Republic of Rwanda

Ministry of Education

Risk Management Policy and Procedures

Year 2021

TABLE OF CONTENTS

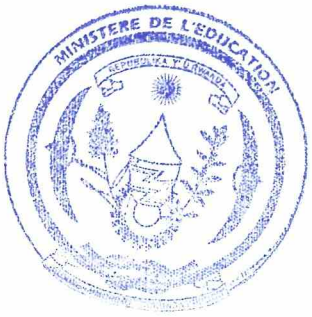
LIST OF TABLES

LIST OF FIGURES

APPENDIX

ACRONYMS AND ABREVIATIONS

AC	Audit Committee
AS/NZS	Joint Australian New Zealand International Standard
CBM	Chief Budget Manager
GoR	Government of Rwanda
ISO	The International Organization for Standardization
MINEDUC	Ministry of Education
NST 1	National Strategy for Transformation
RMC	Risk Management Coordinator
RR	Risk Register



FOREWORD

I am glad to release the Risk Management Policy and Procedures for the Ministry of Education. The main objective of this policy is to ensure sustainable Ministry's growth and to promote a pro-active approach in planning, implementation, evaluation and reporting to ensure effective achievement of Ministry's objectives.

The aim of this policy is to provide guidance regarding management of risks; to minimize, and/or eliminate risks related to operational, compliance, planning, performance, human resources, procurement, financial management, assets management, fraud and corruption, environmental/natural disasters and political risks.

In view of the above risks, a need was felt for a suitable Risk Management Policy, the policy objective is to ensure protection of Government funds and properties and safeguarding value for money through the establishment of integrated Risk Management procedure by identifying, assessing, mitigating, monitoring, evaluating and reporting all risks, to provide clear and strong basis for informed decision making at all levels of the Ministry and to continually strive towards strengthening the Risk Management System through constant learning and improvement.

I appreciate the efforts of the Government of Rwanda through MINECOFIN for providing guidelines towards the formulation of this Risk Management Policy and Procedure. I strongly believe that with the collaboration and support of all including; Risk Management Coordination, Risk Management Committee, Directorates and Units this Risk Management Policy and Procedures will be beneficial for the Ministry's efficiency and effective operations.

Dr. Valentine UWAMARIYA
Minister of Education

TERMS AND DEFINITIONS

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 regards 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, identifying, analyzing, evaluating, treating, monitoring and reviewing risk
Establishing the context	Defining the external and internal parameters to be considered 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 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 comprehensive list of threats and opportunities foregone, 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 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

CHAPTER ONE: INTRODUCTION

The Risk management Policy is a statement of the overall intentions and direction of the Ministry related to risk management. It is central to developing a common understanding of risks and their management within the Ministry and provides the opportunity to articulate its risk management vision and to describe the benefits that it derives from managing risks.

This document includes the introduction part, risk management framework, policy and structure, risk management process and roles and responsibilities of implementers.

The policy at the minimum clearly states Ministry's purpose, objectives, scope, principles, applicability, approval and review processes.

1.1 Purpose

The purpose of this policy is to provide the guidance regarding management of risk to support the achievement of ministry's objectives to minimize and/or eliminate risks related to operational, compliance, planning and performance, human resources, procurement, financial management, assets management, fraud and corruption, environmental and natural disasters.

1.2 Objectives

The objective of this Risk Management Policy is to identify potential problems before they occur and have a response plan to address them. During implementation of the plan, we consider both internal and external risks that can hinder Ministry of Education to achieve its objectives.

1.3 Scope and Applicability

This policy shall apply to all Directorates, Units and Projects within Ministry of Education.

1.4 Effective date of the policy

This policy shall be effective on the date approved by the Minister.

1.5 Approval, review and amendments

This policy is approved by the Minister and shall be reviewed and amended when circumstances dictate or on recommendation of Audit Committee.

CHAPTER TWO:
RISK MANAGEMENT FRAMEWORK, POLICY AND STRATEGY

2.1 Risk Management Principles

The Ministry of Education has adopted AS/NZS ISO 31000: 2009 as amended to date Risk Management Standards whose Principles and Guidelines are presented below:

Table 1: Risk Management Principles

N0	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 the consideration of 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.

The Ministry Management should ensure that risk management principles are adhered to achieve its mandate.

2.2 Risk Management Framework

The Risk Management Framework is reflected in the Ministry' s Risk Management Structure as:

i. Employees will work together with Specialists or Officers/ Directors/ Director Generals / Program Managers to identify risks in their respective fields.

ii. Specialists or Officers/ Directors/ Director Generals/ will work with Risk Management Coordinator to assess and evaluate identified risks then propose treatment actions.

iii. The Risk Management Coordinator will work with the Internal Auditors to evaluate the effectiveness and efficiency of selected risk management treatment actions in relation to internal compliance and control practices.

iv. Risk Management Coordinator shall report the outcomes from iii above to the Chief Budget Manager for further orientation.

2.2.1 Developing the Risk Management Framework

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

Step 1: Risk governance structure

The Senior Management shall oversee the implementation of the risk management policy and the Chief Budget Manager shall have the responsibility to implement risk frameworks, policies and procedures. The Risk Management Committee in collaboration with the audit committee shall have the responsibility for setting risk limits within the approved risk appetite level and tolerance limits.

Departments, Directorates, Units and Projects shall work with the Risk Management Coordinator to carry out risk identification, assessment monitoring, reporting and mitigation of risks. The Internal Auditors shall independently provide the assurance on the adequacy and effectiveness of Risk Management processes within the Ministry.

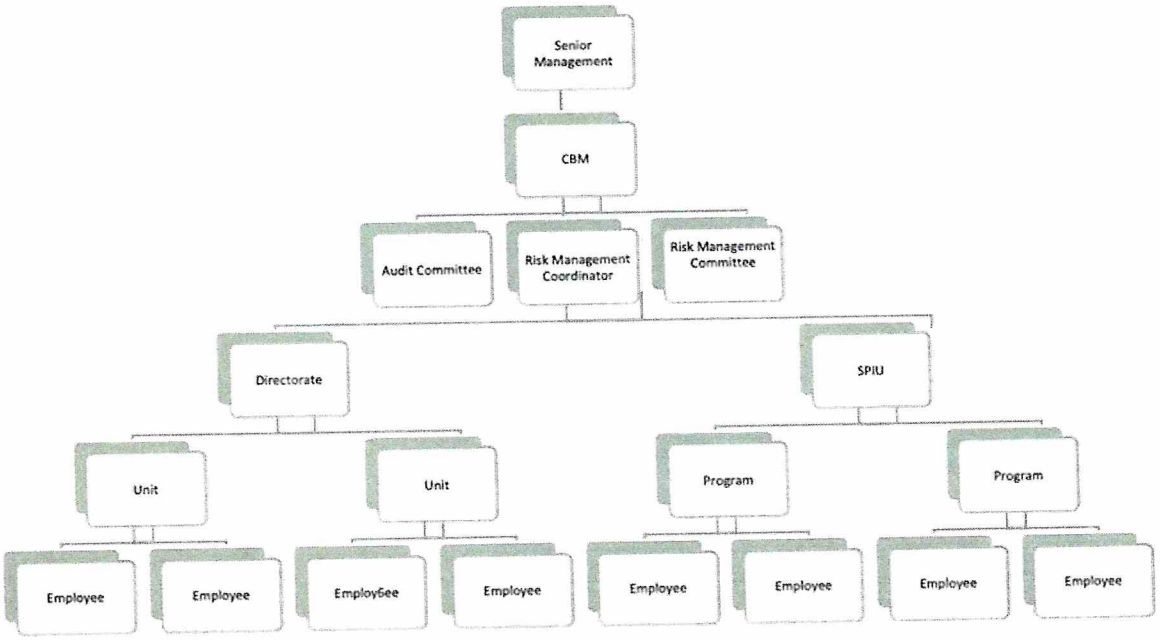


Figure 1: Risk Management Structure

Step 2: Context for risk management

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

Senior Management shall set up acceptable levels of risks for each category of risks. The Ministry risk appetite shall be determined both quantitatively and qualitatively whenever possible. The Ministry shall have zero tolerance for fraud and reputational risks. For other category of risks, the Senior Management shall decide to take either high or low risk appetite depending on the threat that the risk present.

The Senior Management shall begin with identifying values and targets, and the programs in-place for achieving them. It is within this context that the Ministry shall optimize its ability to exploit opportunities and to control or mitigate setbacks and negative occurrences.

Step 3: Approach to risk identification

Risks will be categorized by sources that include operational, compliance, planning and performance, human resources, procurement, financial management, assets management, fraud and corruption, environmental/natural disasters and political.

MINEDUC adopted the following principal approaches to identify risks:

1. Brainstorming: Heads of departments, directorates, units and projects will convene at the beginning of the financial year spearheaded by the Risk Management Coordinator to generate ideas of potential risks and remedies when delivering their duties and responsibilities.
2. Scenario analysis: Scenario analysis is a process of analyzing future events by considering alternative possible outcomes. The Ministry will employ scenario analysis techniques to identify potential risks and risk treatment plan.
3. SWOT analysis: SWOT analysis is a strategic planning technique used to help a person or organization identify strengths, weaknesses, opportunities, and threats. The Ministry will employ to identify potential risks and solutions.
4. Information gathering: The Ministry will gather information from different stakeholders and running project to identify risks that may occur during implementation. The following data collection tools will be used: Interviews, questionnaires, historical reviews and surveys.

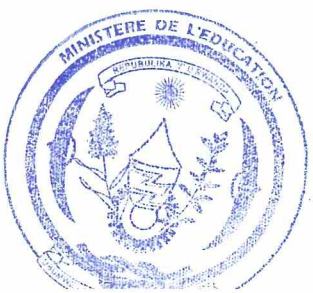
Step 4: Risk assessment matrix

To focus on key threats and opportunities foregone 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 Ministry.

Risk Management Committee in collaboration with the Audit Committee 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.

Step 5: Risk Register

Risk Register (RR) is a comprehensive list of threats and opportunities foregone 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 RR shall be used to record threats and opportunities foregone and to track actions established to address them.

The register shall record a description of the threat or opportunity foregone 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.

The Chief Budget Manager shall oversee the Ministry RR. However, it shall be maintained by the Risk Management Coordinator. Each Departments, Directorates, Units and Projects shall also maintain their RR. The Risk Management Policy shall be a living document that is reviewed and updated every 3 years.

Step 6: Rollout of the Risk Management Framework

The Ministry starts risk management process for the different offices in the Ministry at the beginning of every financial year after the approval of the budget and action plan.

Risk Management will be integrated into ministry planning process. This integration shall begin with the establishment of strategic and operational objectives/targets and deliverables. Each of these targets is assigned to an office or a Director of Unit who, with 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 Risk Management Committee, which determines whether they should be incorporated into and monitored as part of Ministry's risk register or assigned to a lower level within the Ministry.

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 Risk Management Committee and CBM on a regular basis. This shall include formal written reports.

2.3 Risk Management Strategy

Risk Management Strategies are actions, tactics deployed by the Ministry to maintain risks within the accepted tolerable levels (risk appetite) approved by the Senior Management. The Risk Management

Strategy serves to implement the Ministry's risk management policy. The Strategy outlines how the structure of responsibility and accountability across Ministry shall be developed and maintained The Ministry 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
- Integrating risk management into all Ministry activities; and
- Adopting three lines of defense model (as mentioned table 8) 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.

The risk management process is based on AS/NZS ISO 31000:2009. The figure below presents the process in summary form:

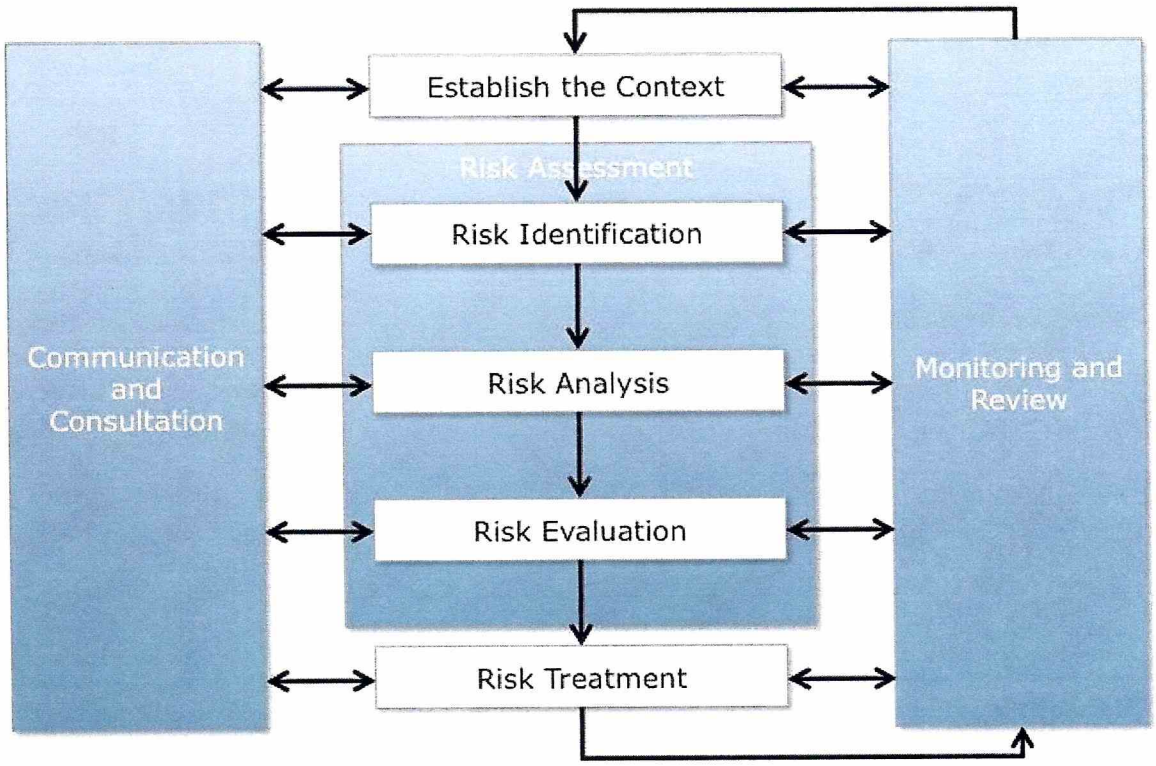


Figure 2: Risk Management Process

Source: AS/NZS ISO 31000

3.1 Establish the context

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

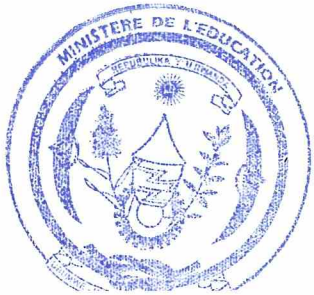
MINEDUC shall actively consider risk and document the assessment formally for any proposed program, project or initiative. It is advisable to always start by identifying the mission, goals and objectives right at the beginning to achieve the pre-determined targets.

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 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 and operational context, so that a complete picture is obtained.

3.2 Risk Identification

The second step in the risk management process will be to identify the risks that might have an impact on the objectives and operations of the Ministry. 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 Ministry's objectives. Risk identification aims 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:

Table 2: Risk identification

No	Question	Question description
1	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?
2	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?
3	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?
4	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
5	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
6	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 **measurable 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, although 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:

Table 3: Likelihood

Rating	Description	Frequency	probability to occur 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.

Table 4: 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 1 million	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 1 to 10 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 10 to 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 on budget allocated to the Directorate. The overall impact will reflect Ministry's benchmark in table 2 above.

3.3.4 Rate the level of risk

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

Table 5: Risk Matrix

←-----Impact-----→						
	5	Catastrophic/Rare 5*1=5	Catastrophic /unlikely 5*2=10	Catastrophic /possible 5*3=15	Catastrophic /likely 5*4=20	Catastrophic /almost certain 5*5=25
	4	Major/Rare 4*1=4	Major/unlikely 4*2=8	Major /possible 4*3=12	Major /likely 4*4=16	Major /almost certain 4*5=20
	3	Moderate/Rare 3*1=3	Moderate /unlikely 3*2=6	Moderate /possible 3*3=9	Moderate /likely (recruitment of incompetent staff) 3*4=12	Moderate /almost certain 3*5=15
	2	Minor/Rare 2*1=2	Minor /unlikely 2*2=4	Minor /possible 2*3=6	Minor /likely 2*4=8	Minor /almost certain (late coming at work) 2*5=10
	1	Insignificant/Rare (injury or illness due to work) 1*1=1	Insignificant/unlikely 1*2=2	Insignificant/possible 1*3=3	Insignificant/likely 1*4=4	Insignificant/almost certain 1*5=5
		1	2	3	4	5
		←----------Likelihood----------→				

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 will consist of deciding whether the risk is acceptable or unacceptable. The Ministry 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 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, programs and directorates.

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

The risk shall be regarded as acceptable or tolerable if the decision has been made not to treat it (in accordance with the next step, Step 5 'Treating the risk'). It is important to remember that regarding a risk as acceptable or tolerable does not imply that the risk is insignificant. Risks that are considered acceptable or tolerable will 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 AS/NZS ISO 31000-2009, the three steps combined; risk identification, analysis and evaluation make the risk assessment and shall be documented in the template below:

Table 6: Risk assessment

Directorate/Project											
Risk Owner											
Risk ID	**Risk Category**	**Unit Assessed**	**Unit Objective**	**Critical Success factors**	**Risk Description**	**Risk Event**	**Risk Source**	**Current Controls**	**Control Effectiveness**	**Risk Rating**	**Mana; Op**

3.5 Treat the risk

This step will ensure 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:

Step 1: Deciding if specific treatment is necessary

Decide if specific treatment is necessary or whether the risk can be adequately treated during 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.

Step 2: 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.

Step 3: 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 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 Ministry 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 (please note this does not refer to safety type risks or hazards).
- 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.

Step 4: 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.

Step 5: 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.

Table 7: Risk Treatment Plan

Area/Department										
Risk Owner										
Date Treatment Developed	Risk Category	Treatment Owner	Risk ID	Risk Description	Control Effectiveness	Risk Treatment			Monitor &Review	Implemer Stat
						Treatment Action	Responsibility	Implementation Date		

Step 6: 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.

Step 7: Assess the level of residual risk

Even when a risk has been treated and the controls are in place, the risk may not be 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

Monitor changes to the source and context of risks, the tolerance for certain risks and the adequacy of controls. The Ministry shall ensure that processes are in place to review and report on risk regularly.

To ensure structured reviews and regular reporting occurs, each Directorate shall identify a process that allows key risks within their area to be monitored. Given the diverse and dynamic nature of the Ministry's environment, it is important to be alert to emerging risks as well monitoring known risks.

3.7 Risk Reporting

Formal risk reporting is an important part of being able to demonstrate the effectiveness of the risk management program. The Ministry is required to report internally within Directorates and MINECOFIN; to achieve this, the Ministry needs to be informed about risks in a timely manner and to be able to access and reproduce those risk assessments easily.

The Risk Management Committee will share the Risk Management Report with Audit Committee for assurance. The Risk Management Coordinator will submit the risk management report on quarterly basis to the Chief Budget Manager (CBM) not later than the 30th of the next quarter. CBM will also submit Risk Management Annual Report to MINECOFIN **every 30th September.**

Formal risk reporting needs to occur via the Ministry's Risk Register or other appropriate formal report. Formal 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 Risk Management Committee for the CBM endorsement. Extreme and high risks will be overseen by Senior Management on regular basis. Risk response/treatment and appropriate action will be agreed between risk owner and RMC. Medium and low risks are to be managed, monitored, reported and reviewed by Director General and Project Coordinator.

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 Ministry, 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 are 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 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 the Ministry 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 Managers of Public Entities to establish and maintain effective, efficient and transparent systems of internal controls and risk management.

Ministry's structure, mission and mandate implies that there are risk management roles and responsibilities assigned to different Directorates and Projects with the following roles and responsibilities:

Table 8: Roles and responsibilities

SN	Function	Responsibilities
1.	The Minister	oversees the implementation of Risk Management Policy within the Ministry and its affiliated Projects
2.	Senior Management Members	i.Approve the design and implementation of risk management approaches, including the risk response, tolerance and the Risk Appetite Statement. ii.Receive and consider the Risk Management Annual Reports; ii.ensure that staff charged with Risk Management responsibilities have appropriate authority to carry out their functions and have appropriate access to SMM; iv.Approve the allocation of resources for effective management of risk; and annual Activity Plan of Risk Management Function
4.	PS/Chief Budget Manager (CBM)	i. Establish and maintain the Ministry'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 Ministry's processes; iii. Identify threats to the achievement of Ministry's objectives; ı. Analyze Cost-effective risk treatment options; ı. Put in place appropriate controls and treatment measures to manage

		identified risks; vi. review regularly, 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;
3.	Risk Management Committee (RMC)	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 on at least a quarterly basis, iv. ensure that Ministry'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
4.	Director General/Project Coordinator/Chief Digital Officer	Director Generals/Project Coordinator/Chief Digital Officer work closely with employees under them and ensure they are managing risks affecting employee's daily operations as well as that risk management systems are maintained remain robust and are compliant with changes in the external environment and fulfils the requirements articulated in the risk management framework. Specific responsibilities for Director Generals/ Project Coordinators and Chief Digital Officer include the following: i. engage in the identification of Risk Managers and allocation of specific risk management responsibilities to each such manager to include primary responsibility for managing risk falling under their scope of control on a day-to-day basis; ii. develop risk appetite / tolerance thresholds for their processes,

		procedures and operations, ensuring that these are communicated to each business area / function as applicable iii. ensure that Risk Management Committee (RMC) reviews and recommends the Directorates' Risk profile for approval by the Audit Committee and Risk Management Committee; iv. establish an annual review cycle which evidences that the risk control framework is effectively established and maintained across the Directorates and/or Projects. v. coordinate the Risk Framework as necessary across the Directorates and/or Projects 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 Directorates and/or Projects; vii. promote risk awareness within their operations; viii. report on the overall risk profile (including but not limited to the key metrics) to the Risk Management Committee via the risk profile report and other periodic and ad-hoc reporting as required by the Directorates and/or Projects Risk Management Framework; ix. ensure that control failures and breaches of policies within their risk's control framework are reviewed and reported (including escalation to the Risk Management Coordinator and Risk Management Committee)
6.	Risk Management Coordinator	The Risk Management Coordinator (**second line of defense**) shall be charged with the responsibility of implementing the whole risk management process and shall also operate and manage the Ministry's risk management database. Risk Management Coordinator shall report functionally to the Chief Budget Manager. He/She shall have a broad knowledge encompassing a range of operational and technical issues of both generic and specific risks relevant to the Ministry.

		The Risk Management Coordinator 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 Ministry; iv) collect and record risk information from Process Owners; v) initiate the review of Risk Management Policy; 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 Risk Management Committee; viii) report on Quarterly basis to the Audit Committee and annually to Senior Management on the overall effectiveness of the Risk Management Framework and Policy; ix) coordination of the quarterly risk identification exercise undertaken by the Directorates and/or Projects; 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 Ministry's Risk Management Framework and risk culture by ensuring there are robust processes in place to identify, communicate and manage material risks across the Ministry; 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 Ministry; and xiv) develop risk response processes, including contingency and continuity of programs.
7.	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 compliance and control practices; ii. Coordinate its program with other Ministry 'assurance' activities such as Risk Management, Monitoring and Evaluation, Compliance and Legal units iii. Assist in monitoring and evaluating the effectiveness of Ministry, risk analysis and monitoring program; iv. Liaise and consulting with the Risk Management Committee 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 once it is requested.
10.	Employees	All employees are the **risk champions/Owners (First Line of Defense)** and must be aware of their responsibilities in managing risk in their day-to-day duties and responsibilities. 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 this Risk Management Policy; 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. Report all accidents, incidents and near misses on timely basis.

APPENDIX I: RISK REGISTER

Risk ID	Date Raised	Unit/Project /Program Assessed	Risk Owner	Unit /Program Objective	Critical Success Factors	Risk Description	Risk event	Risk Source	Likeli hood	Impact	Risk rating	Current Control	Management Option	Treatment Plan	Treatment Plan	Risk Owner