REPUBLIC OF RWANDA

Ministry of Finance and Economic Planning
MINECOFIN

Risk Management Guidelines 2019

May, 2019

TABLE OF CONTENTS

I. ACRONYMS AND ABREVIATIONS

AC - Audit Committee
CBM - Chief Budget Manager
COSO - Committee of sponsoring organizations of the Treadway Commission
EDPRS - Economic Development and Poverty Reduction Strategies
GoR - Government of Rwanda
ISO - The International Organization for Standardization
IT - Information Technology
KRIs - Key risk indicator
Minister - Minister for Finance and Economic Planning
MRC - Management Risk Committee
NST - National Strategy for Transformation
PFM - Public Financial Management
RM - Risk Management
RMC - Risk Management Coordinator
RR - Risk register

II. FOREWORD

The Government of Rwanda is committed to a process of risk management that is aligned to the principles of sound corporate governance. Recognizing that management of risk is an important strategy for the achievement of NST 1, the Organic Law No. 12/2013/OL of 12/09/2013 on State Finances and Property requires every public institution to put in place risk management mechanisms to manage uncertainties that could impede achievement of institution's objectives.

Risk management is an integral part of management, therefore, public entities are required to adopt a comprehensive approach to the management of risk as outlined in the organization's Risk Management Strategy. All public entities have to adhere to the risk management strategy and work together in a consistent and integrated manner, with the overall objective of reducing risk and taking advantage of opportunities, as far as reasonably practicable. Public entities shall adopt an entity-wide approach to risk management and ultimately, the risk management processes shall become embedded into entity's systems and processes, ensuring that responses to risk remain current and dynamic.

These guidelines have been developed to assist public entities to formalize risk management procedures which shall include, among others, risk management frameworks as required under Article 114 of Ministerial Order N°001/16/10/TC of 26/01/2016 relating to financial regulations.

The Public entities shall develop institutional risk management frameworks based on their specific circumstances to lay out the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the entity. They shall put in place a risk management policy and strategies that outline their commitment and direction related to risk management and anti-fraud policy that specifically outline how they will fight against fraud risks.

The risk management policy and strategies shall be reviewed regularly to reflect the current stance on risk management in line with operational and regulatory requirements. Every

employee has a part to play in this important endeavor and we look forward to working with all the stakeholders in achieving these aims.

These guidelines aim at providing principles of risk management which entities can adapt to address the specific circumstances. Additional clarification on how to implement these guidelines can be obtained from the Office of the Chief Internal Auditor in the Ministry of Finance and Economic Planning.

Dr. Uzziel Ndagijimana

Minister

III. TERMS AND DEFINITIONS

For purpose of these guidelines, the following terms shall have this meaning

Term	Meaning
Risk	Effect of uncertainty on objectives. An effect is a deviation from the expected — positive and/or negative
Risk management	Coordinated activities to direct and control an organization with regard to risk
Risk management framework	Set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization
Risk management policy	Statement of the overall intentions and direction of an organization related to risk management
Risk attitude	Organization's approach to assess and eventually pursue, retain, take or turn away from risk
Risk appetite	The broad-based amount of risk an Organization is willing to accept in pursuit of its mission.
Risk management plan	Scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk. Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities
Risk owner	Person or entity with the accountability and authority to manage a risk
Risk management process	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk
Establishing the context	Defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy
External context	External environment in which the organization seeks to achieve its objectives
Internal context	Internal environment in which the organization seeks to achieve its objectives
Communication and consultation	Continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk
Stakeholder	Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation

Risk identification	Process of finding, recognizing and describing risks. Risk identification involves the identification of risk sources, events, their causes and their potential consequences.
Risk source	Element which alone or in combination has the intrinsic potential to give rise to risk
Event	Occurrence or change of a particular set of circumstances
Consequence	Outcome of an event affecting objectives
Likelihood	Chance of something happening
Risk profile	Description of any set of risks
Risk analysis	Process to comprehend the nature of risk and to determine the level of risk
Risk criteria	Terms of reference against which the significance of a risk is evaluated
Level of risk	magnitude of a risk or combination of risks, expressed in terms of consequences and their likelihood
Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable
Risk treatment	Process to modify risk
Control	Measure that is modifying risk
Risk register	A risk register is a comprehensive list of threats and opportunities and actions established to address them. A risk register is simply a documented record of the identified risks, their significance or rating, and how they are managed or treated.
Residual risk	Risk remaining after risk treatment
Monitoring	Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives

CHARPTER ONE

INTRODUCTION

This chapter outlines the purpose and objectives of these guidelines and present the regulatory framework and basis of developing Risk Management guidelines. It provides the scope, principles and applicability of the proposed framework.

These guidelines were prepared to provide guidance to all public entities on the implementation of risk management systems and frameworks.

1.1 Basis of preparation and regulatory framework

Article 13 (7) and (8) of Organic Law N° 12/2013/OL of 12/09/2013 on State Finances and Property requires the Chief Budget Manager (CBM) to establish and maintain effective, efficient and transparent systems of internal controls and risk management.

In addition, Article 114 (1) of Ministerial Order N°001/16/10/TC of 26/01/2016 relating to Financial Regulations requires the Minister to issue guidelines to public entities on risk management policies and procedures to enable public entities develop their own risk management strategies for the approval by their Executive Heads and/or decision making organs before implementation.

Further, Article 11 (7) of Ministerial Order no 003/17/10/TC of 27th October 2017 requires the Chief Internal Auditor to develop and promote risk management guidelines and monitor compliance across Government.

These guidelines shall be implemented within existing Laws and Regulatory Frameworks in force and where there is contradiction with any specific law or regulation, the law or regulation shall take precedence over these guidelines.

1.2 Purpose

The purpose of these guidelines is to help public entities in developing their own risk management, frameworks, policies and strategies and establishing formal risk management

process. While the Government expects to have uniform application and practices of risk management across all public entities, it recognizes that some public institutions may face different types of risks and magnitude, therefore, public entities that operate in sectors or industries with unique risks may use additional specialized risk management standards and methodologies after consulting the Office of Chief Internal Auditor.

1.3 Scope and Applicability

These guidelines shall apply to Public Sector entities including central and local governments and public enterprises.

1.4 Distribution and sensitization

These guidelines shall be distributed to all public entities. There shall be a wider stakeholder consultation and sensitization of all responsible parties in implementation of these guidelines.

1.5 Effective date of the guideline

These guidelines shall be effective on the date approved by the Minister

1.6 Review and amendments

These guidelines shall be reviewed and amended, when circumstances dictate on recommendation of the Chief Internal Auditor.

CHAPTER TWO

RISK MANAGEMENT FRAMEWORK, POLICY AND STRATEGY

2.1 Risk Management Principles

The International Organization for Standardization (ISO) and the Committee of Sponsoring Organization of Tredway Commission (COSO) are worldwide recognized standard setter for Risk Management used in most Organization both private and Public to set up their Enterprise Risk management frameworks.

The Risk management standard to be used is ISO/ NZS ISO 31000: 2009 as amended to date. Its Principles and Guidelines are presented below:

No	Principle	Explanation
1	Creates and protects value	Good risk management contributes to the achievement of an entity's objectives through the continuous review of its processes and systems
2	Is an integral part of organizational processes	Risk management needs to be integrated with an entity's governance framework and become a part of its planning processes, at both the operational and strategic level. Risk management must be incorporated in the entity's corporate and business planning processes.
3	Is part of decision making	The process of risk management assists decision makers to make informed choices, identify priorities and select the most appropriate action. Decision making within the entity, whatever the level of importance and significance, should include consideration of risks and the application of the risk management process as appropriate
4	Explicitly address uncertainty	By identifying potential risks, agencies can implement controls and treatments to maximize the chance of gain while minimizing the chance of loss.
5	Is systematic, structured and timely	The process of risk management should be consistent across an agency to ensure efficiency, consistency and the reliability of results.
6	Is Based on the best available information	To effectively manage risk it is important to understand and consider all available information relevant to an activity and to be aware that there may be limitations on that information. It is then important to understand how all this information informs the risk

		management process.
7	Is tailored	An entity's risk management framework needs to include its risk profile, as well as take into consideration its internal and external operating environment.
8	Takes into account human and cultural factors	Risk management needs to recognize the contribution that people and culture have on achieving an agency's objectives
9	Is transparent and inclusive	Engaging stakeholders, both internal and external, throughout the risk management process recognizes that communication and consultation is key to identifying, analyzing and monitoring risk.
10	Frequent reporting to all stakeholders	The agency's risk management performance should be included in the agencies governance processes. This reporting would be ongoing and highly visible
11	Is dynamic, iterative and responsive to change	The process of managing risk needs to be flexible. The challenging environment entities operate in requires to consider the context for managing risk as well as continuing to identify new risks that emerge, and make allowances for those risks that no longer exist.
12	Facilitates the continual improvement of organizations	- Entities with a mature risk management culture are those that have invested resources over time and are able to demonstrate the continual achievement of their objectives.

Every Government institution is required to prepare risk management policies, strategies and plans that are responsive to their unique context.

2.2 Risk Management Framework

The Risk Management Framework is set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization. The foundations include the policy, objectives, mandate and commitment to manage risk. The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.

The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

2.1.1 Purpose of the Risk Management Framework

The purpose of the Risk Management Framework is to define how management of risk is handled within the associated context (could be organization-wide or for a specific activity such as a project/program). To provide information on roles, responsibilities, processes and procedures, tools, facilities and documentation required.

For effective implementation of Risk Management Framework within public entities, the following best practice principles and strategies shall be applied:

- Promoting an organizational philosophy and culture that says everybody is a risk manager;
- The entity Board of Director, Council or Commission and top management must champion risk management, define and communicate acceptable levels of risk (risk appetite);
- The Entity Executive Management shall establish open communication channels;
- Entities shall adopt the strategy of using teams and committees;
- The entities shall adopt easy, simple and common risk language;
- Each entity shall set up an enterprise-wide Risk Management Function;
- Each entity shall on regular basis communicate Risk Management performance;
- Each entity shall plan and carry out capacity building and continuous Risk Management training for all personnel.

2.1.2 Developing the Risk Management Framework

To develop an effective Risk Management Framework, entities shall follow a systematic approach consisting of the following steps:

- **Step 1: Establishing the risk governance structure**

The oversight responsibility for risk management will be discharged by the entity Board of Directors, Council or Commission depending on the entity structure who shall have the

primary responsibility to approve the entity risk management Framework. The Board/Council may delegate this function to the Audit Committee.

The Senior Management and Management Risk Committees shall have the responsibility for setting risks limits within the approved risk appetite level and tolerance limits. Executive levels, CBM shall have responsibility for implementing risk frameworks, policies and procedures.

Risk Management Department or Units shall carry out risk identification, assessment monitoring, reporting and mitigation of risks. In the entities where Risk Management Department does not exist, management shall select an officer to be assigned the responsibility for risk management until risk management structure is created. The internal auditor shall independently provide the assurance on the adequacy and effectiveness of Risk Management processes within the entity. Detailed roles and responsibility for risk management is presented in chapter three.

Detailed roles and responsibility for each of the key players in risk management is **presented in chapter four of these guidelines.**

- **Step 2: Define the context for risk management- (Risk appetite for the Entity)**

The Board/Council shall begin with identifying values and targets, and the programs in-place for achieving them, in that context that the entity shall optimize its ability to exploit opportunities and to control or mitigate setbacks and negative occurrences.

The amount of risk an entity is prepared to take depends on its mission, values, and objectives or targets. Since risks are the threats and opportunities that could potentially affect achievement of an entity's values and targets.

The entity Board of Directors/ Council or Commission shall set up acceptable levels of risks for each category of risks. The entity risk appetite shall be determined both quantitatively and qualitatively whenever possible. The entities shall have zero tolerance for fraud and reputational risks. For other category of risks, the Board/Council shall decide to take either high or low risk appetite depending of the threat or opportunity that the risk present.

- **Step 3: Develop an approach to risk identification**

Developing a systematic approach to identifying risks improves the likelihood of capturing significant threats and opportunities and provides a basis for categorizing them and linking them to the organization's targets or values the impact. Risks shall be categorized by sources.

Entities may adopt two principal categories: internal risks, which are threats and opportunities that arise through the course of operations of the entity; and external risks, which arise from risks outside of the organization and which can be Political, Economic, Social, and Legal, Technological, Security, Environmental or Natural disaster.

Internal risks shall be further broken down into sub-categories such as people; equipment, technology, processes and financial resources to achieve its targets and objectives. The process of risk assessment and management involves identifying the risks, analyzing, evaluating and coming up with strategies for treating the risks in line with ISO 31000 as presented **in chapter three of these guidelines**.

- **Step 4: Build a risk assessment matrix**

Management Risk Committee in collaboration with the top management shall construct an assessment matrix that lays out the criteria for ranking risk (both threats and opportunities) and, depending on their ranking, the level of action and monitoring required to manage such risks.

In order to focus on key threats and opportunities and establish priorities for action, risks shall be assessed and ranked in terms of their probability of occurrence and their estimated impact/consequence on the targets of the organization.

- **Step 5 Establish a risk register**

The Chief Budget Manager shall own the entity Risk Register that shall be maintained by the RMC. Each Department/Unit shall also maintain its Risk Register. The register shall be a living document that is regularly reviewed and updated.

A risk register is a comprehensive list of threats and opportunities and actions established to address them. It is a documented record of the identified risks, their significance or rating, and how they are managed or treated. A risk register shall be used to record threats and opportunities and to track actions established to address them.

The register shall record a description of the threat or opportunity as well as the category (see Step 3 above) it fits into. The objective impacted by the risk shall also be identified as well as its estimated impact, probability of occurrence and time horizon (see Step 4 above). Any planned action shall also be documented, along with the manager accountable for the action and its expected completion date.

- **Step 6: Rollout of the Risk Management Framework**

It is advisable that entities start risk management process within one or two selected Division/department and then rollout to other departments after the successful implementation in the pilot division/department.

An effective approach for incorporating risk management into entity's way of doing business is to integrate it into the entity's planning process. This integration shall begin with the establishment of strategic and operational objectives/targets and deliverables. Each of these targets is assigned to a Divisional/Departmental head who, with his or her managers and staff, identify and rank the potential opportunities and threats that might affect achievement of these targets.

The identified risks and their rankings are then reviewed by the Management Risk Committee, which determines whether they should be incorporated into and monitored as part of entity's risk register, or assigned to a lower level within the entity.

- **Step 7: Incorporate Risk Management into performance monitoring**

The Risk Management Coordinator shall develop a process for reporting the status of the risk register to the Board of Directors/ Council or Commission and top management team on a regular basis. This shall include formal written reports.

2.3 Risk Management Policy

The Risk management Policy is a statement of the overall intentions and direction of an entity related to risk management. The policy clearly states entity's objectives for, and commitment to, risk management. It is central to developing a common understanding of risk and its management within the entity, and provides the opportunity to articulate its risk management vision and to describe the benefits that it derives from managing risk.

The Policy shall contain as a minimum the following: policy Statement; aims and objectives; purpose, scope and applicability; and approval and review processes among others. Public entities risk management policy shall be approved by the entity's Executive Head/Executive Authority and shall be reviewed at least once every three years.

2.4Risk Management Strategy

Risk Management Strategies are actions, tactics deployed by the entity to maintain risks within the accepted tolerable levels (risk appetite) approved by the Board/Council. The Risk Management Strategy serves to implement the entity's risk management policy. The Strategy outlines how the structure of responsibility and accountability across entity shall be developed and maintained. The entities shall deploy one of the following risk management strategies among others:

- Reducing the probability of event happening and or its consequence once it occurs
- Accepting or retaining the risks depending on costs and benefits analysis of deploying other risk management strategies
- Risk avoidance or termination- discontinuing the event that causes the risks
- Risk transfer in the form of taking insurance cover
- Risk mitigation such as Business Continuity Plan
- Integrating risk management into all entity activity; and
- Adopting three lines of defense model into risk management

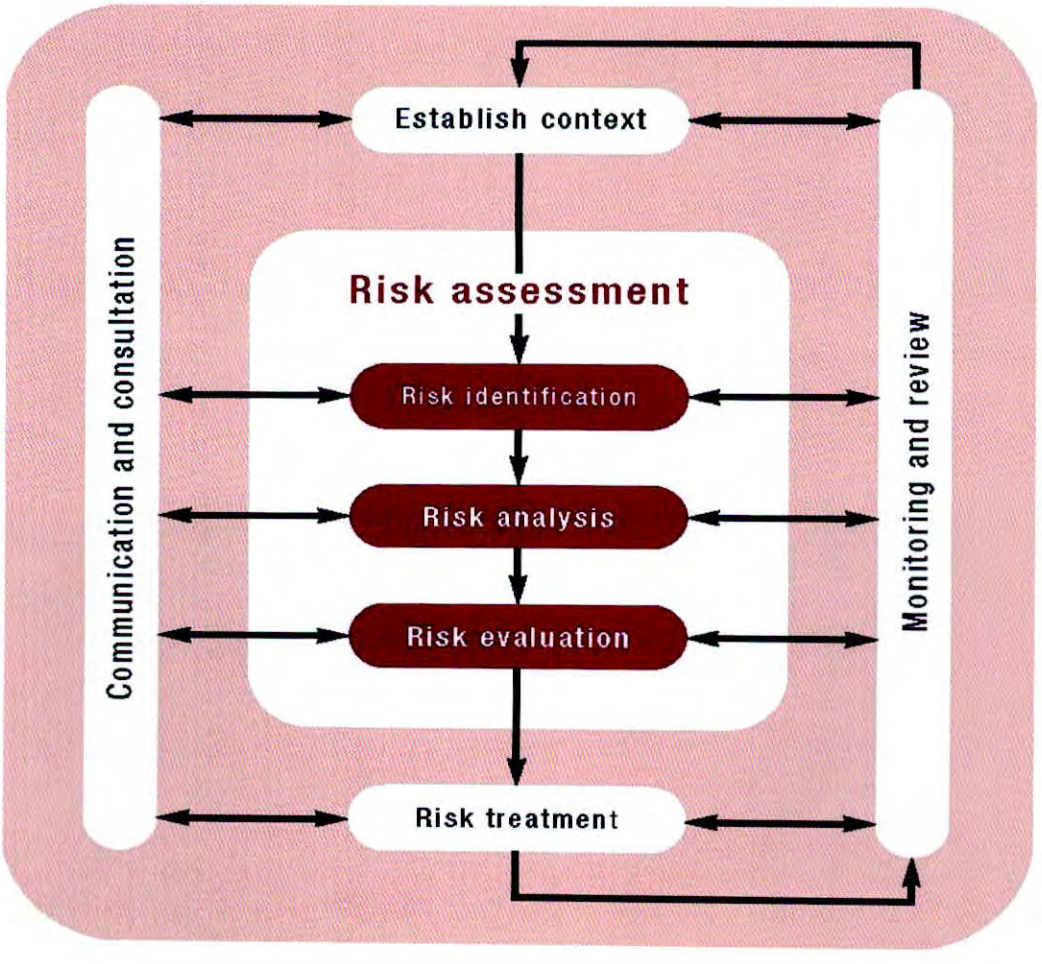
CHAPTER THREE

RISK MANAGEMENT PROCESS

Risk Management process is a systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risks.

Public entities shall adopt and customize the risk management process prescribed in ISO 31000:2009 as revised and amended to date. This process should be an integral part of management, embedded in the culture and practices, and tailored to the business processes of the entity. The process takes into account the uniqueness and environment of the entity in which it operate. The figure below presents the process in summary form:

Figure 1: Risk Management Process



Source: ISO 31000

3.1 Establish the context

The first step in risk management process is to establish the context by identifying the objectives of the entity and consider the internal and external parameters within which the risk must be managed.

Public entities shall actively consider risk and document the assessment formally for any proposed program, project or initiative. It is advisable to always start by identifying the purpose and objectives right at the beginning to avoid being overwhelmed by details and data.

Establishing the context sets the framework within which the risk assessment should be undertaken, ensures the reasons for carrying out the risk assessment are clearly known, and provides the backdrop of circumstances against which risks can be identified and assessed. In general, the following steps are followed in establishing the context for risk management:

- **Set the scope** for the risk assessment by identifying *what* you are assessing – is it a new program, project or perhaps an event?
- **Define the broad objectives.** Identify the reason for the risk assessment – perhaps a change in law, a request from an external auditor or regulator, an operational change or review.
- **Identify the relevant stakeholders.** Aim for an appropriately inclusive process from the outset: be sure to identify the areas that are, or might be, impacted and seek their input. Make sure that appropriate delegations are being exercised even at this early stage.
- **Gather background information.** Having proper information is important. Ask the right people and identify the information that is available. Sometimes it is useful to identify information that is not available (immediately) but may be necessary. Consider: Strategic & business plans, Audit reports, inspections, site visit reports, Personal experience, corporate knowledge & 'institutional memory', previous event investigations or reports, Surveys, questionnaires and checklists, etc. Where possible, consider both the strategic context and operational context, so that a complete picture is obtained.

3.2Risk Identification

The second step in the risk management process is to identify the risks that might have an impact on the objectives of the entity or process, program or activity. This involves identifying sources of the risk, areas of impact, events (including changes in circumstances) and their causes and potential consequences. Describe those factors that might create, enhance, prevent, degrade, accelerate or delay the achievement of the entity's objectives. Risk identification aim also to identify the issues associated with not pursuing an opportunity; that is, the risk of doing nothing and missing an opportunity.

In identifying risk, the following six questions are considered:

No	Question	Question description
i.	What could happen	What might go wrong, or what might prevent the achievement of relevant goals? What events or occurrences could threaten the intended outcome?
ii.	How could it happen	Is the risk likely to occur at all or happen again? If so, what could cause the risk event to recur or contribute to it happening again?
iii.	Where could it happen	Is the risk likely to occur anywhere or in any environment/place? Or is it a risk that is dependent on the location, physical area or activity?
iv.	Why might it happen	What factors would need to be present for the risk to happen or occur again? Understanding why a risk might occur or be repeated is important if the risk is to be managed
v.	What might be the impact	If the risk were to eventuate, what impact or consequences would or might this have? Will the impact be felt locally or will it impact on the whole entity

vi	Who does or can influence the event? How much is within the Entity's control or influence?	Make sure that those with delegations, control, influence, resources and budgets are at least informed if not actively involved. This becomes more important when considering the treatments for the risk?

Wherever possible, provide quantitative and/or qualitative data to assist in describing the risk or to support the risk rating. Sources of information may include past records, staff expertise, industry practices, literature and expert opinion.

3.3 Risk analysis

This is the third step in the process of risk management. Analyzing the risk consists of developing detailed understanding of the risk. Once the risk has been identified and the context, causes, contributing factors and consequences have been described, look at the strengths and weaknesses of existing systems and processes designed to help control the risk. Knowing what controls are already in place, and whether they are effective, helps to identify what – if any further action is required.

The Risk analysis consists of four consecutive steps that is:

- identify the existing controls;
- assessing the likelihood of event occurring;
- assessing the impact once it occurs; and
- rate the level of risk.

3.3.1 Identify the existing controls

Determine what controls are already in place to mitigate the impact of the risk. Controls may be strong or weak; they can be measureable and repeatable. Controls include legislation, policies or procedures, staff training, segregation of duties, personal protective measures and equipment, and structural or physical barriers (e.g. setting up IT firewalls or guards around machinery)

Once the controls have been identified, and their effectiveness analyzed, an assessment is made

of the likelihood of the risk occurring and the consequence if the risk were to occur. This produces an accurate, albeit subjective, assessment of the level of risk -or risk rating and helps in the next step to determine whether risks are acceptable or need further treatment.

3.3.2 Assessing the likelihood

The likelihood of the risk occurring will be described as rare, unlikely, possible, likely, or almost certain and will have the following meaning and probabilities in public entities:

Table1: Likelihood

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

3.3.3 Assessing the impact

The consequences or potential impact if the risk event occurred shall be described in public entities as insignificant, minor, moderate, major or catastrophic. The Risk Management Coordinator shall determine the levels of risk exposure to the entity/unit if the risk materialized. This will be measured in terms of loss of monetary value to the extent possible to determine such amount or it can be measured in terms of effect on reputation to the entity or achievement of the objective.

Table2: Impact

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

The assessment of likelihood and impact is mostly subjective, but can be informed by data or information collected, previous audits, inspections, personal experience, corporate knowledge or institutional memory of previous events, insurance claims, surveys and a range of other

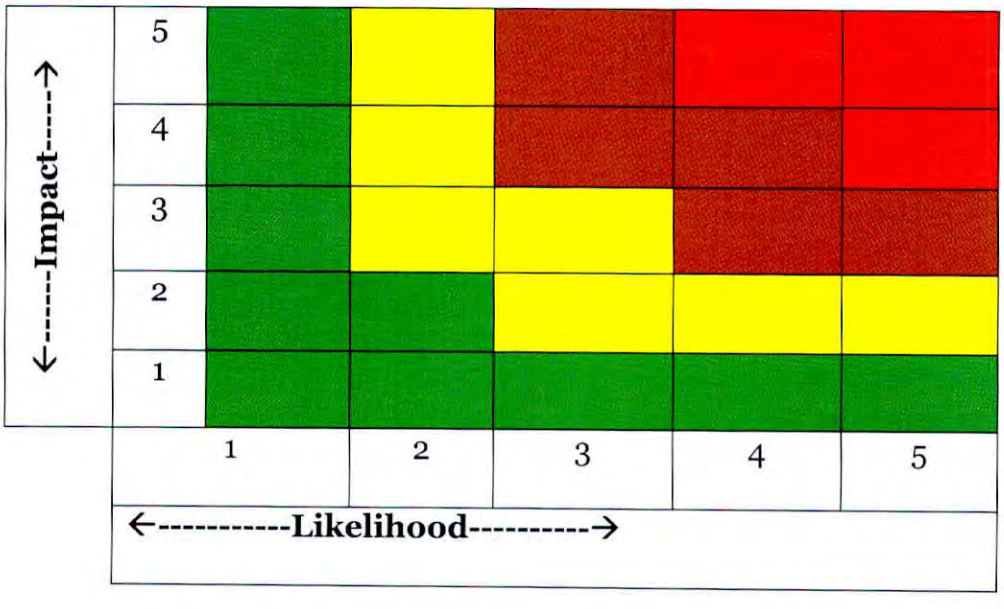
available internal and external information.

The Level of impact sensitivity will depend among others on the size of the entity, the nature and operations. For instance a loss of Frw 10 million may be insignificant in one entity while it is significant in another entity.

3.3.4 Rate the level of risk

Public entities shall use a five by five risk matrix to determine whether the risk rating is *low, medium, high or extreme as presented below:*

Risk Matrix



Scores between 1 to 5 (green color) are ranked Low risk;
Scores between 6 to 10 (yellow color) are medium Risk;
Scores between 12 to 16 (umber color) are ranked high risks; and
Scores between 20 to 25 (red) are ranked extreme risks.

3.4 Risk evaluation

The evaluation step of risk management process consists of deciding whether the risk is acceptable or unacceptable. The entity shall use understanding of risk to make decisions about future actions. These may include:

- not to undertake or proceed with the event, activity, project or initiative;
- actively treat the risk;
- prioritizing the actions needed, if the risk is complex and treatment is required; and
- accepting the risk.

Whether a risk is acceptable or unacceptable relates to a willingness to tolerate the risk; that is, the willingness to bear the risk after it is treated in order to achieve the desired objectives. The attitude, appetite and tolerance for risk is likely to vary over time, across the entity as a whole and for individual process, program, department or activity.

A risk may be acceptable or tolerable in the following circumstances:

- No treatment is available ;
- Treatment costs are prohibitive;
- The level of risk is low and does not warrant using resources to treat it; and
- The opportunities involved significantly outweigh the threats.

A risk is regarded as acceptable or tolerable if the decision has been made not to treat it in accordance with the next step. It is important to remember that considering a risk as acceptable or tolerable does not imply that the risk is insignificant. Risks that are considered acceptable or tolerable may still need to be monitored. When conducting a risk assessment, there are generally lots of potential consequences identified. This is not necessarily a problem as a number of these can be addressed by the risk treatments, or they may not need any specific action. As presented in figure 1: Risk Management Process in ISO 31000, the three steps combined; risk identification analysis and evaluation make the risk assessment and shall be documented in the template below:

RISK ASSESSMENT TEMPLATE

Area/Department				**Risk Register ID**			**Evaluation**
Date of Risk Assessment				**Risk Category**			
Risk Owner				**Assessment Conducted By**			
Establish the Context		**Risk Description**		**Effectiveness of Controls**		**Analysis**	
Objective	**Context**	**Risk Source**	**Description**	**Current Controls**	**Control Rating**	**Risk Rating**	

3.5 Treat the risk

This step ensures that effective strategies are in place to minimize the frequency and severity of the identified risk. Develop actions and implement treatments that aim to control the risk.

Once the risk assessment phase is complete, identify the options for treatment if there are any; otherwise tolerate the risk. Where options for treatment are available and appropriate, record those treatment options as part of the risk treatment plan. Treatment options not applied to the source or root cause of a risk are likely to be ineffective and promote a false belief within the organization that the risk is controlled. Risk treatment passes through the following sequences:

- **Deciding if specific treatment is necessary**

Decide if specific treatment is necessary or whether the risk can be adequately treated in the course of standard management procedures and activities; that is, embed the treatment into day-to day practices or processes.

In assessing what treatments could be implemented, it is useful to consider ways in which standard practices already serve as a control, or ways in which those standard practices could be modified to adequately control the risk.

- **Working out what kind of treatment is desirable for a particular risk**

Determine what the goal is in treating this particular risk; is it to avoid it completely, reduce the likelihood or consequence, transfer the risk (to someone else such as an insurer or contractor) or accept the level of risk based on existing information? The type of risk treatment chosen will often depend on the nature of the risk and the tolerance for that risk.

- **Identifying and designing a preferred treatment option once the goal of treatment is known**

  - If the goal is to reduce the likelihood or possibility of the risk, then you may need to adjust what is happening or might be planned: successfully altering the approach will depend on identifying the causes of the threat and the causal links between the threat and its impact – both of which should have been identified in the risk assessment phase.
  - If it is not possible to change the approach of the project or activity, then it may be possible to take some other intervening actions to mitigate the event's occurrence or reduce the likelihood of the threat. Understanding the nature of the risk event and how it occurs will make it easier to identify any possible intervening actions that would operate to reduce the risk.
  - If the goal is to reduce the consequence or impact of the risk, then contingency plans might be required to respond to a threatening event if it occurs. This planning may be undertaken in combination with other controls – that is, even if steps have been taken to minimize the likelihood of the risk, it may still be worthwhile to have a plan in place to reduce the consequences if the event actually occurs.
  - If the goal is to share the risk, then involving another party, such as an insurer or contractor, may help. Risk can be shared contractually, by mutual agreement, and in a variety of ways that meet all parties' needs. Any such arrangement should be formally recorded – whether through a contract or agreement or by letter. Sharing the risk does not remove obligations and does not avoid entity suffering consequential damage if something unexpected happens or something goes wrong.
  - If the risk is so significant that the goal is to eliminate or avoid it altogether then the options are limited to changing the project materially, choosing alternative approaches or processes to render the risk irrelevant or abandoning the activity or partner or program.

It is not often that a risk can be eliminated completely and balance is an important part of the risk assessment exercise.

- Sometimes, a decision is made to ***accept or tolerate*** the risk, due to the low likelihood or minor consequences of the risk event, or the fact that the cost of effectively controlling the risk is unjustifiably high or that the opportunity outweighs the risk.

Evaluate treatment options and assess their feasibility

- Do the controls selected appear to have the desired treatment effect (that is, will they stop or reduce what they are meant to stop or reduce)?
- Will the controls trigger any other risks? For example, a sprinkler system installed to counter fire risk may cause water damage, presenting a different risk requiring consideration or management.
- Are the controls beneficial or cost efficient?
- Does the cost of implementing the control outweigh the cost that would flow from the event occurring without the control in place?
- Overall, is the cost of implementing the control reasonable for this risk?

The cyclical process of treating a risk, deciding whether residual risk levels are tolerable and assessing the effectiveness of that treatment are all case-by-case assessments that depend on a good understanding of the risk and a focus on the end objective of the activity being assessed.

Document the risk treatment plan

Once the treatment options have been identified, a risk treatment plan should be prepared. Treatment plans should identify responsibilities for action, time frames for implementation, budget requirements or resource implications, performance measures and review process where appropriate. The review process should monitor the progress of treatments against critical implementation milestones.

Risk Treatment Plan Template

Area/Department				**Risk Register ID**		
Date Treatment Developed				**Risk Category**		
Risk Owner				**Treatment Owner**		
Risk Description	**Control Effectiveness**	**Risk Treatment**			**Monitor &Review**	**Implementation Status**
		Treatment Action	**Responsibility**	**Implementation Date**		

- **Implement agreed treatments**

Once any options requiring authorization for resourcing, funding or other actions have been approved, treatments should be implemented by those identified as having the responsibility to do so. The person assigned with the primary responsibility for the risk, is ultimately accountable for the treatment of the risk.

- **Assess the level of residual risk**

Even when a risk has been treated and the controls are in place, the risk may not be completely eliminated. The level of residual risk refers to the likelihood and consequence of the risk occurring after the risk has been treated. Once implemented, treatments provide or modify the controls. The residual risk rating is generally lower than the original risk rating otherwise the controls were not effective.

The residual risk should be documented and monitored and reviewed. Where appropriate, further treatment might be prudent. Having a good awareness of residual risk is important in monitoring and reviewing risk on an ongoing basis.

3.6 Monitor and Review

To ensure structured reviews and regular reporting occurs, each Unit/Department shall identify a process that allows key risks within their area to be monitored. Given the diverse and dynamic nature of the Entity's environment, it is important to be alert to emerging risks as well monitoring known risks. Monitoring changes to the source and context of risks, the tolerance for certain risks and the adequacy of controls shall be carried out regularly.

3.7 Risk Reporting

Formal risk reporting is an important part of being able to demonstrate the effectiveness of the risk management program. The entity is required to report to various internal and external bodies and stakeholders; to achieve this the entity needs to be informed about risks in a timely manner and to be able to access -and reproduce -those risk assessments easily.

The Chief Budget Manager will submit on quarterly basis to the Audit Committee, the risk management report. He or she will also submit Risk Management Annual Report **every 30th September.** The reporting needs to occur via the entity's Risk Register or other appropriate report. The reports shall identify new risks, detail the progress with treating existing risks and report outcomes from the monitoring and review process.

Annual risk reporting shall confirm that all risks are being adequately and appropriately managed. In addition, any risk verified as an extreme risk will require a risk assessment and management plan to be prepared by the senior manager for the CBM endorsement. Extreme and high risks will be overseen by the Entity Management Risk Committee (MRC) on regular basis. Risk response/treatment and appropriate action will be agreed between the officer with primary responsibility (risk owner) and the RMC. Medium and low risks will to be managed and reported by the Head of Unit, monitored and reviewed by the same as necessary.

To ensure that risk management is effective, and to provide evidence of a demonstrable risk management system, it is important to have a documented formal record of the risk management process and outcomes. The tool for recording risks in the entity, is the **Risk Register**. A risk register is simply a documented record of the identified risks, their significance or rating, and how they are managed or treated.

3.8 Communicate and Consult

Effective communication and consultation is essential to ensure that those responsible for implementing risk management, and those with a vested interest, understand the basis on which decisions are made and the reasons why particular treatment options are selected.

Management shall communicate and consult with internal and external stakeholders during any and all stages of the risk management process, particularly when plans are being first

considered and when significant decisions need to be made. Risk management is enhanced through effective communication and consultation when all parties understand each other's perspectives and, where appropriate, are actively involved in decision-making.

CHAPTER FOUR

ROLES AND RESPONSIBILITIES

The risk management within an entity is every body's responsibility. However, Article 13 (7) of Organic Law N° 12/2013/OL of 12/09/2013 on State Finances and Property requires the Chief Budget Manager of Public Entities to establish and maintain effective, efficient and transparent systems of internal controls and risk management. The Law also provides responsibility of the Minister and the Chief Internal Auditor with regards to risk management.

Each entity, depending on its structure, mission, mandate and nature of its activity will have risk management roles and responsibilities assigned to different Organs/ Structures and functions, but for purpose of uniformity and consistence across public entities, the Organs, Structures and functions will have as a minimum the following roles and responsibilities in risk management:

	Organ/Function	**Responsibilities**
1.	The Minister	develop and issue Risk Management Guidelines and oversees their implementation in public entities and annually receive an annual risk management report from the Chief Internal Auditor
2.	Chief Internal Auditor (CIA)	i. Advise the Minister on the development of risk management guidelines; ii. Provide annually an opinion on the adequacy and effectiveness of risk management practices in the Public entities; iii. Support public entities in developing and implementing institutional risk management frameworks; iv. Create awareness and technical training on risk management to public officials from across public sector and capacity building; and v. Consolidate information on risk management from public entities.

3.	Board of Directors or District Council Audit Committees	i. Approve the design and implementation of risk management approaches, including the risk response, tolerance and the Risk Appetite Statement; ii. Receive and consider on quarterly basis the risk Management Reports; iii. Review the entity risk profile on quarterly basis; iv. Define risk threshold levels for referral to the Board/District Council v. ensure that staff charged with Risk Management responsibilities have appropriate authority to carry out their functions and have appropriate access to the Board/District Council; vi. Approve the allocation of resources for effective management of risk; and annual Activity Plan of Risk Management Function
4.	Chief Budget Manager (CBM)	i. Establish and maintain the entity's overall Risk Management, internal controls and governance processes and systems and ensure that they are operating efficiently and effectively; ii. Embed Risk Management practices in all entity's processes; iii. Identify threats to the achievement of entity's objectives; iv. Analyze Cost-effective risk treatment options; v. Put in place appropriate controls and treatment measures to manage identified risks; vi. Review on monthly basis, exposure to all forms of risk and reduce it as-far-as reasonably practicable or achievable; vii. Apply a Robust risk management processes as part of a wider management system;
5.	Management Risk Committee (MRC)	i. Ensure that all risks are identified as-far-as is reasonably foreseeable, each risk is appropriately assessed in terms of likelihood

		and consequence, ii. Develop risk response plan and assessing adequacy of responses, appropriate operational controls are implemented to maximize opportunities and mitigate against potential losses, iii. Ensure that all material risks are monitored as a whole on at least a quarterly basis, iv. Ensure that Entity's risk management methodology is undertaken at the commencement of any substantial project/program or major undertaking by the entity and is reviewed throughout the life of the project/program or undertaking v. Establish mechanisms and tools, which shall include constituting Risk Identification Teams, aimed at realizing risk management responsibilities
6.	Head of Department/ Unit	Heads of Units are Risk Owners for their functions, they are responsible for managing risks affecting their daily operations and ensuring that risk management systems maintained remain robust and appropriate in the light of material changes to the business model, compliant with changes in the external environment and fulfils the requirements articulated in the risk management framework. Specific responsibilities include the following:

t with changes model, complianin the external environment and
uirements articu fulfils the reqdated in the risk management
fic responsibilitie framework. Specis include the following:

model, compliant with changes in the external environment and fulfils the requirements articulated in the risk management framework. Specific responsibilities include the following:

t with changes model, complianin the external environment and
isk management uirements articu fulfils the reqdated in the rt
wing: fic responsibilitie framework. Specis include the follo

environment and model compliant with changes in the external l

		Audit Committee; iv. Establish an annual review cycle which evidences that the risk control framework is effectively established and maintained across the entity; v. Coordinate the Risk Framework as necessary across the entity and gaining input from relevant stakeholders; vi. Ensure that the requirements of the control framework are communicated effectively and providing support, guidance and training to help the embedding of the risk management practices within the business; vii. Define and establish key metrics and other measures for reporting and monitoring exposures against risk appetite; viii. Promote risk awareness within their operations; ix. Report on the overall risk profile (including but not limited to the key metrics) to the Management Risk Committee via the risk profile report and other periodic and ad-hoc reporting as required by the entity Risk Management Framework; x. Ensure that control failures and breaches of policies within their risk's control framework are reviewed and reported by the business (including escalation to the Director, Risk Management Coordinator and Management Risk Committee that appropriate action plans are in place to bring risk exposures back in line with the entity risk appetite; xi. Prepare risk analysis worksheets on risks concerning their area of operations (quarterly); xii. Oversee remediation of control weaknesses relating to their risk, ensuring that these are set up and resourced appropriately by the business and tracked to conclusion; and xiii. Monitor Management Information (MI) to verify that the control framework is implemented and operating effectively across the business and to ensure consistency of policy application across the

		entity.
7.	Risk Management Coordinator (RMC)	The Risk Management Coordinator shall be charged with the responsibility of orchestrating the whole risk management process and shall also operate and manage the entity's risk management database. He or she shall report functionally to the Chief Budget Manager. The MRC shall have a broad knowledge encompassing a range of operational and technical issues of both generic and specific risks relevant to the entity. The MRC shall have the following responsibilities: i) Develop and implement the Risk Management Plan; ii) Champion of risk management at strategic and operational levels; iii) Facilitate the identification, analysis and evaluation of risks within the entity; iv) Collect and collate risk information from Process Owners; v) Initiate the review of Risk Management Policy and Strategy ; vi) Process information to generate a risk register and populate the risk management data base; vii) Present risk management reports at risk review meetings including updating and regularly reporting any material items in the Risk Register to the CBM and the Management Risk Committee; viii) Report on Quarterly basis to the Audit Committee; and annually to the Board on the overall effectiveness of the Risk Management Framework, Policy and Strategy; ix) Coordination of the quarterly risk identification exercise undertaken by unit/function managers; x) Pre-identification of risk categories and provide these to management to aid in their thinking of the various types of risks; xi) Implement initiatives to continually strengthen entity's Risk

		Management Framework and risk culture by ensuring there are robust processes in place to identify, communicate and manage material risks across the entity; xii) Promote risk management awareness via education to management and staff as required; xiii) Coordinate the various functional activities which advise on Risk Management issues within the entity; and xiv) Develop risk response processes, including contingency and business continuity programs.
8.	Internal Audit	Internal Audit as "third line of defense" functionally reports to the Audit Committee and administratively reports to the CBM. The Internal Audit will be responsible for: i. Independently evaluating the effectiveness and efficiency of selected risk management and internal control and compliance practices; ii. Coordinate its program with other entity 'assurance' activities such as Risk Management, Monitoring and Evaluation, Compliance and Legal units iii. Assist in monitoring and evaluating the effectiveness of entity, risk analysis and monitoring program; iv. Liaise and consulting with the RMC and the Management Risk Committee (MRC) on selected risk and compliance matters, which include attendance at their meetings on invitation; v. Coordinate risk reporting to the Audit Committee, Auditor General and other external auditors as the case may be.
9.	Staff and contractors	All staff and contractors must be aware of their responsibilities in managing risk in their day-to-day roles. This includes: i. Carrying out their roles in accordance with all policies and

		procedures; ii. Identifying risks and reporting these to relevant risk owners in accordance with reporting protocols; iii. Report ineffective or inefficient controls; iv. Be aware of the risks that relate to their roles and activities; v. Ensuring that his or her work environment and practices reflect good risk management standards in order to protect their own health and safety as well as the health and safety of others; vi. Observe and inform Managers or Team Leaders of any specific public risk; vii. Familiarize themselves with all risks (current and potential) that relate to their area of responsibility and actively support and contribute to risk management initiatives; and iii. Report all accidents, incidents and near misses on timely basis.

APPENDIX I: EXAMPLE OF RISK REGISTER TEMPLATE

ENTITY'S NAME RISK REGISTER

This template should be customized to each entity to reflect its specific nature and environment. The risks provided in the template are those found in most organizations and not necessary present in each entity.

Risk category	Risk Description	Objective affected	Plausible Risk source	Likelihood	Impact	Risk ranting	Control	Treatment option
Strategic Risks	Inability by the entity to achieve its Mandate	Mandate	Constitution, Law establishing the Entity Governance, Strategic Plan	Unlikely	Catastrophic	Medium 2*5= 10	The Entity Strategic Plan with SMART targets and Output Governing Board and Oversight Organs Monitoring and Evaluation system	
	Inability by the entity to accomplish its Mission	Mission	Law establishing the Entity Governance, Strategic Plan Operational Plans	Possible	Major	Medium 3*4= 12	Clearly defined mission statement and strategies and tactics to realize it Strategic and Operational	

Risk category	Risk Description	Objective affected	Plausible Risk source	Likelihood	Impact	Risk ranting	Control	Treatment option
							Plan Executive management to drive the Entity towards accomplishment of its mission Governing Board and Other Oversight Organs	
	Inability for the entity to realize its Vision	Vision	Law establishing the Entity Governance, Strategic Plan Operational Plans	Likely	Major	High 4*4= 16	Clear vision Committed Management team with required resources Governing Board and Other Oversight Organs	
	Undefined or unclear strategic vision Strategic plan not	Strategic objectives	Governance Structure, Executive Management	Likely	Major	High 4*4= 16	Budgeting and Planning Committee Monitoring	

Risk category	Risk Description	Objective affected	Plausible Risk source	Likelihood	Impact	Risk ranting	Control	Treatment option
	implemented		Planning and Monitoring				and evaluation Function Regular reviews Approval processes Internal Audit External Audit	
Operational	Lack of required Financial Resource		Planning and Budgeting Resource Mobilization Investment Plans	Likely	Catastrophic	Extreme 4*5= 20	Resource mobilization Budget Committee Investment Committee Financial Rules and Regulations Monitoring and evaluation Budget execution reporting Expenditure control	

Risk category	Risk Description	Objective affected	Plausible Risk source	Likelihood	Impact	Risk ranting	Control	Treatment option
							Approvals	
	Lack of sufficient Human Resource		Recruitment Training Performance Evaluation				Staff Rules and Regulations Training policy Appraisal system Career development plan Workload analysis Competence and skill development plan	
	Lack of needed Technology		**Infrastructure**- hardware and software and Networks **People**- Knowledge and competences Protocols- Conventions, Agreements etc.					

Risk category	Risk Description	Objective affected	Plausible Risk source	Likelihood	Impact	Risk ranting	Control	Treatment option
	Lack of required Information/data		Source Quality Quantity Timing					
Compliance	Internal requirements		Rules and Regulations Policies and Procedures Guidelines and plans					
	External Requirements		Laws Regulations Standards Protocols					
Planning and Performance	Inaccurate expenditure forecasting Inaccurate revenue forecasting Over/ under spending budget allocations							
Human Resource	Inability to attract and retain staff/ Staff turnover Job roles/ accountabilities unclear							

Risk category	Risk Description	Objective affected	Plausible Risk source	Likelihood	Impact	Risk ranting	Control	Treatment option
Procurement	Non-delivery of goods and services by supplier Delivery of goods that are in line with specifications Overpayment for goods and services							
Financial Management	Wasteful or unproductive expenditure							
Asset Management	Failure to maintain/ repair assets Failure to maintain assets/ equipment Un-authorized use/ Misuse of fleet vehicles Underinsurance/ Assets not insured							
Fraud and Corruption	Unethical business practices							

Risk category	Risk Description	Objective affected	Plausible Risk source	Likelihood	Impact	Risk ranting	Control	Treatment option
Environmental and Natural Disasters	Pandemic and Infectious Disease Outbreak Failure of/ No fire suppression system		Fire, flooding bushfires thunders					
Political	Strikes and workplace unrest Sexual harassment/ violence Terrorist attack/ Bomb threat etc.							