommended by the internal auditors, external auditors and other assurance providers which, in their opinion, will enhance controls at a reasonable cost;
- reporting to the Audit Committee on the risk process and resultant risk/ reward profiles;
- defining the roles, responsibilities and accountabilities at senior management level.

Audit Committee

The Audit Committee is responsible for providing the Accounting Officer with independent counsel, advice and direction in respect of risk management. The stakeholders rely on the Audit Committee for an independent and objective view of the institution's risks and effectiveness of the risk management process. In this way, the Audit Committee provides valuable assurance that stakeholder interests are protected.

The Audit Committee oversees the roles and responsibilities of the Internal Audit team, specifically relating to providing assurance in respect of ERM.

The Audit Committee will be responsible for ***addressing the governance requirements*** of ERM and ***monitoring the institution's performance with ERM activities***. The Audit Committee will meet quarterly and has a defined mandate and terms of reference, which covers the following aspects:

- ✓ Constitution; membership; authority; terms of reference; and Meetings.

The Audit Committee further

- Reviews written reports furnished by the **Risk Management Committee detailing** the adequacy and overall effectiveness of the institutional Risk Committee's function and its implementation by management.
- Review risk philosophy, strategy, policies and processes recommended by the **Risk Management Committee and** consider reports by the **Risk Management Committee** on implementation and communication to ensure incorporation into the culture of the institutions.
- Ensure that risk definitions and contributing factors, together with risk policies, are formally reviewed on an annual basis.
- Review the acceptability of the risk profile in conjunction with the overall risk appetite of the institution, taking into account all risk mitigation factors, including, but not limited to, internal controls, business continuity and disaster recovery planning, etc.
- Ensure compliance with the risk policy and framework.
- Oversee the Fraud Prevention Committees of the institutions to ensure they are operating effectively and to receive periodic reports (quarterly) on their respective activities.
- Reviews the completeness of the risk assessment process implemented by management to ensure that all possible categories of risks, both internal and external to the institution, have been identified during the risk assessment process. This includes an awareness of emerging risks pertaining to the institution.
- Facilitates and monitors the coordination of all assurance activities implemented by the institution.
- Reviews and recommends any risk disclosures in the annual financial statements;
- Provides regular feedback to the Accounting Officer on the effectiveness of the risk management process implemented by the institution.
- Reviews and ensures that the internal audit plans are aligned to the risk profile of the institution.
- Reviews the effectiveness of the internal audit assurance activities and recommends appropriate action to address any shortcomings.
- Departmental Heads
- **Heads of Departments in charge of institutional departments have overall responsibility for managing risks related to their department's objectives and are responsible for:**
- identifying, assessing and responding to risk relative to meeting the department's objectives;
- ensuring that the processes utilized are in compliance with the institution's Enterprise Risk Management policies and that their activities are within the established risk tolerance limits;
- reporting on progress and issues to the institutional Chief Risk Officer;
- complying with Enterprise Risk Management policies and developing techniques tailored to the department's activities;
- applying ERM techniques and methodologies to ensure risks are appropriately identified, assessed, responded to, reported on and monitored;
- ensuring risks are managed on a daily basis; and
- Providing leadership with complete and accurate reports regarding the nature and extent of risks in the department's activities.

Chief Risk Officer (CRO)

The primary responsibility of the CRO is to bring to bear his / her specialist expertise to assist the institution to embed and leverage the benefits of risk management to achieve its stated objectives. The CRO should be accountable to the Accounting Officer for enabling the business to balance risk and reward, and is responsible for coordinating the institution's ERM approach.

- Working with senior management to develop the overall enterprise risk management vision, risk management strategy, risk management policy, as well as risk appetite and tolerance levels for approval by the Accounting Officer;
- undertakes a Gap Analysis of the institution's ERM process at regular intervals;
- performs reviews of the risk management process to improve the existing process;
- facilitates annual risk management assessments and risk assessments for all major changes and incidents, such as accidents, purchases of capital equipment, restructuring of operational processes etc.;
- develops systems to facilitate risk monitoring and risk improvement;
- ensures that all risk categories are included in the assessment;
- ensures that key risk indicators are included in the risk register;
- aligns the risk identification process with the institution's targets and objectives;
- agrees on a system of risk quantification;
- identifies relevant legal and regulatory compliance requirements;
- compiles a consolidated risk register on an annual basis;
- costs and quantifies actual non-compliance incidences and losses incurred and formally reports thereon;
- formally reviews the occupational health, safety and environmental policies and practices;
- consolidates all information pertaining to all risk related functions, processes and activities;
- reviews the Business Continuity Management Plans;
- liaises closely with the Internal Audit to develop a risk based audit plan and management assurance plans,
- benchmarks the performance of the risk management process to the risk management processes adopted by other entities both within Uganda and abroad;
- assists in compiling risk registers for all functional areas at strategic, tactical and operational levels;
- communicates the risk strategy to all management levels and to employees;
- ensures that the necessary risk management documentation is developed in respect of the risk management process;
- communicates with the Audit Committee and the Risk Committee regarding the status of ERM;
- regularly visits functional areas and meets with senior managers to promote embedding risk management into the culture and daily activities of the institution;
- works with institutional leaders to ensure institutional plans and budgets include risk identification and management;
- Compiling the necessary reports to the Risk Management Committee;
- Providing input into the development and subsequent review of the fraud prevention strategy, business continuity plans, occupational health, safety and environmental policies and practices, and disaster management plans.

Internal Audit

Internal Audit is accountable to the Accounting Officer for providing independent assurance regarding the risk management activities of an institution. Hence, Internal Audit is responsible for providing independent assurance that management has identified the institution's risk and has responded effectively. Internal audit may also play an advisory and consulting role to Management regarding risk management matters.

The role of Internal Audit in governance is defined by the Institute of Internal Auditors as follows: "To support the Board and Management in identifying and managing risks and thereby enabling them to manage the organization effectively". This is achieved by:

- ✓ enhancing their understanding of risk management and the underlying concepts;
- ✓ assisting them to implement an effective risk management process, and
- ✓ Providing objective feedback on the quality of organizational controls and performance."

Internal Audit is responsible for:

- Reviewing the risk philosophy of the institution. This includes the risk management policy, risk management strategy, fraud prevention plan, risk management reporting lines, the values that have been developed for the institution;
- Reviewing the appropriateness of the risk tolerance levels set by the institution taking into consideration the risk profile of the institution;
- Providing assurance over the design and functioning of the control environment, information and communication systems and the monitoring systems;
- Providing assurance over the institution's risk identification and assessment process;
- Utilizing the results of the risk assessment to develop long term and current year internal audit plans;
- Providing independent assurance as to whether the risk management strategy, risk management implementation plan and fraud prevention plan have been effectively implemented within the institution;
- Providing independent assurance over the adequacy of the control environment. This includes providing assurance over the effectiveness of the internal controls implemented to mitigate the identified risks.

The Auditor-General's Office – External Audit

The Auditor-General is the Supreme Audit Institution (SAI) of Uganda, responsible for auditing financial statements of national government and local government, and selected public entities.

The Auditor-General is responsible for providing an opinion on:

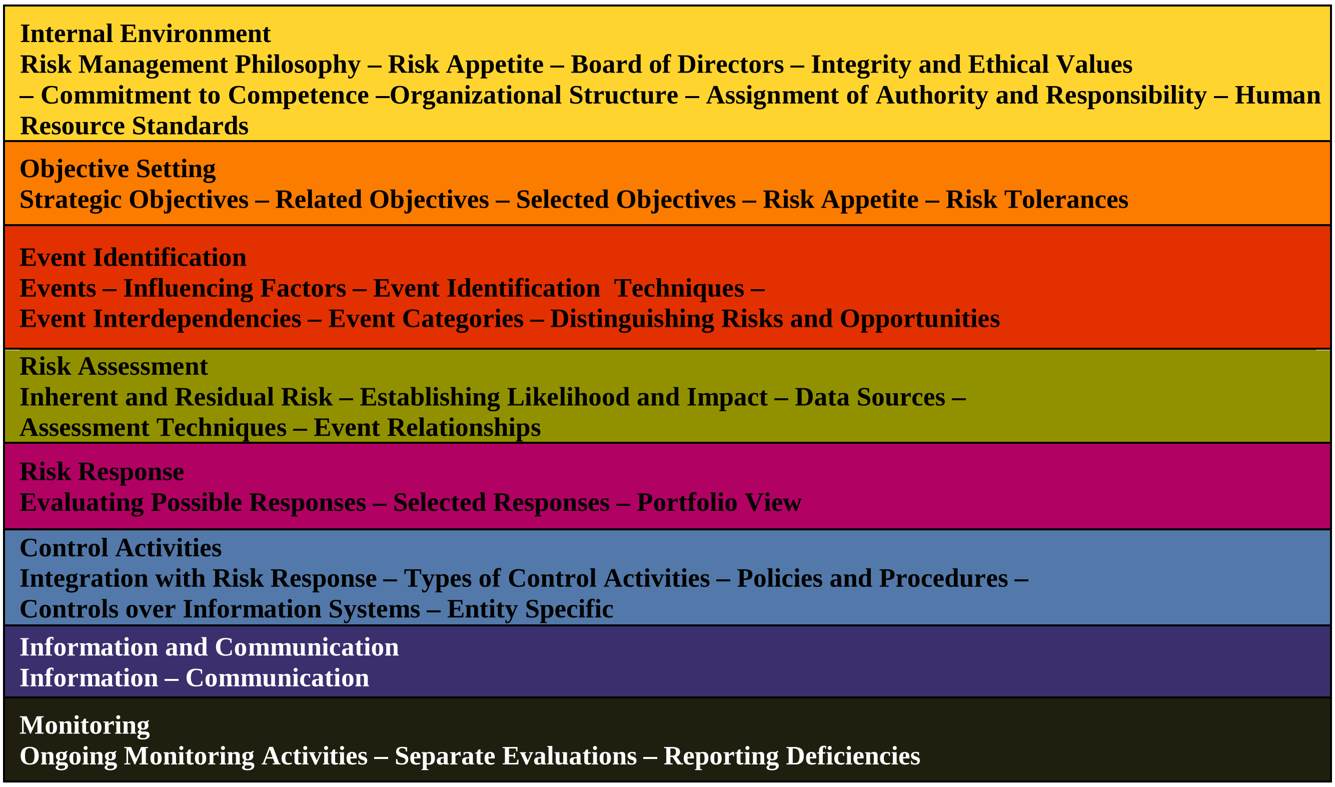
- The reasonability of the financial statements; and
- Compliance with applicable legislation

In addition, the Auditor-General is required to highlight weaknesses or deficiencies in the performance reporting of government institutions. In providing an opinion on compliance with legislation, the Auditor-General will provide independent assurance on the effectiveness of the risk management activities. Within this mandate, the Auditor-General has undertaken to review and comment on the risk management practices within MWE. This framework therefore aims to assist MWE in ensuring that the requirements of the Act are met through the application of effective risk management that is integrated with Internal Audit for the purposes of effective financial reporting and management of risk.

Enterprise Risk Management (ERM) Approach

Introduction

The ERM approach is based on the COSO Risk Management Framework depicted in the diagram below.



Internal Environment
Risk Management Philosophy – Risk Appetite – Board of Directors – Integrity and Ethical Values – Commitment to Competence –Organizational Structure – Assignment of Authority and Responsibility – Human Resource Standards

Objective Setting
Strategic Objectives – Related Objectives – Selected Objectives – Risk Appetite – Risk Tolerances

Event Identification
Events – Influencing Factors – Event Identification Techniques –
Event Interdependencies – Event Categories – Distinguishing Risks and Opportunities

Risk Assessment
Inherent and Residual Risk – Establishing Likelihood and Impact – Data Sources –
Assessment Techniques – Event Relationships

Risk Response
Evaluating Possible Responses – Selected Responses – Portfolio View

Control Activities
Integration with Risk Response – Types of Control Activities – Policies and Procedures –
Controls over Information Systems – Entity Specific

Information and Communication
Information – Communication

Monitoring
Ongoing Monitoring Activities – Separate Evaluations – Reporting Deficiencies

The implementation of enterprise-wide risk management is guided by the methodology outlined in this document. The methodology allows for a consistent approach to be applied by all MWE and MWE entities in the Province and facilitates the interaction, on risk management matters, between the various institutions and functional areas within the institutions.

Internal Environment

The internal environment encompasses the tone of MWE, influencing the risk consciousness of its people, and is the basis for all other components of Risk Management, providing discipline and structure. Internal environment factors include MWE's risk management philosophy; its risk appetite; oversight by the board of directors; the integrity, ethical values, and competence of the entity's people; and the way management assigns authority and responsibility, and organizes and develops its people.

Objective Setting

MWE objectives are set at the strategic level, establishing a basis for operations, reporting, and compliance objectives. MWE faces a variety of risks from external and internal sources, and a precondition to effective event identification, risk assessment, and risk response is establishment of objectives. Objectives are aligned with MWE's risk appetite, which drives risk tolerance levels for the entity.

Objectives should be identified in the following MWE planning documents:

Strategic objectives: The MWE's targets for achieving strategic priorities and direction, as stated in the strategic plan;
Operational objectives: Operational targets for business units to achieve within a planning cycle, as stated in business unit operational plans and annual budget planning; and
Project objectives: Aim or purpose of a project as stated in the project business case and/or plan.

Risk Identification and Assessment

MWE management will identify potential events that, if they occur, will affect MWE objectives, and determine whether they represent opportunities or whether they might adversely affect MWE's ability to successfully implement strategy and achieve objectives. Events with negative impact represent risks, which require management's assessment and response. Events with positive impact represent opportunities, which management will channel back into the strategy and objective-setting processes. When identifying events, management will consider a variety of internal and external factors that may give rise to risks and opportunities, in the context of the full scope of the organization.

The Risk identification and assessment process is broken down into the following 5 steps:

Step 1. Identifying Risk's to the achievement of a MWE objective;

Step 2. Identifying measures that are currently in place to control our exposure to a risk;

Step 3. Providing an assessment of the amount of exposure we face from a risk;

Step 4. Identifying plans to conduct work that will reduce our future exposure to a risk; and

Step 5. Reviewing Risk information so that it is of ongoing benefit to decision making.

Step One: Identify Risks

The first key activity in the risk management process is Risk Identification. Risk identification is the activity that examines each element of MWE to identify associated root causes, begin their documentation, and set the stage for their successful management.

Purpose

- The intent of risk identification is to answer the question "What can go wrong?" by:
- Looking at current and proposed staffing, process, design, supplier, operational employment, resources, dependencies, etc.,
- Monitoring test results especially test failures (readiness results and readiness problems for the sustainment phase),
- Reviewing potential shortfalls against expectations, and
- Analyzing negative trends.

Risks are the effect of uncertainty about how MWE can manage events or changes which have implications on its ability to achieve objectives. MWE may not be able to influence or stop an event or change occurring, but it can dictate how we react to that event or change.
The risk identification process should cover all risks, regardless of whether or not such risks are within the direct control of the institution. These might include external and internal factors:

External Factors	**Economic and**	Related risks might include emerging or movements in the international, national markets and globalizations
	Natural	Risks might include such natural disasters as flood, fire or Earthquake, and sustainable development.
	Political	Risks might include newly elected government officials, political agendas and new legislation and regulations. The influence of international governments and other governing bodies
	Social	Risks might include such natural disasters as flood, fire or Earthquake, and sustainable development.
	Technological	Risks might include evolving electronic commerce, expanded availability of data and reductions in infrastructure costs.
Internal Factors	**Infrastructure**	Risks might include unexpected repair costs, or equipment incapable of supporting production demand.
	Human resource	Risks might include increase in number of on-the-job accidents, increased human error or propensity for fraudulent behaviour.
	Process	Risks might include product quality deficiencies, unexpected downtime, or service delays.
	Technology	Risks might include inability to maintain adequate uptime, handle increased volumes, deliver requisite data integrity, or incorporate needed system modifications. Values and ethics, transparency, policies, procedures and processes
	Governance and accountability	Values and ethics, transparency, policies, procedures and processes

Risk identification should be strengthened by:

- Review of internal and external audit reports;
- Financial analyses;
- Historic data analyses;
- Actual loss data;
- Interrogation of trends in performance data;
- Benchmarking against peer groups;
- Market and sector information;
- Scenario analyses; and
- Forecasting and stress testing

There are a number of techniques that can be used for risk identification. The following options have been identified that can be used to assist role players in identification and recording of perceived risks.

Technique	**Advantages**	**Disadvantages**
Individual Interview	Ensures consistent drawing out of issues. Personal interaction can be useful in generating a better understanding of risks.	Takes up a considerable amount of time for both interviewer and interviewee. May miss significant risks unless a well-qualified interviewer is used.
Workshops	Generates a shared understanding and “ownership”. Promotes team working through a process of brainstorming.	Team dynamics may take over (e.g. risks not identified because the “boss” is present which inhibits discussion). Negativity amongst the team affects risk ranking.
A Combination of the Above	Risks from interviews can be discussed and agreed. New risks can be brought out in a team environment.	Takes up officers’ time and largely depends upon the skills of the interviewer / facilitator.

Staff Surveys	Consistent questions asked and documented responses. Can identify risks, evaluate them and capture action plans.	Could be a better use of resources or be seen as bureaucratic and generate little “buy-in” from teams. Could there be some collation / analysis issues when results received.
Selected Groupings	If senior managers are involved they should quickly identify key strategic risks and the process can help to generate corporate working.	Fairly cost effective but the opinion of those “already converted” or risk educated may be sought which may not adequately capture or address a holistic approach.

Risk Categories

Potential risks are grouped into categories. By aggregating risks horizontally across an organization and vertically within operating units, management develops an understanding of the interrelationships between risks, gaining enhanced information as a basis **for risk assessment.**

Risk Categories	Definition of Risk Categories
1. Strategic and service delivery risks	Risks arising from policy decisions or major decisions affecting national MWE and organizational priorities; Risks arising from senior-level decisions on priorities. Strategy and Business Intelligence failures. Risks that have an effect of hindering service delivery due to inefficient, ineffective and uneconomical use of resources. Risks related to not delivering the appropriate quality of services to the citizens.
2. Intergovernmental and Interdepartmental Co- ordination Risks	Risks emanating from the relationship between the spheres of government in National and Local levels as well as between MWE departments, and are having the effect of impeding the attaining of objectives
3. Governance, Compliance/ Regulatory and Reputational Risks	Values and ethics, transparency, policies, procedures and processes as well organizational structures. Compliance with legal requirements such as legislation, regulations, standards, codes of conduct/practice, contractual requirements and internal policies and procedures. This category also extends to compliance with additional ‘rules’ such as policies, procedures or expectations, which may be set by contracts or customers. The reputation risks exposures due to the conduct of MWE as a whole, the viability of product or service, or the conduct of employees or other individuals associated with the business.
4. Political Risks	Risks relating to newly elected government officials, political agendas and new legislation and regulations or amendments thereof. The influence of international governments and other governing bodies on the institutional strategy. Risks emanating from political factors and decisions that have an impact on the institution’s mandate and operations. Possible factors to consider include: ● Political unrest; ● Local and National elections; and ● Changes in officebearers.
5. Economic Risk	Risks relating to emerging or movements in the international, national markets and globalizations Factors to consider include: ● Inflation; ● Foreign exchange fluctuations; ● Interest rates; and ● Pricing.
6. Environmental Risks	Risks relating to natural disasters as flood, fire or earthquake, and sustainable development.
7. Social Risks	Risks relating to poverty alleviation, changing demographics, shifting of family structures, work/life priorities, social trends, unemployment and the level of citizen engagement.
8. Infrastructure Risks	Risks relating to infrastructure e.g. roads, buildings, etc.

Risk Categories	Definition of Risk Categories
9. Financial Risks	Risks arising from spending on capital projects. Risks from failed resource bids and insufficient resources. Risks encompassing the entire scope of general financial management. Potential factors to consider include: ● Cash flow adequacy and management thereof; ● Financial losses; ● Wasteful expenditure; ● Budget allocations; ● Financial statement integrity; ● Revenue collection; and ● Increasing operational expenditure.
10. Health and Safety/Security Risks	Risks arising from outbreak of diseases and pandemic. Risks that is associated with the safety and security of the communities as well as the execution of institutional mandate. Security of networks, systems and information.
11.Shareholder Risks	Risks associated with shareholding interests that the institution has with its stakeholders. Risks that could have a systemic impact on the sector within which MWE operates and/or on the economy and service delivery.
12.Human Resources	Risks associated with staff capacity in relation to: ● Integrity and honesty; ● Recruitment; ● Skills and competence; ● Employee wellness; ● Employee relations; ● Retention; ● Non-familiarity of staff with the set guidelines and procedures, and ● Occupational health and safety
13.Technological and System Risks	Risks associated with evolving electronic commerce, expanded availability of data and reductions in infrastructure costs. Failure of application system to meet user requirements. Absence of in-built control measures in the application system. Risks relating specifically to the institution's IT objectives, infrastructure requirement, etc. Possible considerations could include the following when identifying applicable risks: ● Security concerns; ● Technology availability (uptime); ● Applicability of ITinfrastructure; ● Integration / interface of the systems; ● Effectiveness of technology; and ● Obsolescence of technology.
14. Process/operational	Ineffective and inefficient processes. Inadequate controls in the operational processes.
15. Project risks	Risks associated with not meeting project scope, costs, duration and deliverables
16. Fraud and Corruption Risks	These risks relate to illegal or improper acts by employees resulting in a loss of the institution's assets or resources.
17. Cultural	Risks relating to an institution's overall culture and control environment. The various factors related to organizational culture include: ● Communication channels and the effectiveness; ● Cultural integration; ● Entrenchment of ethics and values; ● Goal alignment; and ● Management style.

Risk Categories	Definition of Risk Categories
18. Disaster Recovery/Business Continuity	Risks related to an institution's preparedness or absence thereto to disasters that could impact the normal functioning of the institution e.g. natural disasters, act of terrorism etc. This would lead to the disruption of processes and service delivery and could include the possible disruption of operations at the onset of a crisis to the resumption of critical activities. Factors toconsiderinclude: Disaster management procedures; and Contingency planning.
19. Knowledge and information management	Risks relating to an institution's management of knowledge and information. In identifying the risks consider the following aspects related to knowledge management: Availability of information; • Stability of theinformation; • Integrity of informationdata; • Relevance of theinformation; • Retention; and • Safeguarding.
20. Litigation	Risks that the institution might suffer losses due to litigation and lawsuits against it. Losses from litigation can possibly emanate from: • Claims by employees, the public, service providers andother third party; • Failure by institution to exercise certain rights that are to its advantage.
21. Loss / theft of assets	Risks that an institution might suffer losses due to either theft or loss of an asset of the institution.
22. Material resources (Procurement risk)	Risks relating to an institution's material resources. Possible aspects to consider include: • Availability of material; • Costs and means of acquiring / procuring resources; and • The wastage of material resources.
23.Thirdpartyperformance	Risks related to an institution's dependence on the performance of a third party. Risk in this regard could be that there is the likelihood that a service provider might not perform according to the service level agreement entered into with an institution. Nonperformance could include: • Outright failure toperform; • Not rendering the required service in time; • Not rendering the correct service; and • Inadequate / poor quality of performance.
24. Natural environment	Risks relating to the institution's natural environment and its impact on normal operations. Consider factors such as: • Depletion of naturalresources; • Environmental degradation; • Spillage; and • Pollution.

What Are the Risks to Our Objectives?

It is easy for MWE to confuse a Risk's cause or consequence for the risk itself. To reduce this confusion MWE risk management requires to simultaneously establish a risk's cause and consequence's in the process of identifying the risk.
Given staff understanding of an objective, MWE strategy for achieving the objective and stakeholder engagement, they should identify the following:

- What event or change that has the potential to have large implications on MWE's ability to achieve a particular objective?

    - *Generally there is a Risk associated with every event or change you identify that has the potential to have large implications on MWE’s ability to achieve an objective.*
- What is responsible for producing this event or change?
    - *This is the cause of the Risk;*
- What are the consequences of this event or change occurring that MWE wants to avoid?
    - *These are the consequences of the Risk; and*
- What effect does not knowing if MWE can appropriately manage the implications of this event or change, have on MWE’s ability to achieve this objective?
    - *This is the Risk.*

Step Two: Identify Existing Controls
Measures for controlling Risk take two distinct forms, existing controls or risk treatments.

- Existing controls reduce or contain our current exposure to a Risk;
- Risk treatments are potential measures for the future management of risk exposure.
- *Only existing controls reduce or contain how exposed MWE is to a Risk. In order to understand the extent of our vulnerability, existing controls need to be identified and assessed. This is vital information for determining how exposed our objective is, and is essential in identifying which risk treatments will be most beneficial.*
- Existing controls are defined as measures that are in place and actively modifying (reducing or containing) MWE's exposure to the Risk you are associating the control with.
- If a control is in the planning, implementation or testing phase (not fully active), it is not an existing control; and/or
- If a control is active in modifying a related risk, but is not directly involved in actively modifying exposure to the Risk you are associating it with, it is not an existing control on that risk.

Existing controls can include procedures, practices, processes, technology, techniques, methods, or devices that modify MWE’s exposure to a Risk.

Information Required for Describing an Existing Control

Different existing controls may be known by the same name. In order to distinguish the correct control from others, sufficient information needs to be collected to form a unique identifier for each control.
The information used for describing an existing control is as follows:

- Name of the existing control – The title the control in known by;
- Type of existing control – The type of function the control performs (Types of Existing Controls);
- Document reference – A published control’s document name and record reference number;
- Authority over the control – Business area that administers and enforces the control; and
- Responsibility for the control – Position responsible for applying the control to the Risk.

Not all existing controls have published documentation. Published documentation refers to documented guidance that is known by, and readily accessible to, those who are to apply the control.

Types of Existing Controls	
Type	Definition
Policy procedure	Documented procedure under an approved MWE TPC Rule.
Business unit control	Business unit controls are measures that are pre-defined and have procedural reference documentation. NOTE: Business unit controls are measures for the conduct of operations within the set annual business unit budget and staffing allocation.
Ad hoc control	Ad hoc business unit controls are measures that are not pre-defined and have no procedural reference documentation. NOTE: Ad hoc business unit controls are measures for the conduct of operations within the set annual business unit budget and staffing allocation.
Monitoring process	Documented process for monitoring a business activity, during the conduct of that activity. NOTE: Monitoring processes that are defined in the procedures under a Rule or Policy should be identified for control type purposes as a "Monitoring process".
Review process	Documented process for the review of a business activity, after the completion of that activity. NOTE: Review processes that are defined in the procedures under a Rule or Policy should be identified for control type purposes as a "Review process".
Benchmarking	Survey of MWE business activity performance measured against similar assumed or known industry performance.

Step Three: Assess Control Performance and Level of Risk Exposure

The MWE's exposure to a Risk is influenced by the risk's existing controls. A control's purpose is to reduce or contain the most significant aspects of our risk exposure. The most efficient controls manage our exposure to consequences MWE wants to avoid, that arise from a risk occurring.

Rating an Existing Controls Performance

Before assigning a rating to the performance of an existing control, use your knowledge of the control and good judgment to determine:

- Is the existing control appropriate for its purpose in managing this risk?
  - ➢ To determine if a control is appropriate you will need to establish if the control has the capacity to reduce or contain the consequences that MWE wants to avoid, to an amount we think is suitable, given the effort and cost of applying the control.
- How well is the control currently performing it purpose relative to its potential to perform its purpose at MWE?
  - ➢ The input a control receives and the way a control is executed, will influence its maximum potential capacity to function. When assessing how well a control is performing, assess its current performance compared to its maximum capacity to perform within MWE's operating environment.
- Once you have decided how appropriate an existing control is, and you have assessed the controls performance, assign the control a performance rating:

Control Performance Ratings	
Rating	Definition
Effective	The existing control is appropriate for the Risk, and is achieving the majority of its intended capacity to modify exposure to the Risk.
Sound	The existing control is appropriate for the Risk, and is achieving some of its intended capacity to modify exposure to the Risk. NOTE: The existing control has the capacity to perform better. Risk treatments should be targeted at increasing the controls capacity.
Minimal	The existing control is not currently appropriate for the Risk, or is only achieving a small amount of its intended capacity to modify exposure to the Risk. NOTE: The existing control requires alteration to perform better. Risk treatments should be targeted at reengineering the control into a more appropriate controlling measure.
Unsatisfactory	The existing control is inappropriate for the Risk. NOTE: The existing control should be removed from this risk's control environment. Risk treatments should be targeted at replacing the control with more appropriate controlling measures.
Non-existent	No existing controls are in place to modify our exposure to the Risk. NOTE: Used as an assessment of the overall existing control environment only. NOTE: Risk treatments should be targeted at implementing and activating appropriate controlling measures.

Rating the Performance of the Overall Control Environment

The control environment is the accumulative influence of all existing controls on MWE's exposure to a Risk. This singular assessment is used to communicate the status of a Risk's overall control environment for evaluation and reporting purposes.

Using good judgment and your knowledge of the existing controls, assign a single overall control performance rating to the risk's control environment. This control environment performance rating should be based on the performance of the most important or relied on controls, as well as being an average rating of all controls. If there are no identifiable existing controls for a Risk, the control environment is non-existent and receives a rating of "non-existent".

Rating the Likelihood of a Risk Occurring

The likelihood of a Risk reflects the potential frequency of the Risk occurring. To determine the likelihood you need an understanding of what's influencing MWE's exposure to the risk. These influences will come from:

- The predominance of the cause of the Risk.
    - ➢ Is MWE experiencing an increase or decrease in the prevalence of this cause, or is it always present? Does experiencing the cause, always lead to the Risk occurring or only sometimes? and
- The MWE's existing control environment's ability to prevent the Risk occurring.
    - ➢ Do any of the existing controls influence or stop the cause, or the risk, from occurring? How well are these preventative controls performing their purpose?

Assign a likelihood rating to the risk based on the predominance of the risk's cause, and the ability of the risk's control environment to prevent the risk occurring:

Risk Likelihood Ratings	
Rating	**Definition**
Almost Certain	This Risk is being actualised or it is expected to occur in the current control environment: ● Multiple times within a 12 month period; or ● More than 80% of the time.
Likely	In the current control environment the Risk is expected to occur: ● Once within a 12 month period; or ● 61% – 80% of the time.
Possible	In the current control environment the Risk will probably occur: ● Within a 5 year period; or ● 31% – 60% of the time.
Unlikely	In the current control environment the Risk may occur: ● Within a 10 year period; or ● 5% – 30% of the time.
Almost Never	In the current control environment the Risk will only occur in exceptional or unforeseen circumstances.

Rating the Impact of a Risk Occurring

A Risk's impact is the effect on the objective from the consequences, if the Risk occurs. To determine the impact rating you need an understanding of the objective's vulnerability to the effect of the risk's consequences.

- What will experiencing the consequences mean for MWE's ability to achieve the objective?
- Do any of the existing controls soften the blow to the objective, from the consequences of the risk occurring?

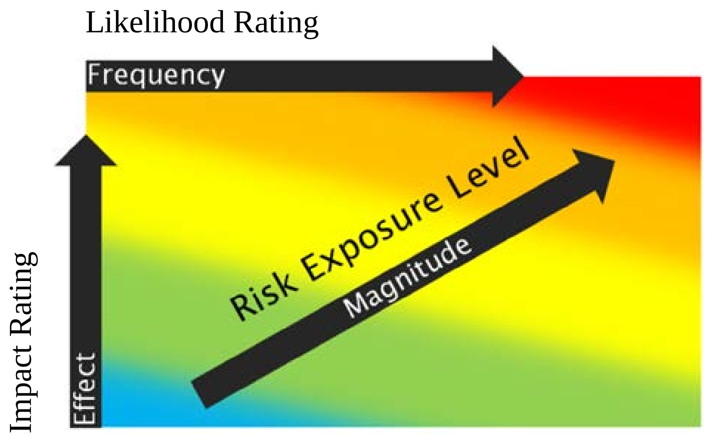
Assign an impact rating to the Risk based on the vulnerability of the objective to the effect of the consequences, and the ability of the existing controls to soften the consequences effect:

Risk Impact Ratings	
Rating	Definition
Severe	The impact from the consequences of the Risk, if they were to occur, would result in the objective being unachievable.
Major	The impact from the consequences of the Risk, if they were to occur, would render a significant proportion, or component, of the objective unachievable.
Moderate	The impact from the consequences of the Risk, if they were to occur, would significantly obstruct our ability to achieve the objective.
Minor	The impact from the consequences of the Risk, if they were to occur, would significantly delay or impair our ability to achieve the objective.
Insignificant	The impact from the consequences of the Risk, if they were to occur, can be managed by MWE so as to not impede the achievement of the objective.

Identify the Level of Risk Exposure Faced by the Objective

The exposure level provides an indicator of a Risk's influence on MWE's ability to achieve its objective. As a risk increases in potential frequency or effect, the magnitude of MWE's exposure to the Risk increases.

Risk Exposure Heat Map



Identify the level of risk exposure an objective faces to a Risk, by plotting the risk's likelihood and impact ratings on the set matrix. The intersection of the likelihood column and impact row indicates the risk exposure level:

Matrix of Risk Exposure Levels

		Likelihood				
		Almost Never	Unlikely	Possible	Likely	Almost Certain
Impact	Severe	High	High	High	Critical	Critical
	Major	Medium	Medium	High	High	Critical
	Moderate	Low	Medium	Medium	High	High
	Minor	Low	Low	Low	Medium	Medium
	Insignificant	Very Low	Very Low	Low	Low	Low

Evaluating Whether the Exposure to a Risk is Acceptable

Whether a Risk is acceptable or unacceptable depends on MWE's perception of its current ability to manage the risk. As a rule accepting the risk means finding the current circumstances acceptable, not accepting the risk indicates MWE needs to improve the current situation.
Factors that affect whether a Risk is deemed acceptable or unacceptable include:

- The Risk appetite approach assigned to achieving the objective being risk assessed;
- The level of risk exposure MWE objective has to the Risk (this is dependent on the performance of the risks control environment); and
- The strategy for achieving the objective, including the influence of operational constraints.

Using good judgment and your knowledge of the objective being risk assessed, provide a Risk evaluation rating for the risk:

Risk Evaluation Ratings	
Rating	Definition
Acceptable	The current level of exposure the objective faces from the Risk is acceptable, or manageable within current standard business operations. • The current level of exposure to the Risk is acceptable in regards to the Risk appetite approach to the objective; or • The MWE has made an educated decision to accept the burden of the current exposure to our objective from the Risk. Risk treatments do not need to be applied to the risk. The control environment should be enforced and monitored, and changes in our exposure to the risk communicated.
Unacceptable	The MWE's ability to achieve its objective is unacceptably exposed to the influence of the Risk. Our current management of the risk needs to be improved. •The current level of exposure the objective faces to the Risk is unacceptable given the Risk appetite approach to the objective; or •The MWE needs to act to reduce our objective's future exposure to the Risk to enable the objective to be achieved. Risk treatments should be applied in line with resource allocation to reduce the objective's future exposure to this risk. Where treatments cannot be applied, a full explanation of why this is the case needs to be provided. The control environment should be enforced and monitored, and changes in our exposure to the risk communicated.

Step Four: Identifying Risk Treatments

Not all Risks need risk treatment. Treatments are proposed measures, undergoing development, implementation, or activation which once in place will reduce or contain our future exposure to a risk. Risk treatments treat deficiencies in MWE's current ability to manage risk, if no changes are needed in our management of risk, no treatments are needed.

Where treatments are needed, they are to be identified, monitored and reported alongside (but separate from) a risk's existing controls. Treatments should be targeted to make the largest possible difference to our risk exposure, given the effort and cost of applying the treatment. A treatment's target should reflect the cause of the Risk, the performance of the risk's existing control environment and MWE's ability to influence both.

Information used to document risk treatments is as follows:

- Name of the risk treatment – The title the treatment in known by;
- Purpose – The purpose of a treatment, and how the treatment is to accomplish this purpose.
- This framework provides rating based indicators for a treatment's purpose (Indicator of Treatments Purpose). Detail on how the treatment will go about changing the control environment, or the cause of a risk, should also be documented;
  - ✓ Approvals – Statement of whether all approvals needed to develop, implement and activate the treatment has been officially provided / received (Indicator of Yes, No or Partially).
- Funding - Statement of whether all funding needed to develop, implement and activate the treatment has been officially allocated to the treatment (Indicator of Yes, No or Partially).
- Due date – The timeframe in which the treatment is expected to be implemented and activated;

- Status-The status of progress towards treatment implementation and activation (Indicator of Treatment Status);
- Authority over the treatment – Business area that is implementing and will activate the treatment; and
- Responsibility for the treatment – Position responsible for aligning the treatment's purpose with reducing our future exposure to the Risk.

Indicator of Treatments Purpose

Indicator	Definition
Enhance *existing controls*	An enhancement to the control environment performance, to further reduce the likelihood or impact of consequences MWE wants to avoid occurring. The prevailing circumstances are such that: • The current level of exposure to this risk is deemed unacceptable; and
	• It is a more efficient use of resources to enhance the Risk's control environment, over changing strategy to avoid the cause of the risk; and • Operational constraints allow for the enhancement of the control environment for this Risk.
Avoid *a cause*	Changing strategy to avoid the cause of the Risk and remove our objectives exposure to the impact of the consequences occurring. The prevailing circumstances are such that: • The current level of exposure to this risk is deemed unacceptable; and • It is a more efficient use of resources to change strategy and avoid the cause of the Risk, over enhancing the risk's control environment; and • Operational constraints will allow for implementation of an alternative strategy to achieving the objective, which avoids the cause of this risk.
Share *the impact from a consequence*	Sharing the burden of the consequences impact with another party or parties (i.e. contract, insurance etc.). The prevailing circumstances are such that: • The current level of exposure to this risk is deemed unacceptable; and • It is a more efficient use of resources to share the burden of the consequences impact, over changing strategy or applying other enhancements to the risk's control environment; and • Operational constraints will allow for Risk sharing to be applied.

Indicator of Treatment Status

Indicator	Definition
Promoted	The treatment is implemented, activated and is modifying our exposure to the Risk.
As Planned	Progress towards implementation and activation of the Risk treatment is on track as planned.
Delayed	There is a delay in implementing or activating the Risk treatment. The delay is being addressed, the treatment is expected to be implemented and activated in full at a

	later time than originally planned.
Off Track	Large setbacks have occurred in the implementation or activation of the Risk treatment; or A significant component of the treatment is not likely to be implemented or activated.
Not Started	As planned, implementation of the Risk treatment has yet to commence.
No Status	No status update has been provided on this Risk treatment.

Promoting a Risk Treatment on Implementation and Activation

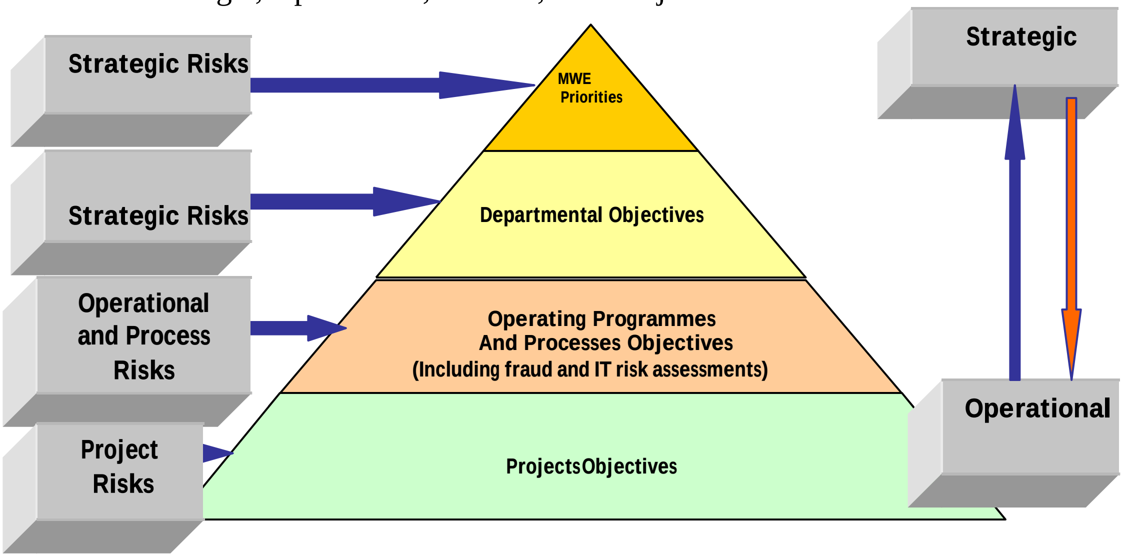
Once an enhancing or sharing treatment has been implemented and is active, it is absorbed into the Risk's existing control environment. Where a treatment's purpose was to improve an existing control, it may increase the existing control's performance rating. If its purpose was to form a new control, the new control is to be added to the risk's existing controls.

Where a treatment's purpose is to avoid the cause of a risk, the treatment could change the Risks faced by MWE. This may mean MWE's objectives are no longer exposed to an original risk, or the consequences of a risk occurring may be significantly different.

Regardless of the purpose of a risk treatment, a treatment's implementation, activation and promotion should prompt a Risk review.

Risk Profiles

Risk profile plans shall be developed and reviewed on an annual basis. Four levels of risk profiles need to be developed and maintained at the institutions (this will also depend on the capacity level within MWE, for example MWE may opt to perform the strategic and operational assessment as a start). These are: Strategic, Operational; Process; and Project.



The development and maintenance of the profiles should be a continuous process but management should formally assess and agree the profiles annually. This is usually achieved through facilitated workshops where management collectively agrees on the risk identification, assessment and actions.

Strategic level (TPC/TPM and Water and Environment Sector Working Group, ENRS-SWG, WSS-SSWG).

- top-down risk assessments at strategic level should be performed when the vision, long-term development priorities and objectives are determined as part of the NDP, Ministerial Development Plan (SDP), Sector Strategic Investment Plan, national Climate Change Policy, National Environment Management Policy, Tree Planting Act, water policy et.

- strategic risk identification should precede the finalization of strategic choices, and related annual budgetary processes, to ensure that potential risk issues are factored into the decision making process for selecting the strategic options;
- in order to achieve this, the strategic risk assessment activities should be aligned to the activities in the IDP process plan and budget timetable and there should be a clear link between the challenges documented in the IDP and the key risks included in the strategic risk profile;
- strategic risk assessment should be updated during the annual review of the Integrated Development Plan and budgetary processes;
- in performing the strategic level risk assessment, risk owners assess the extent to which current management controls and strategies effectively mitigate identified risks to within the risk tolerance and overall risk appetite of the organization;
- Actions are implemented to respond to key gaps in risk mitigation, and monitoring of strategic risks, existing controls and actions should be integrated into day-to-day business.

Operational level (Departmental)

- operational risk identification should seek to establish vulnerabilities introduced by employees, internal processes and systems, contractors, regulatory authorities and external events;
- operational risk assessments should be performed during the annual departmental planning and budgeting processes, and be continually monitored for new and emerging risks;
- specific operational risk assessments may need to be performed in certain areas using specialist skills, such as fraud risk assessments (refer 6.3 below), information technology risk assessments, compliance risk assessments and safety and health risk assessments;
- in performing operational risk assessments, risk owners assess the extent to which current management controls and strategies effectively mitigate identified risks to within the risk tolerances;
- Actions are implemented to respond to gaps in risk mitigation, and monitoring of operational risks, controls and actions should be integrated into operational day-to-day business.

Process level (Divisional Sections, De-concentrated Structures like TSUs, WMZs, WSDFs, Umbrella Organizations etc.

- process risk identification should seek to establish risks to the achievement of the specific process objectives;
- in performing process level risk assessments, risk owners assess the extent to which current management controls and strategies effectively mitigate identified risks to within the risk tolerances;
- Actions are implemented to respond to gaps in risk mitigation, and monitoring of process level risks, controls and actions should be integrated into process level operations.

Project level

- this involves the identification of risks inherent to particular projects;
- risks should be identified for all major projects, covering the whole project lifecycle;
- it is aimed to facilitate risk owners in ensuring that adequate and effective strategies and controls are implemented and monitored throughout the project lifecycle;
- Risks documented in project risk register, monitored and regularly reviewed to identify new and emerging risks.
- Common project risks revolve around (i) risks associated by the contractor due to lack of qualified staff. (ii) risks associated with the consultant in form of late submission of drawings

and response to contractor’s queries, (iii) issues associated by the client in form of late possession of the site, late release of project funds, conflicts associated by land compensation, community sensitization about the project, cultures and norms, (iv) risks associated with natural causes such as rains, floods and landslides.

Step 6. Identifying Actions to Mitigate Risk Exposure

The residual risk gap identifies possible improvement opportunities. Action steps should be identified for the risks where there are residual risk gaps. The actions should specify the responsibilities and due dates. Management should track to progress and completion of the actions.

TIMESCALE FOR ACTION		
Colour-code of risk	**Timescale for action**	**Timescale for review**
Green – insignificant	Action within 12 months or accept risk	Review controls within 12 months
Yellow – minor	Action within 6 months	Review within 9 months
Yellow – moderate	Action within 3 months	Review within 6 months
Red – major	Action within 1 month	Review within 3 months
Red – critical	Action immediately	Review within 1 month

Communication and Reporting

Like any other process, the success of risk management depends on the availability of reliable information and effective communication at various levels. Pertinent information should be identified, captured and communicated in a form and time frame that enable people to carry out their responsibilities. Information is needed at all levels to identify, assess and respond to risks. The challenge for management is to process and refine large volumes of data into relevant and actionable information. Risk information is to be maintained on a risk management database by the Risk Officer. Line management will be responsible for ensuring that the risk information is complete, accurate and relevant. The database will allow the access to the risk officials and line management to execute the relevant functions. The database structure is based on the institution risk profiles, as follows:

- Strategic
- Operational (Including Fraud and Corruption and IT)
- Project specific (where there are such projects)

Additional assessments can be maintained – for example incident tracking and compliance assessments. For each profile the following minimum information is to be maintained on the database:

- Strategic and business objectives
- Risk category
- Risk name
- Risk description (including root cause and consequence)
- Risk owner
- Inherent risk rating
- Risk Indicator
- Control names for controls that mitigate the risk
- Control descriptions (including whether it is a preventative, detective or corrective control)
- Control effectiveness rating
- Residual risk ratings
- Task information where identified – details, due dates and the accountable officials.
- Key Performance Indicator

The databases will be used to extract the required reports to evidence the status of risk management at MWE.

Combined Assurance

Internal Audit is required by the PFMA 2015 to plan the audit coverage to address the risks identified through the risk management processes developed and maintained by management.

It is therefore imperative that the risk assessment process and the internal audit planning process be aligned so that timely and relevant risk information is available to internal audit when they are devising their audit coverage plans. The risks identified cannot all be reviewed by Internal Audit. Some risks, for example reputation, are not able to be reviewed and others, such as technical construction, cannot reasonably be expected to be reviewed by Internal Audit. There are several assurance functions that may exist in an institution at any time and include:

- The Office of the Auditor General,
- Internal Audit,
- Consulting engineers,
- Ethics' specialists,
- Compliance and Legal specialists,
- Culture and climate surveys,
- Health and safety inspectors,
- Information security,
- Quality,
- Loss Control Units, and
- Monitoring and evaluation Units

The assurance that they provide is reported to different management structures and this may be outside the Internal Audit governance reporting structures, including the Audit Committees. Internal Audit takes the responsibility to ensure the assurance activities are coordinated, provide optimal coverage of the risk profiles, where possible, and are reported to the appropriate management and governance forum. The Audit Committee approves the overall/combined assurance plan and extent of assurance coverage. They will also review the appropriateness of the recipients of the different assurance activities. Each assurance provider should develop their coverage plan based on the risk profiles of the institution(s). Typically the plan should consider the risk assessment ratings. Where management has assessed that there is a high residual risk gap and has actions to address the gap, the assurance provider should consider reviewing the actions rather than confirming management's assessment. Conversely where there is a low or negligible gap the controls that have been assessed by management as mitigating the risk should be evaluated.

The results of the work performed should be used by the chief risk officer to facilitate, if necessary, a rerating of the risk and incorporating the agreed management actions into the risk management tasks. This will enable a central tracking capability for all such tasks and actions. Where their work is in response to an incident or event, e.g. loss control, the results of the work performed should be used by the chief risk officer to facilitate, if necessary, a rerating of the risk and incorporating the agreed management actions into the risk management tasks.

Monitoring

If existing controls are weak and exposes the organization's activities to risks, the management should come up with the action plans to reduce risk to an acceptable level. Management should decide on the implementation date of the agreed upon action plan and the responsibility for the implementation of action plan should be assigned to capable officials. It is critical that management should develop key performance indicators regarding the performance of agreed upon controls. Key performance indicators will provide the feedback regarding effectiveness of controls against identified risks.
Management's performance with the processes of ERM will be measured and monitored through the following performance management activities:

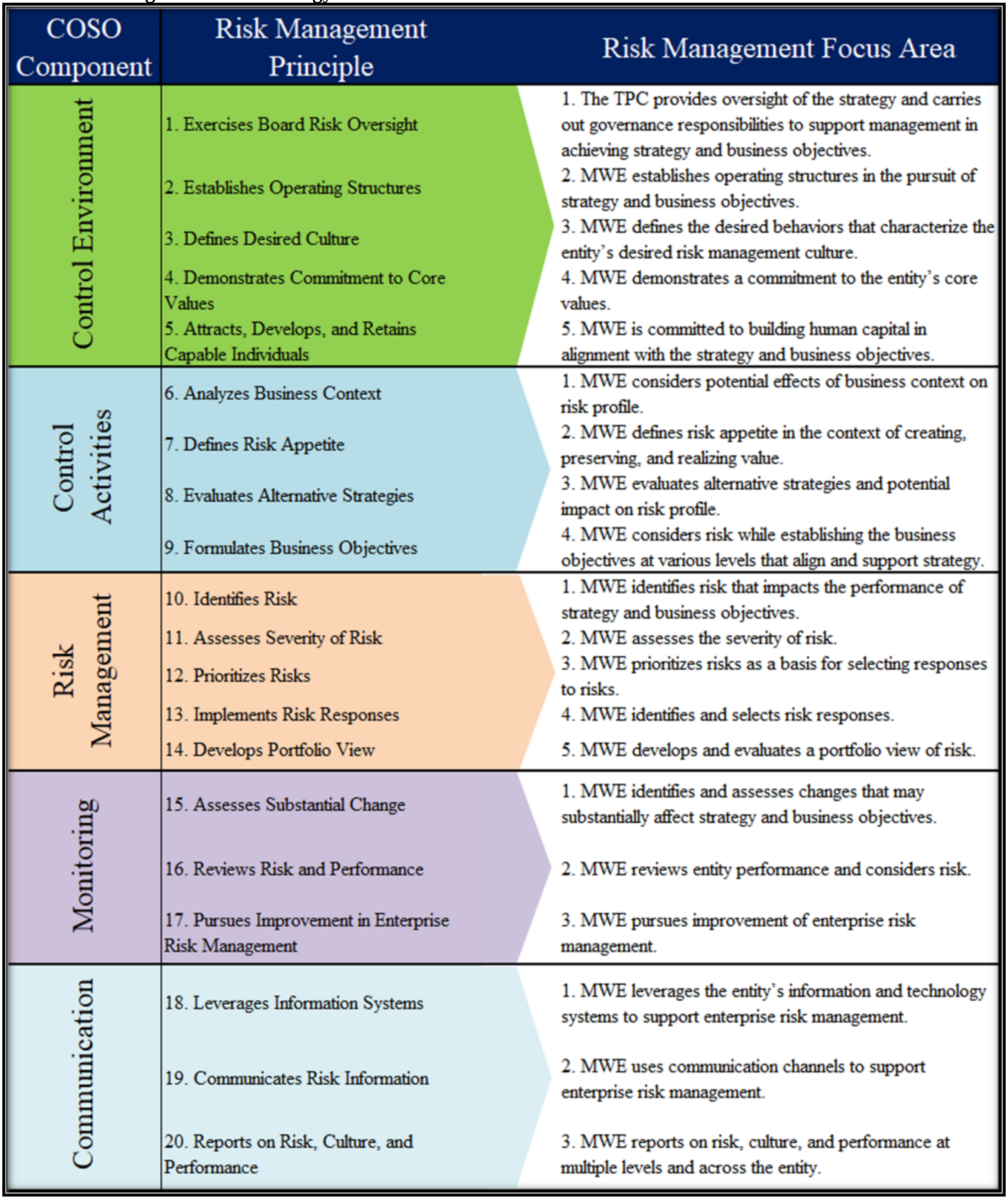
- monitoring of progress made by management with the implementation of the ERM methodology;
- monitoring of key risk indicators;
- monitoring of loss and incident data;
- management's progress made with risk mitigation action plans; and
- an annual quality assurance review of ERM performance.

Embedding Risk Management

Value is created, preserved or eroded by management decisions ranging from strategic planning to daily operations of the institution. Inherent in decisions is the recognition of risk and opportunity, requiring that management consider information about the internal and external environment deploys precious resources and appropriately adjusts institution activities to changing circumstances. For governmental institutions, value is realized when constituents recognize receipt of valued services at an acceptable cost. Risk management facilitates management's ability to both create sustainable value and communicate the value created to stakeholders. The following factors require consideration when integrating ERM into institutional decision making structures:

- Aligning risk management with objectives at all levels of the institution;
- Introducing risk management components into existing strategic planning and operational practices;
- Communicating institutional directions on an acceptable level of risk;
- Including risk management as part of employees' performance appraisals and Business Units' annual operational plans; and
- Continuously improving control and accountability systems and processes to take into account risk management and its results.

Annexure 1 Integration with Strategy



COSO Component	Risk Management Principle	Risk Management Focus Area
Control Environment	1. Exercises Board Risk Oversight	1. The TPC provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.
	2. Establishes Operating Structures	2. MWE establishes operating structures in the pursuit of strategy and business objectives.
	3. Defines Desired Culture	3. MWE defines the desired behaviors that characterize the entity's desired risk management culture.
	4. Demonstrates Commitment to Core Values	4. MWE demonstrates a commitment to the entity's core values.
	5. Attracts, Develops, and Retains Capable Individuals	5. MWE is committed to building human capital in alignment with the strategy and business objectives.
Control Activities	6. Analyzes Business Context	1. MWE considers potential effects of business context on risk profile.
	7. Defines Risk Appetite	2. MWE defines risk appetite in the context of creating, preserving, and realizing value.
	8. Evaluates Alternative Strategies	3. MWE evaluates alternative strategies and potential impact on risk profile.
	9. Formulates Business Objectives	4. MWE considers risk while establishing the business objectives at various levels that align and support strategy.
Risk Management	10. Identifies Risk	1. MWE identifies risk that impacts the performance of strategy and business objectives.
	11. Assesses Severity of Risk	2. MWE assesses the severity of risk.
	12. Prioritizes Risks	3. MWE prioritizes risks as a basis for selecting responses to risks.
	13. Implements Risk Responses	4. MWE identifies and selects risk responses.
	14. Develops Portfolio View	5. MWE develops and evaluates a portfolio view of risk.
Monitoring	15. Assesses Substantial Change	1. MWE identifies and assesses changes that may substantially affect strategy and business objectives.
	16. Reviews Risk and Performance	2. MWE reviews entity performance and considers risk.
	17. Pursues Improvement in Enterprise Risk Management	3. MWE pursues improvement of enterprise risk management.
Communication	18. Leverages Information Systems	1. MWE leverages the entity's information and technology systems to support enterprise risk management.
	19. Communicates Risk Information	2. MWE uses communication channels to support enterprise risk management.
	20. Reports on Risk, Culture, and Performance	3. MWE reports on risk, culture, and performance at multiple levels and across the entity.

Annexure 2: Glossary of Terms

Basic Terms	Definition
General Terminology	
Risk	Combination of the **probability** of an **event** and its **consequence** Note 1: Risk is a condition in which the possibility of loss exists Note 2: deviation from the expected outcome or event Note 3: Risk arises as much from failing to capture business opportunities when pursuing strategic and operational objectives as it does from a threat that something bad will happen.
Consequence or Impact or Severity	Outcome of an **event** Note 1: There can be more than one consequence from one event Note 2: Note 3: Consequences can be expressed qualitatively or quantitatively
Probability	Extent to which the **event** is likely to occur Note 1: Frequency (the probability of an event occurring at intervals) rather than the probability (the relative likelihood of an event happening) may be used in describing risk Note 2:Degrees of believe about probability can be chosen as classes or ranks, such as rare/unlikely/moderate/likely/ almost certain, /improbable/remote/occasional/ probable/frequent
Event	Occurrence of a particular set of circumstances Note 1: Note 2: The event can be a single occurrence or a series of occurrences Note 3: The **probability** associated with the event can be estimated for a given period of time.
Source/Cause	Item or activity having a potential for a **consequence**
Risk Criteria	Terms of reference by which the significance of **risk** is assessed. Note : Risk criteria can include associated cost and benefits, legal and statutory requirements, socio economic and environmental aspects, the concern of stakeholders, priorities and other inputs to the assessment
Risk Management	Set of elements of an organization's management system concerned with managing **risk** Note 1: Management system elements can include strategic planning, decision making and other processes for dealing with risks Note 2: The culture of an organization is reflected in its risk management system.
<u>Terms Related to People or Organization Affected by Risk</u>	
Stakeholder	Any individual, group or organization that can affect, be affected by, or perceive itself to be affected by a **risk** Note 1: The decision maker is also a stakeholder
Cost of risk	Costs associated with: • Insurance premiums • Self-retained losses (incurred loss) • Loss control expenses including safety, security, property conservation, quality control programs, etc. • Administrative costs (internal and external) including risk management department, internal claims staff, fees paid to brokers, risk management consultants, outside claims and loss control services, including your time as risk manager and claims administrator
Interested Party	Person or group having an interest in the performance or success of an organization. Example: Customers, owners, people in an organization, suppliers, bankers, unions, partners or society Regulators and Government are particularly interested in terms of the requirements of the Public Finance Management Act (PFMA 2015). The Accounting Officer's duties in terms of the PFMA 2015 (and other Acts / Regulations as amended from time to time) are specifically noteworthy. Note : A group can comprise an organization, a part thereof, or more than one organization

Basic Terms	Definition
Risk Perception	Way in which a stakeholder views a risk based on a set of values or concerns Note 1: Risk perception depends on the **stakeholder's** needs, issues and knowledge Note 2: Risk perception can differ from objective data
Risk Communication	Exchange or sharing of information about **risk** between the decision- maker and other **stakeholders** Note : The information can relate to the existence, nature, form, probability, severity, acceptability, treatment or other aspects of risk
Terms Related to Risk Assessment	
Risk Assessment	Overall process of **risk analysis** and **risk evaluation** in order to identify potential opportunities or minimize loss. Note: Risk assessment can be of a speculative nature (i.e. opportunity cost, poor operational efficiency, social impact on MWE etc.) as well as pure perils (loss of assets, revenue etc.).
Risk Analysis	Systematic use of information to identify **sources** and to estimate the **risk** Note1: Risk analysis provides a basis for **risk evaluation, risk treatment** and **risk acceptance.** Note 2: Information can include historical data, theoretical analysis, informed opinions, and the concerns of **stakeholders**
Risk Identification	Process to find, list and characterize elements of **risk** Note 1: Elements can include source or hazard, event, consequence and probability Note 2: Risk identification can also reflect the concerns of stakeholders
Source Identification	Process to find, list and characterize **sources** Note : In the context of safety, source identification is called hazard identification
Risk Driver	The technical, programmatic and supportability facets of risk.
Risk Estimation	Process used to assign values to the **probability** and **consequences** of a **risk** Note : Risk estimation can consider cost, benefits, the concerns of **stakeholders** and other variables, as appropriate for **risk evaluation**
Risk Evaluation	Process of comparing the estimated **risk** against given **risk criteria** to determine the significance of the risk Note 1: Risk evaluation may be used to assist in the decision to accept or to treat a risk.
Terms Related to Risk Treatment and Control	
Risk Treatment	Process of selection and implementation of measures to modify **risk** Note 1: The term "risk treatment" is sometimes used for the measures themselves Note 2: Risk treatment measures can include avoiding, optimizing, transferring or retaining risk.
Risk Control	Actions implementing **risk management** decisions Note : Risk control may involve monitoring, re-evaluation, and compliance with decisions
Risk Optimization	Process, related to a **risk** to minimize the negative and to maximize the positive **consequences** and their respective **probabilities** Note 1: In the context of safety, risk optimization is focused on reducing the risk. Note 2: Risk optimization depends upon **risk criteria**, including costs and legal requirements. Note 3: Risks associated with **risk control** can be considered
Risk Reduction	Actions taken to lessen the **probability of** negative **consequences** or both, associated with a **risk**
Mitigation	Limitation of any negative **consequence** of a particular **event**
Risk Avoidance	Decision not to become involved in, or action to withdraw from, a risk situation Note: The decision may be taken based on the result of **risk evaluation**
Risk Transfer	Sharing with another party the burden of loss or benefit of gain, for a **risk** Note 1: Legal or statutory requirements can limit, prohibit or mandate the transfer of certain risk Note 2: Risk transfer can be carried out through insurance or other agreements Note 3: Risk transfer can create new risks or modify existing risk Note 4:

Basic Terms	Definition
Risk Financing	Provision of funds to meet the cost of implementing **risk treatment** and related costs Note: In some industries, risk financing refers to funding only the financial consequences related to the **risk**
Risk Retention	Acceptance of the burden of loss, or benefit of gain, from a particular **risk** Note 1: Risk retention includes the acceptance of risks that have not been identified Note 2: Risk retention does not include treatments involving insurance, or transfer by other means. Note 3: There can be variability in the degree of acceptance and dependence on **risk criteria**
Risk Acceptance	Decision to accept a **risk** Note 1: The verb "to accept" is chosen to convey the idea that acceptance has its basic dictionary meaning Note 2: Risk acceptance depends on **risk criteria**
Residual Risk	The level of **Risk** remaining after **risk treatment**
Inherent Risk	The risk to an organization in the absence of any management might take to alter either the risk probability or impact
Chief Risk Officer (CRO) / Process Owner	An official of MWE who has no *other* responsibilities except for advising on, formulating, overseeing and managing all aspects of an organization's **risk management system** and monitors the organization's entire risk profile, ensuring that major risks are identified and reported upwards. The CRO provides and maintains the risk management infrastructure to assist the TPC in fulfilling its responsibilities.
Process Champion	A senior executive within MWE who will lend support to the process and ensure senior managements buy-in. The risk process champion ensures that the **CRO** is provided with the necessary resources, capabilities and authority in order to fulfil the requirements of the Risk Management Framework.
Risk Officers/Champions	The risk officers assist the **CRO** in the fulfilment of their duties. These persons can be in line management in the departments but have an alternative reporting line to the **CRO** or report directly to the **CRO**.
Risk Matrix	The numbers of levels of probability and consequences chosen against which to measure risk.
Risk Profile	MWE has an **inherent** and **residual** risk profile. These are all the risks faced by MWE, ranked according to a **risk matrix** and indicated graphically on a matrix. The Risk Score is determined by multiplying the frequency and severity of the risk.
Risk Appetite	The level of **residual risk** that the organization is prepared to accept without further **mitigation** action being put in place, or the amount of risk an organization is willing to accept in pursuit of value Note: An organization's risk appetite will vary from risk to risk
Risk Register	A formal listing of risks identified, together with the results of the **risk analysis, risk evaluation** procedures together with details of **risk treatment, risk control, risk reduction** plans
Key Risks	Risks which the organization perceives to be its most significant risks
Key Risk Indicators	Indicators by which key risks can be easily identified
Risk Tracking	The monitoring of key risks over time to determine whether the level of risk is changing.

Annexure 3: Project - Risk Management Cheat Sheet

1. Project Objectives - Reasons for Conducting the Project

- What is the projects purpose?
- Why is it being undertaken? and
- What are the core outputs, benefits or changes the project has been instigated to achieve?

This information forms the projects objectives which you will then risk assess.

2. Risk Appetite towards Each Project Objective

For each project objective, discern whether the objective is:

- Required to achieve a MWE strategic objective or enable continued MWE business as normal ~ Risk averse
- Required to achieve more sustainable MWE operations ~ Balanced
- Required to create a competitive advantage for MWE ~ Positive risk taking

In discussion with the Project Owner and using good judgement, set the appetite for each project objective.

3. Project Constraints and Management Strategies

- What are the constraints the project faces?
- What events or changes can you expect with some certainty will occur during the life of the project?
- What strategies are going to be used to manage achieving the objectives within or around the identified constraints, events or changes?

Knowing the projects constraints and management strategies is essential for identifying risks to the objectives.

4. Risks to the Project Objectives

Risks are the implications of our choices regarding the Projects strategy and management. The risks you are identifying, are the risks of not making the best management choice for achieving the projects objectives.

- What is the constraint, or what is responsible for producing the event/change (cause)?
- What are the specific consequences of the constraint/change that MWE wants to avoid (consequence)?
- What do you have to watch out for
- What effect does not making the best choice for managing or avoiding the consequences of this cause, have on MWE's ability to achieve the project objective (Risk)?

5. Existing Controls for Managing Risk Exposure

- What controls are already in place to manage this risk generally at MWE?
- Are any of these controls being applied to this project? If so these are the existing controls for this project risk.
- How are the controls performing collectively, as a control environment, to manage this risk?

6. Identify the Risk Exposure

Risk Likelihood Rating + Risk Impact Rating = Risk Exposure Level

Is this exposure level acceptable, given the risk appetite and importance of the objective?

Yes: accept the level of Risk to the objective. Monitor existing controls and review risk as needed.

No: apply risk treatments if they are available. Monitor existing controls and review risk as needed.

- Treatments for the Control Environment
- Identify treatments to the risks control environment based on deficiencies in that control environment.
- Indicate the purpose of each treatment & how each treatment will accomplish its purpose.
- Monitor the treatments progress towards implementation and activation.

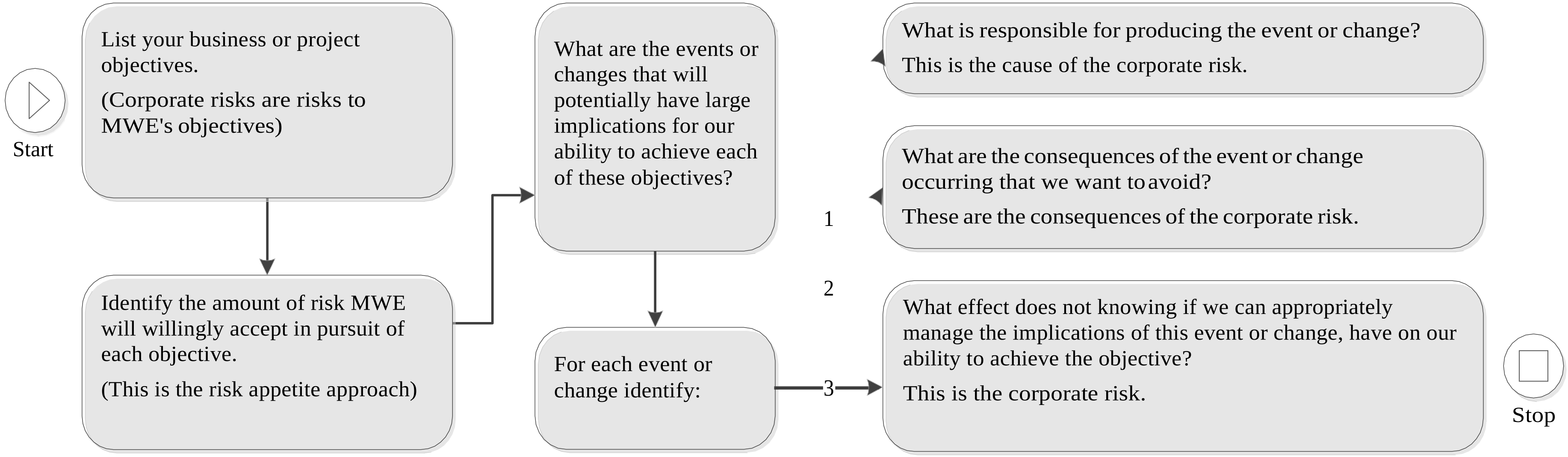
7. Communicate the Risk

- Project Owner & Steering Committee
- Project Control Board
- MWE TPC Committee's (High & Critical Risks)
- Review the Risk Register
  - ✓ Reviews are prompted by:
  - ✓ Changes to the risk, the risks control environment, or finalisation of a risk treatment;
  - ✓ Changes to the project objectives;
  - ✓ Reaching major decision/authorisation points or stage gates within a projects life.

Annexure 4: Corporate Risk Identification and Assessment Process Map

Step One: Identifying Business Risks

In identifying corporate risks, you identify the effects of our uncertainty around how to manage events or changes with potentially large implications, on our ability to achieve objectives.



List your business or project objectives.

(Corporate risks are risks to MWE's objectives)

Identify the amount of risk MWE will willingly accept in pursuit of each objective.

(This is the risk appetite approach)

What are the events or changes that will potentially have large implications for our ability to achieve each of these objectives?

For each event or change identify:

What is responsible for producing the event or change?

This is the cause of the corporate risk.

What are the consequences of the event or change occurring that we want to avoid?

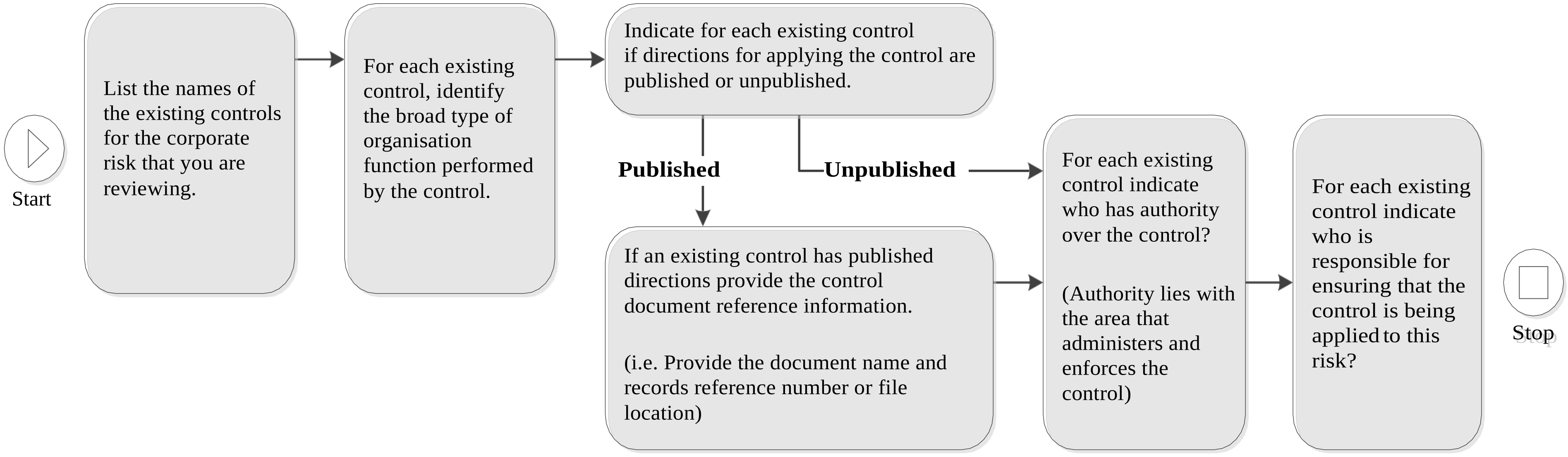
These are the consequences of the corporate risk.

What effect does not knowing if we can appropriately manage the implications of this event or change, have on our ability to achieve the objective?

This is the corporate risk.

Step Two: Identify Existing Controls

In identifying existing controls you are recording the measures or processes that are in place and that are actively modifying our exposure to the corporate risk.



List the names of the existing controls for the corporate risk that you are reviewing.

For each existing control, identify the broad type of organisation function performed by the control.

Indicate for each existing control if directions for applying the control are published or unpublished.

If an existing control has published directions provide the control document reference information.

(i.e. Provide the document name and records reference number or file location)

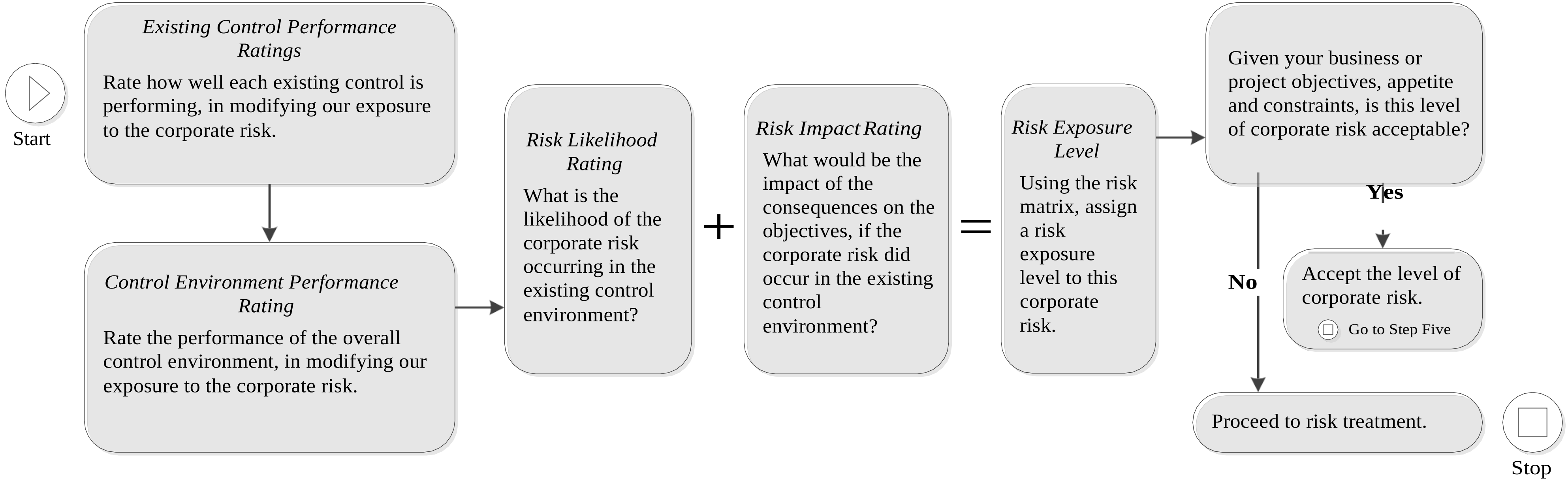
For each existing control indicate who has authority over the control?

(Authority lies with the area that administers and enforces the control)

For each existing control indicate who is responsible for ensuring that the control is being applied to this risk?

Step Three: Assess Control Performance and Level of Corporate Risk Exposure

In assessing control performance and risk ratings you provide an indicator of how significantly the achievement of our objective is exposed to a corporate risk.



Existing Control Performance Ratings

Rate how well each existing control is performing, in modifying our exposure to the corporate risk.

Control Environment Performance Rating

Rate the performance of the overall control environment, in modifying our exposure to the corporate risk.

Risk Likelihood Rating

What is the likelihood of the corporate risk occurring in the existing control environment?

Risk Impact Rating

What would be the impact of the consequences on the objectives, if the corporate risk did occur in the existing control environment?

Risk Exposure Level

Using the risk matrix, assign a risk exposure level to this corporate risk.

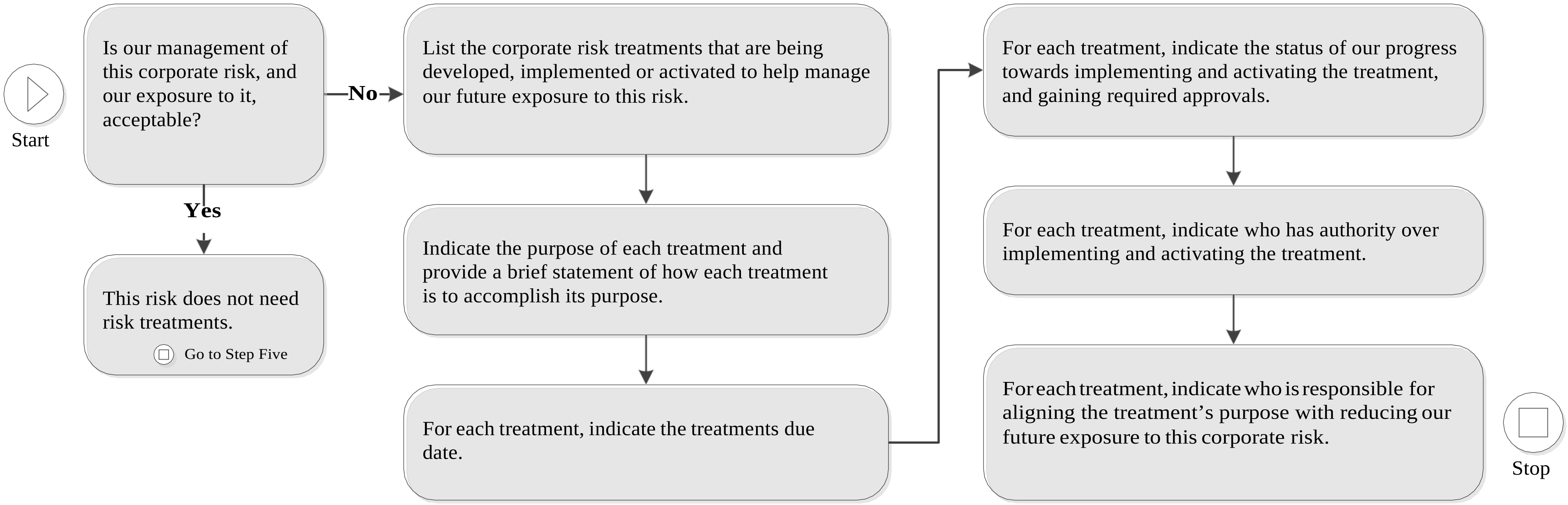
Given your business or project objectives, appetite and constraints, is this level of corporate risk acceptable?

Accept the level of corporate risk.

Proceed to risk treatment.

Step Four: Identifying Corporate Risk Treatments

Corporate risk treatments are proposed measures that will reduce our future exposure to a corporate risk by treating deficiencies in MWE’s current ability to manage the risk.



Is our management of this corporate risk, and our exposure to it, acceptable?

This risk does not need risk treatments.

List the corporate risk treatments that are being developed, implemented or activated to help manage our future exposure to this risk.

Indicate the purpose of each treatment and provide a brief statement of how each treatment is to accomplish its purpose.

For each treatment, indicate the treatments due date.

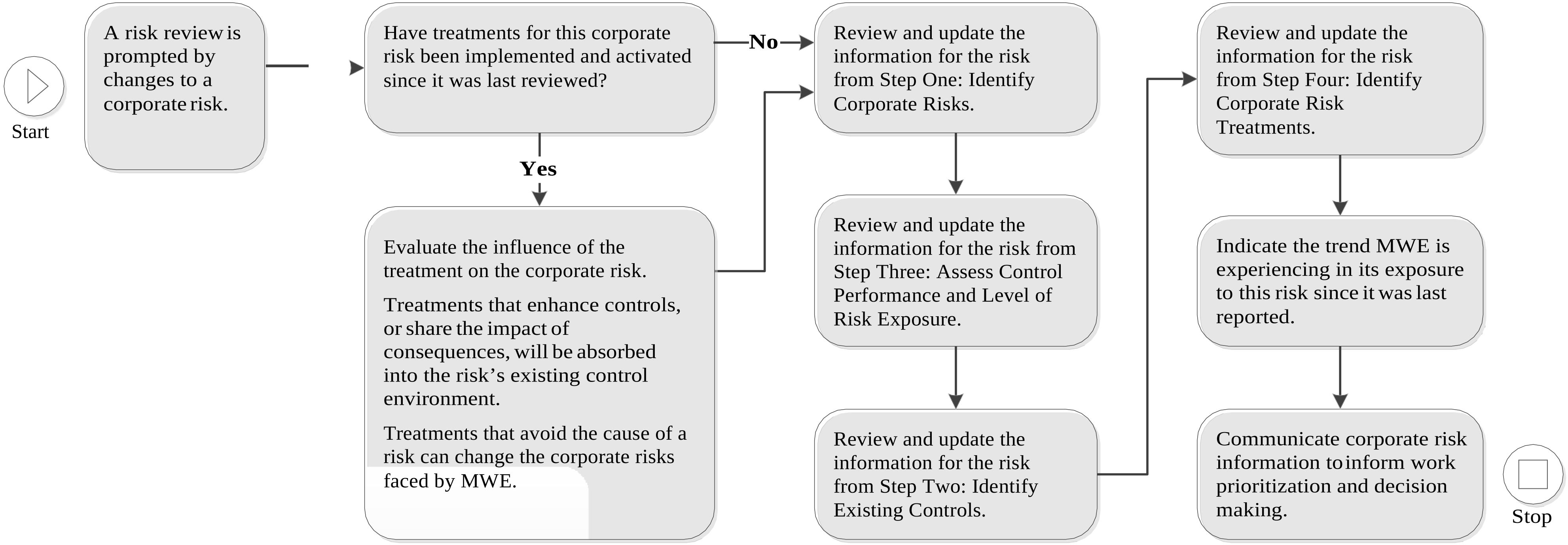
For each treatment, indicate the status of our progress towards implementing and activating the treatment, and gaining required approvals.

For each treatment, indicate who has authority over implementing and activating the treatment.

For each treatment, indicate who is responsible for aligning the treatment’s purpose with reducing our future exposure to this corporate risk.

Step Five: Review Corporate Risk Information and Exposure

Corporate risk reviews update risk information so it can be communicated in an effective manner and considered in organisational decision making.



Start
A risk review is prompted by changes to a corporate risk.
Have treatments for this corporate risk been implemented and activated since it was last reviewed?
No
Yes
Evaluate the influence of the treatment on the corporate risk.
Treatments that enhance controls, or share the impact of consequences, will be absorbed into the risk’s existing control environment.
Treatments that avoid the cause of a risk can change the corporate risks faced by MWE.
Review and update the information for the risk from Step One: Identify Corporate Risks.
Review and update the information for the risk from Step Three: Assess Control Performance and Level of Risk Exposure.
Review and update the information for the risk from Step Two: Identify Existing Controls.
Review and update the information for the risk from Step Four: Identify Corporate Risk Treatments.
Indicate the trend MWE is experiencing in its exposure to this risk since it was last reported.
Communicate corporate risk information to inform work prioritization and decision making.
Stop

MINISTRY OF WATER AND ENVIRONMENT

Fraud Risk Management Framework

Table of Contents

1.0 Introduction 3

1.1 MWE Fraud Risk Management Principles 3

1.2 Definition …………………………………………………………………………………………4

1.3 Ethics……………………………………………………………………………………………..5

2.0 The Fraud Risk Management Framework 5

2.1 Control Environment 5

2.2 Risk Assessment 6

2.3 Control activities 6

2.4 Fraud Prevention 6

2.5 Fraud Detection 7

2.6 Communication and information 7

2.7 Monitoring activities 7

3.0 Roles and Responsibilities for Preventing and Detecting Fraud 8

3.1 MWE TPC and Audit and Risk Committee 8

3.2 Line Managers 8

3.3 All Employees 8

3.4 Internal Audit 9

3.5 External Audit 9

4.0 FRAUD RESPONSE PLAN 9

4.1 Introduction 9

4.2 Objectives of this Plan 10

4.3 Notifying Suspected Fraud 10

4.4 The Investigation Process 10

4.5 Liaison with Police & IGG 11

4.6 Initiation of Recovery Action 11

4.7 Reporting process 11

4.8 Part 3: Reporting 12

4.9 Managing public relations 12

ANNEX B: DOs & DON’Ts……………………………………………………………13

List of Abbreviations

1.0 Introduction

The COSO's internal control framework, which the organization revised in 2013, sets forth seventeen principles of internal control associated with five internal control components. For a system of internal control to be effective, according to COSO, each of the seventeen principles must be "present," "functioning," and operating "in an integrated manner." Principle 8 of COSO's 2013 "Internal Control – Integrated Framework" requires organizations to consider the potential for fraud in assessing risks to the achievement of objectives.

A sound ethical culture and an effective system of internal control are essential elements of MWE's anti-fraud strategy. Effective internal controls reduce exposure to financial risks and 'contribute to the safeguarding of assets, including the prevention and detection of fraud'.

The purpose of this fraud risk management framework and policy is to assist management with the fraud risk management process within the Ministry of Water and Environment ("MWE"). This policy will assist MWE management to make informed decisions that will enable management to provide a level of assurance that current fraud risks rated as significant are managed effectively.

MWE is committed to ensuring that high legal, ethical and moral standards are in place across the organization and is committed to countering any fraud or corruption. MWE commits to having a robust and comprehensive system of risk management, control and corporate governance that includes the prevention and detection of corruption, fraud, bribery and irregularities.

This Policy sets out the roles and responsibilities of staff, management and other parties towards achieving this. Specifically, the sections which follow outline responsibilities for preventing and detecting fraud and set out how staff should respond if they suspect that a fraud is or has been taking place.

The policy applies to any fraud, or suspected fraud, involving employees as well as consultants and contractors.

1.1 Ministry of Water and Environment Fraud Risk Management Principles

The Ministry of Water and Environment (MWE) will put in place the following key principles to proactively establish an environment that effectively manages the risk of fraud in the organization:

i. **Principle 1**: As part of MWE's governance structure, this fraud risk management framework and policy has been developed to convey the expectations of the Top Policy Committee (TPC) and senior management regarding the prevention and management of fraud risk in the organization.

ii. **Principle 2**: Fraud risk exposure will be assessed periodically by MWE to identify specific potential schemes and events that the MWE needs to mitigate in order to effectively prevent fraud in the organization.

iii. **Principle 3**: MWE will continuously explore and establish various fraud risk prevention techniques to avoid potential key fraud risk events and where feasible, to mitigate possible impacts on the MWE.

iv. **Principle 4**: MWE will establish appropriate Fraud Risk detection techniques to uncover fraud events when preventive measures fail or unmitigated risks are realized.

v. **Principle 5**: MWE will put in place a reporting process to solicit input on potential fraud. In addition, MWE will also develop a coordinated approach to Fraud investigation and corrective action should to help ensure potential fraud is addressed appropriately and timely.

These principles are drawn from the internal control framework issued by the Committee of Sponsoring Organizations of the Treadway Commission ("COSO"). These are founded on Principle 8 of the COSO framework i.e. "The organization considers the potential for fraud in assessing risks to the achievement of objectives". Therefore, Fraud Risk Management is part of MWE's Risk management strategies.

1.2 Definition

The MWE recognizes that a proactive rather than re-active fraud control plan is an integral part of its Governance Framework.

For purposes of this Fraud Risk Management Framework, Fraud is defined as: "***The dishonest misuse of MWE's resources or using one's position and power for personal gain"***.

A basic test for fraud includes the following questions.

i) Was deceit employed?
ii) Was the action unlawful?
iii) Did it result in money/benefits being received to which the person was not entitled?

Examples of fraud include:

- Theft of any MWE property by staff or third parties.
- Forgery or alteration of any document, for example, a cheque.
- Destruction or removal of records without appropriate authority.
- Falsifying documents such as expense claims or timesheets – this is a form of theft.
- Misusing time during working hours – e.g. taking unauthorized absences or falsely claiming to be sick.
- Disclosing confidential information to outside parties without authority.
- Unauthorized use of MWE assets.
- Falsifying accounting or other records.
- Inappropriate relationships with third parties causing conflicts of interest and loss/gains to MWE.
- Giving or receiving bribes.
- Gaining an unfair advantage, personally or for family and friends
- Using MWE name, logo or letterhead for improper or personal reasons and to imply that MWE has sanctioned the content of any documentation.
- Completing a recruitment application stating that particular qualifications and/or membership of professional bodies are held when they are not or failing to disclose convictions or other required information.
- Making offers of or accepting monetary or other benefit to undertake a particular course of action.

This list is illustrative and not exhaustive; other examples of fraud also exist.

1.3 Ethics

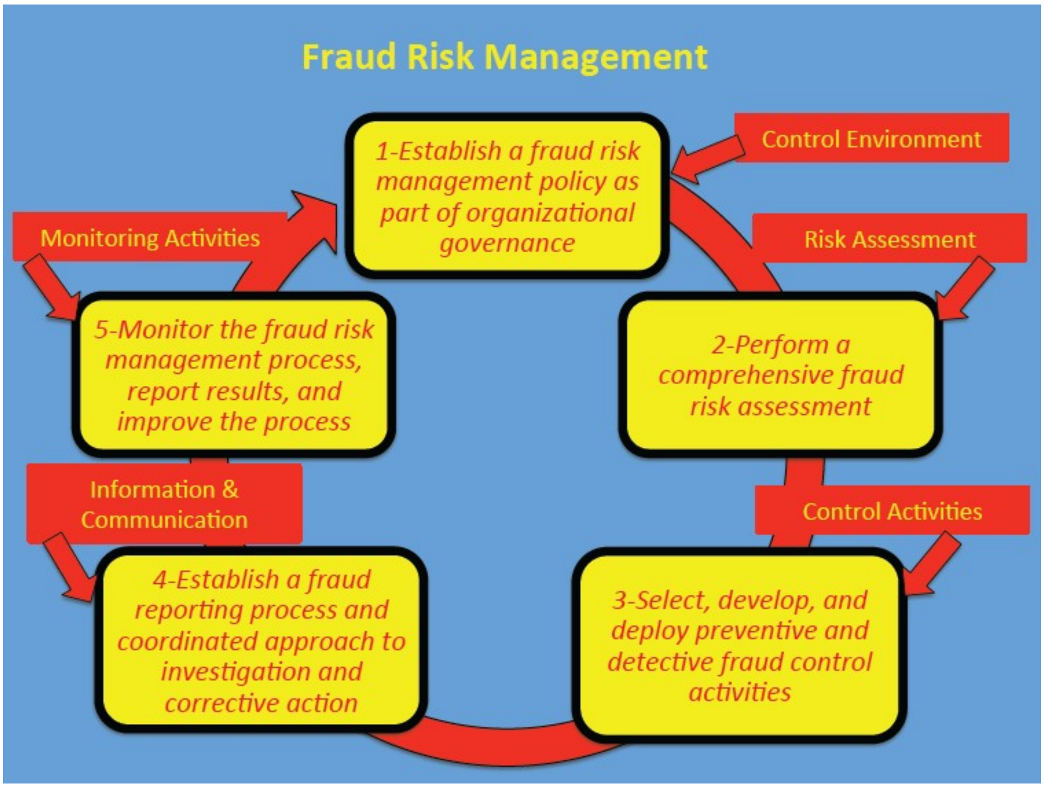
The MWE recognizes that fraud prevention requires the maintenance of an ethical climate which encourages all staff to be active in protecting MWE's funds and assets, and in reporting any breaches of accepted standards.

The MWE's Code of Conduct guides Management and staff in what is accepted practice and behavior and sets our ethical standards at a level above the Law.
MWE's values also reinforce ethical behavior:-
Employees will always:

- Act with fairness
- Act with honesty and integrity
- Act openly

Managers must be mindful of their responsibility to foster and develop in their areas the highest standards of ethical behavior and commitment to a highly ethical workforce culture.

2.0 The Fraud Risk Management Framework


Fraud Risk Management
1-Establish a fraud risk management policy as part of organizational governance
Control Environment
Monitoring Activities
Risk Assessment
5-Monitor the fraud risk management process, report results, and improve the process
2-Perform a comprehensive fraud risk assessment
Information & Communication
Control Activities
4-Establish a fraud reporting process and coordinated approach to investigation and corrective action
3-Select, develop, and deploy preventive and detective fraud control activities

2.1 Control Environment

MWE will establish and communicate a Fraud Risk Management Policy as part of organizational governance that demonstrates the expectations of the TPC and senior management and their commitment to high integrity and ethical values regarding managing fraud risk. To achieve this, MWE will demonstrate the following principles in its Fraud risk Management.

i. The MWE will demonstrates a commitment to integrity and ethical values
ii. TPC will be independent from management and will exercise oversight over the development and performance of internal control.

iii. Management with TPC oversight will establishes structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
iv. MWE commitments to attracting, developing, and retaining competent staff in alignment with objectives.
v. MWE will continuously hold staff accountable for their internal control responsibilities in the pursuit of objectives.

2.2 Risk Assessment

The MWE will perform comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks. To achieve this, the following principles will be put into consideration.

1. The MWE specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
2. The MWE identifies risks to the achievement of its objectives across MWE and analyzes risks as a basis for determining how the risks should be managed.
3. The MWE considers the potential for fraud in assessing risks to the achievement of objectives.
4. The MWE identifies and assesses changes that could significantly impact the system of internal control.

2.3 Control activities

The MWE will select, develop, and deploy preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner. To achieve this;

5. The MWE will selects and develop control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
6. The MWE will select and develops general control activities over technology to support the achievement of objectives.
7. The MWE will deploy control activities through policies that establish what is expected and procedures that put policies into place.

2.4 Fraud Prevention

The MWE recognizes the importance of prevention in its approach to fraud and has in place various measures including denial of opportunity, effective leadership, auditing and employee screening.

The MWE will minimize Fraud through well designed and consistently applied management procedures which deny opportunities for fraud. In particular, financial systems and procedures will take into account the need for internal checks and internal control. Additionally, the possible misuse of information technology will be prevented through the management of physical access to terminals and protecting systems with electronic access restrictions where appropriate.

The MWE has in place a number of policies and related guidance that assist in preventing fraud which include the following:

- Financial Regulations

- Anti-Bribery policy and guidance
- Travel and expenses policy
- Staff rewards and incentives policy
- Whistle blowing policy

The MWE's Audit and Risk Committee will provide an independent and objective view of internal controls by overseeing Internal and External Audit Services, reviewing reports and systems and procedures and ensuring compliance with MWE's Financial Regulations and the requirements of the public financial management. These external reviews of financial checks and balances and validation testing provide a further deterrent to fraud and advice about system development/good practice.

2.5 Fraud Detection

Whilst it is accepted that no systems of preventative measures can guarantee that frauds will not occur, MWE has in place detection measures to highlight irregular transactions. All internal management systems are designed with detective checks and balances in mind and this approach is applied consistently utilizing wherever possible the expertise and advice of MWE's Auditors.

The approach includes the need for segregation of duties, reconciliation procedures, the random checking of transactions and the review of management accounting information including exception reports. As set out in the whistleblowing policy, concerns expressed by staff, students or others associated with MWE are looked into by MWE without adverse consequences for the complainant, maintaining confidentiality wherever possible.

The MWE views its preventative measures by management, coupled with sound detection checks and balances as its first line of defense against fraud.

2.6 Communication and information

The MWE will establish a communication process to obtain information about potential fraud and deploy a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.

8. The MWE will obtain or generate and uses relevant, quality information to support the functioning of internal control.
9. The MWE will internally communicate information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
10. The MWE will communicate with external parties regarding matters affecting the functioning of internal control.

2.7 Monitoring activities

MWE will select, develop, and perform ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates Fraud Risk Management Program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the TPC.

11. The MWE selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

12. MWE evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and TPC, as appropriate.

3.0 Roles and Responsibilities for Preventing and Detecting Fraud

All MWE senior managers and employees have a clear responsibility for the prevention and detection of fraud.

The key responsibilities of individuals and groups are set out below.

3.1 Ministry of Water and Environment TPM/TPC and Audit and Risk Committee

The TPM is ultimately responsible for ensuring that systems are in place for the prevention, detection and investigation of fraud, whilst day-to-day operation of relevant policies, procedures and controls is delegated to management.

The TPM, together with the Audit and Risk Committee, are responsible for:

- Adopting and approving a formal fraud policy and response plan.
- Setting the framework with regard to ethos, ethics and integrity.
- Ensuring that an adequate and effective control environment is in place.
- Ensuring that adequate audit arrangements are in place to investigate suspected fraud.

3.2 Line Managers

Line managers are responsible for implementing this Policy in respect of fraud prevention and detection and in responding to incidents of fraud. In particular, this involves ensuring that the high legal, ethical and moral standards are adhered to in their departments. The practical requirements of line managers are to:

- Have an understanding of the fraud risks in their areas and to consider whether processes under their control might be at risk.
- Have adequate processes and controls in place to prevent, deter and detect fraud.
- Be diligent in their responsibilities as managers, particularly in exercising their authority in authorizing transactions such as timesheets, expense claims, purchase orders, returns and contracts.
- Deal effectively with issues raised by staff including taking appropriate action to deal with reported or suspected fraudulent activity.
- Report suspected frauds according to the process outlined in Section 5.
- Provide support / resource as required to fraud investigations.

3.3 All Employees

The MWE expects all employees to be responsible for:

- Upholding the high legal, ethical and moral standards that are expected of all individuals connected to MWE.
- Adhering to the policies and procedures of MWE
- Safeguarding MWE’s assets
- Alerting management and / or other contacts should they suspect that the possibility of a fraud exists.

- Being aware of MWE policies and procedures to the extent they are applicable to their role.

3.4 Internal Audit

The MWE's Internal Auditors are not responsible for detecting fraud. As with all aspects of governance, control and risk management is the responsibility of management. However, Internal Audit's role in respect of fraud is to:

- Regularly review fraud policies, procedures, prevention controls and detection processes making recommendations to improve these processes as required.
- Discuss with management any areas which it suspects may be exposed to fraud risk.
- Help determine the appropriate response to a suspected fraud and to support any investigation that takes place.
- Facilitate corporate learning on fraud, fraud prevention and the indicators of fraud.

3.5 External Audit

External Audit is not responsible for detecting fraud. However, should the impact of fraud, as with all material misstatements, be of such magnitude as to materially distort the truth and fairness of the financial statements, the external auditors should detect the fraud and report it to the Audit and Risk Committee.

4.0 Fraud Response Plan

4.1 Introduction

This plan deals mainly with the responsibilities of all staff in deterring losses to public funds. There are additional responsibilities borne by managers. The document deals mainly with the internal response and actions that we need to take within the Office to both deter fraud, and to respond to any suspicion of it that comes to our attention. That said, it is important to remember that fraud could be carried out by people outside the Office and we each of us need to be aware of this in our dealings with external parties.

Any suspicion of fraud will be investigated as set out in this plan. Any proven instance of fraud will result in disciplinary action being taken against any member of staff involved. The policy of the Commissioner is to notify the police in circumstances where there is evidence that a crime may have been committed.

The Staff Code of Conduct sets out standards which staff are expected to meet at all times, particularly with regard to the safeguarding of public funds.

This fraud response plan provides a checklist of actions and a guide to follow in the event that fraud is suspected. It covers:

- Notifying suspected fraud;
- The investigation process;
- Liaison with police and IGG;
- Initiation of recovery action;
- Reporting process;
- Communication.

4.2 Objectives of this Plan

The objectives of having a widely circulated and understood response plan are:

- To deter fraud by publicizing steps that will be taken if any is discovered.
- To set out managers' responsibilities in this area.
- To set out clear guidance on the appropriate steps to be taken if managers become aware of, or suspect that, fraud may be taking place.

4.3 Notifying Suspected Fraud

It is important that all staff are able to report their concerns without fear of reprisal or victimization and are aware of the means to do so. MWE must provide appropriate protection for those who voice genuine and legitimate concerns through the proper channels. See the separate Whistle Blowing Policy for further details.

In the first instance, any suspicion of fraud, theft or other irregularity should be reported, as a matter of urgency, to your line manager. If such action would be inappropriate, your concerns should be reported upwards to one of the following persons:

- Head of Function or Head of Team
- Accounting Officer.

Additionally, all concerns must be reported to the Chief Risk Officer (CRO).

2.4. Every effort will be made to protect an informant's anonymity if requested. However, MWE will always encourage individuals to be identified to add more validity to the accusations and allow further investigations to be more effective. In certain circumstances, anonymity cannot be maintained. This will be advised to the informant prior to release of information.

4.4 The Investigation Process

Suspected fraud must be investigated in an independent, open-minded and professional manner with the aim of protecting the interests of both MWE and the suspected individual(s). Suspicion must not be seen as guilt to be proven.

The investigation process will vary according to the circumstances of each case and will be determined by the Accounting Officer in consultation with the CRO, the appropriate Director and the Head of Internal Audit. An "Investigating Officer" will be appointed to take charge of the investigation on a day-to-day basis. This will normally be the Head of Internal Audit or, exceptionally, another independent manager.

The Investigating Officer will appoint an investigating team. This will normally comprise staff from within the Internal Audit team but may be supplemented with other resources from within MWE or from outside.

Where initial investigations reveal that there are reasonable grounds for suspicion, and to facilitate the ongoing investigation, it may be appropriate to suspend an employee against whom an accusation has been made. This decision will be taken by the Accounting Officer in consultation with the Head of Human Resources and Organizational Development and the Investigating Officer. Suspension should not be regarded as disciplinary action nor should it imply guilt. The process will follow the guidelines set out in MWE's and Public Service Terms and Conditions of Service relating to such action.

It is important, from the outset, to ensure that evidence is not contaminated, lost or destroyed. The investigating team will therefore take immediate steps to secure physical assets, including computers and any records thereon, and all other potentially evidential documents. They will also ensure, in consultation with management, that appropriate controls are introduced to prevent further loss.

The Investigating Officer will ensure that a detailed record of the investigation is maintained. This should include a chronological file recording details of all telephone conversations, discussions, meetings and interviews (with whom, who else was present and who said what), details of documents reviewed, tests and analyses undertaken, the results and their significance. Everything should be recorded, irrespective of the apparent significance at the time.

All interviews will be conducted in a fair and proper manner. Where there is a possibility of subsequent criminal action, the police will be consulted and a statement may be recorded. The findings of the investigation will be reported to the Accounting Officer, who will determine, in consultation with the Investigating Officer, what further action (if any) should be taken.

4.5 Liaison with Police & IGG

The police generally welcome early notification of suspected fraud, particularly that of a serious or complex nature. Some frauds will lend themselves to automatic reporting to the police (such as theft by a third party). For more complex frauds the Accounting Officer, following consultation with the Director of Finance, Head of Human Resources and Organizational Development and the Investigating Officer will decide if and when to contact the police. The Director of Finance and Corporate Services will report suspected frauds to the IGG at an appropriate time.

All staff will co-operate fully with any police or IGG enquiries, which may have to take precedence over any internal investigation or disciplinary process. However, wherever possible, teams will co-ordinate their enquiries to maximize the effective and efficient use of resources and information.

4.6 Initiation of Recovery Action

MWE will take appropriate steps, including legal action if necessary, to recover any losses arising from fraud, theft or misconduct. This may include civil action against third parties involved in the fraud, or whose negligent actions contributed to the fraud, to recover any losses.

4.7 Reporting process

Throughout any investigation, the Investigating Officer will keep the Accounting Officer, Director of Finance and Corporate Services and Head of Human Resources and Organizational Development informed of progress and any developments. These reports may be verbal or in writing. On completion of the investigation, the Investigating Officer will prepare a full written report setting out:

- Background as to how the investigation arose;
- What action was taken in response to the allegations;
- The conduct of the investigation;

- The facts that came to light and the evidence in support;
- Action taken against any party where the allegations were proved;
- Action taken to recover any losses;
- Recommendations and/or action taken by management to reduce further exposure and to minimize any recurrence.

In order to provide a deterrent to other staff a brief and anonymized summary of the circumstances may be published on MWE intranet.

4.8 Part 3: Reporting

The CRO is responsible for compiling reports on a quarterly basis that needs to be discussed with SMT members; where after the final reports must be presented to the TPC.
All incidents and/or allegations formally reported to the CRO in writing must be added onto the confidential unethical incident register where it will be monitored by the CRO. The unethical incident register must also be tabled at SMT and Audit Committee meetings:

All reports of fraud, theft and corruption must be treated confidentially. The progress of investigations will not be disclosed or discussed with any person(s) other than those who have a legitimate right to such information as determined by the Accounting Officer and/or CRO. This is a precaution by MWE to avoid compromising the reputations of suspected persons who are subsequently exonerated from any wrongful conduct.
No employee is authorized to supply any information with regard to reports of fraud, theft and corruption, covered within this policy, to the media, or any other party, without the permission of the Accounting Officer in consultation with the CRO.

The Accounting Officer in consultation with the CRO will decide whether any information relating to corrective actions taken or sanctions imposed, regarding incidents of fraud should be brought to the attention of other employees or made public through any other means.

4.9 Managing public relations

Any requests for information from the press or anyone outside MWE concerning any investigation of irregularity must be referred directly to MWE PS. The advice of the Director of Communications will be taken into consideration by MWE PS prior to issuing any statements. Under no circumstances should the investigating officer or other manager/employee provide statements to press or external persons.

ANNEX B: DOs & DON'Ts

DO	DON'T
• **Make a note of your concerns** Record all relevant details, such as the nature of your concern, the names of parties you believe to be involved, details of any telephone or other conversations with names dates and times and any witnesses. Notes do not need to be overly formal, but should be timed, signed and dated. Timeliness is most important. The longer you delay writing up, the greater the chances of recollections becoming distorted and the case being weakened. • **Retain any evidence you may have** The quality of evidence is crucial and the more direct and tangible the evidence, the better the chances of an effective investigation. • **Report you suspicions promptly** In the first instance, report your suspicions to your line manager. If this action would be inappropriate, further guidance on disclosure can be found in the Fraud Response Plan and Whistle-blowing Policy. Additionally, all concerns must be reported to the Head of Internal Audit	• **Be afraid of raising your concerns** The Public Interest Disclosure Act provides protection for employees who raise reasonably held concerns through the appropriate channels – whistle blowing. You will not suffer discrimination or victimization as a result of following these procedures and the matter will be treated sensitively and confidentially. • **Convey your concerns to anyone other than authorized persons** There may be a perfectly reasonable explanation for the events that give rise to your suspicion. Spreading unsubstantiated concerns may harm innocent persons. • **Approach the person you suspect or try to investigate the matter yourself** There are special rules relating to the gathering of evidence for use in criminal cases. Any attempt to gather evidence by persons who are unfamiliar with these rules may destroy the case.