GENDER MONITORING OFFICE
(GMO)

Risk Management Policy & Framework

NOVEMBER, 2025

Version Control

Version	Date	Update	By whom
1.00	8/7/2024	Initial Draft	GMO
1.01	29/7/2024	Final	GMO
2.00	5th September 2025	The Risk Management Committee (RMC) customised the version 1.01 in the following areas; ✓ Risk Management statement ✓ Acronyms ✓ Defining risk categories ✓ Risk management governance structure ✓ Risk management roles and responsibilities ✓ Risk Management Implementation Plan	GMO RMC & MINECOFIN
2.01			
2.02			
2.03			

Table of Contents

FOREWORD

Risk management plays a pivotal role in ensuring the effective and efficient operation of GMO. By implementing a comprehensive risk management framework, we can identify potential risks, assess their impact, and develop strategies to mitigate or minimize them. This policy outlines our commitment to managing risks and fostering a culture of proactive risk management within GMO.

The objective of our Risk Management Policy is to establish a framework that enables us to:

a) Identify, evaluate, and manage risks associated with operations, programs, projects, and processes.
b) Provide guidance on managing risks to support the achievement of GMO objectives, related to ensuring adherence to Gender Equality principles, promoting gender accountability at all levels, and combating Gender-Based Violence and related injustices.
c) Promote a risk-aware culture where all employees understand their role in managing risks.
d) Enhance decision-making by considering risk factors and their potential impact.
e) Safeguard reputation, assets, and resources.
f) Ensure compliance with relevant laws, regulations, and standards.

The GMO shall apply ISO 31000:2018 Risk Management standard in development of its Risk Management framework and implementing Risk Management process. The GMO shall use Risk Management tools to actualise a practical application of Risk Management. The Risk & Controls Self-Assessment tool shall be the basis of identifying, analysing, evaluating and treating risks. The risk monitoring tools to be used are Key Risk Indicators, Compliance Management, Incident Management and Action Tracking. The review and improvement of risk management shall apply the Risk-Based Internal Audit tool to provide independent assurance on effectiveness of Risk Management.

Regular reporting mechanisms will be implemented to provide the Management with comprehensive risk reports, including emerging risks, their potential impact, and progress in implementing risk treatment strategies.

By adopting this Risk Management Policy, GMO reaffirms its commitment to effectively managing risks and safeguarding its operations. This policy will serve as a guiding framework for all risk-related activities within the organization.

UMUTONI GATSINZI Nadine
Chief Gender Monitor
GMO

1. Acronyms and Glossary of Terms

1.1 Acronyms

GMO	Gender Monitoring Office
GBV	Gender-Based Violence
HMC	High Monitoring Council
ERM	Enterprise Risk Management
IRL	Inherent Risk Level
ISO	International Standards Organisation
KRI	Key Risk Indicator
PFM	Public Finance Management
RBIA	Risk-based internal audit
RC	Risk Champion
RCSA	Risk and Control Self-Assessment
RMC	Risk Management Committee
RRL	Residual Risk Level
SP	Strategic Plan
CBM	Chief Budget Manager
RAG	Red Amber Green escalation criteria
CSF	Critical Success Factor
IR	Inherent risk
RR	Residual Risk
RCSA	Risk and Control Self-Assessment
IIA	Institute of Internal Auditors

1.2 Glossary of Terms

Assessed unit
Refers to office, unit, function or a programme of GMO of which risk assessment is to be undertaken.

Control
Any measure or action that modifies or maintains risk, which may include; any policy, procedure, practice, process, technology, technique, method, or device. Risk treatments become controls, or modify existing controls, once they are implemented.

Control effectiveness
The extent to which a control is fit for purpose, well designed, consistent, complete, reliable and timely operated in risk mitigation.

Critical Success Factor (CSF)
The resources, inputs and capabilities that must be present in order to achieve an objective.

Event
An occurrence or incident, from external or internal sources, that affects the achievement of GMO's objectives. Events can have negative consequences, positive consequences, or both. Events with negative consequences represent threats. Events with positive consequences represent opportunities.

Inherent (gross) Risk (IR)
The exposure arising from a specific risk before any action or control has been put in to manage it.

Management organs of GMO
The organs of the Office are as follows:
1° the High Monitoring Council of the Office;
2° the Executive Secretariat;
3° the Consultative Committee.

High Monitoring Council of the Office
The High Monitoring Council is the supreme organ of the Office in the overall management and making decisions which help in the fulfilment of its responsibilities.

Near miss
An incident that didn't evolve into a consequence.

Process
Refers to a set of interrelated or interacting activities which transform inputs into outputs in order to achieve desired results.

Residual (net) Risk (RR)
The exposure arising from a specific risk after an action or control has been put in place to manage it and making the

assumption that the action or control is effective.

Risk
Risk is the effect of uncertainty of objectives.

Risk and Control Self-Assessment (RCSA)
A process used by Management to identify, measure and evaluate risks and controls.

Risk bow tie analysis
A graphical presentation of the risk event, the causes and consequences.

Risk champion
Is a staff representing an assessed unit who supports and defends risk management cause. Therefore, a champion of risk management will promote its benefits, educate the business unit's management and staff in the actions they need to take to implement it and will encourage them and support them in taking those actions.

Risk impact
The outcome of an event affecting objectives.

Risk likelihood
The chance of a risk event happening.

Risk matrix
A tool for ranking and displaying risks by defining ranges for consequences and likelihood.

Root cause analysis
Refers to the identification of *underlying causes* of identified risk events or incidents, so that the most effective control measures can be identified and implemented.

Risk criteria
It is a term of reference against which the significance of risk is evaluated. The criteria can be derived from standards, laws, policies and other requirements.

Risk assessment
The overall process of analysis and evaluation of a risk with regard to its consequence and the likelihood of being realized, and the selection of an appropriate risk response by GMO.

Risk culture
The set of shared attitudes, values and practices that characterize how GMO considers risks in its day-to-day activities

Risk driver
It is a cause or source of a risk event.

Risk indicator
This is a measurement or parameter used by management to show how risky an event or activity is. It warns of the most obvious area where problem may arise, thus the term Key Risk Indicator.

Risk owner
This is a staff who has accountability and authority to manage risk. This can be: Chief Gender Monitor, Deputy Chief Gender Monitor, Executive Secretary, Director.

Risk profile/register
A documented and prioritized assessment of the range of specific risks faced by GMO.

Risk management framework
The totality of the structures, methodologies, procedures and definitions that GMO adopts to implement its risk management processes.

Risk treatment

The set of actions that may be taken in response to a risk, which may include:

- **Transfer the risk:** This may be done by GMO asking a third party to take on the risk.
- **Accept/tolerate the risk:** Decision to not put in place further mitigation measures because the ability to take effective action is limited, or the cost of taking action may be disproportionate to the potential benefit gained.
- **Treat the risk:** Taking direct action to reduce either its potential impact or its likelihood of occurrence.

Stakeholders
The person(s) or organisation(s) that can affect, be affected or perceive themselves to be affected by a decision or activity of GMO.

Upside of risk
The potential of a risk event to generate a positive impact to the organisation.

2. Preamble

2.1 Background

The Mission of GMO

The Gender Monitoring Office (GMO) is a public institution established by the constitution of the Republic of Rwanda Official Gazette n°4 Special of 04/08/2023 of 2023, in its article 140. As stipulated in the law N° 51/2007 of 20/09/2007 determining the responsibilities, organization and functioning of the Gender Monitoring Office in Rwanda, it has legal personality, an administrative and financial autonomy and supervised by the office of the prime Minister with a mandate to monitor the respect of Gender Equality principles, promote gender accountability at all levels and fight against Gender Based Violence and related injustices.

GMO Core Values:

Value	Description
Integrity	Professionalism, moral uprightness, honesty, incorruptibility and trustworthiness
Accountability	GMO willingly takes responsibility and ownership of its actions and results.
Transparency	The work of GMO and engagement with other stakeholders and partners has to be open, professional and participatory
Equity	Promotion of inclusiveness and social justice for all will be the guiding principle in GMO's work and operations.

Responsibilities of GMO

Gender Monitoring Office/GMO has the following responsibilities:

A. In general, the Office has the following responsibilities:

1° Monitoring and carrying out evaluation on a permanent basis of compliance with gender indicators

intended to respect gender in the context of the vision of sustainable national development and serving as a reference point on matters relating to gender equality and equity;

2° Submitting to various institutions recommendations relating to the program of gender promotion in national development;

3° Monitoring the respect of the principle of gender in national development and submit to the cabinet its annual programme of action and the activity reports and reserve copies to other state organs as it is required by the law.

B. In particular, the Office has the following responsibilities:

1° Monitoring on how the fundamental principles of gender are respected in all organs at governmental, private, non-governmental and religious levels;

2° Examining and monitoring the national policy and programs intended at ensuring the promotion of gender equality;

3° Monitoring the existence of the policy, programs as well as different projects aimed at promoting gender equality, their implementation and the system of their budget allocation;

4° Ensuring the implementation of the international agreements and programmes relating to the respect of the principles of gender;

5° Fighting against Gender Based injustice and violence;

6° Advocating for the respect of gender equality at all levels;

7° Raising awareness for all institutions and the population to build a nation which respects principles of gender;

8° Disseminating national Laws and international Conventions aimed at promoting gender;

9° Providing, upon request or at own initiative, opinion on the draft laws, policy and strategy documents or any other decisions relating to gender equality;

10° Encouraging all institutions to mainstream and to respect gender equality in all their programs;

11° Carrying out research based on statistics on specific issues in the framework of mainstreaming and respecting the principles of gender and disseminating the results after analysis;

12° Developing gender awareness indicators in all sectors;

13° Identifying where there is Gender Based inequalities in all national bodies and providing a way to rectify them;

14° Proposing to the relevant administrative institutions the strategies to be taken in order to avoid violations of gender equality;

15° Advising all institutions to respect the principles of gender equality;

16° Building and increasing the capacity of the office and its staff.

Background of Risk Management in GMO

Risk Management at GMO is viewed as part of the Public Finance Management (PFM) reforms in areas such as accounting reforms, Audit reforms and Governance reforms. Article 20.7 of Organic law n° 002/2022.OL of 12/12/2022 on public finance management requires the Chief Budget Manager to establish and maintain effective, efficient and transparent systems of internal controls and risk management.

Risk Management is key to the GMO in achieving effective management of public resources, reducing surprises, formalizing risk management processes and introduce a formal structure for risk management. Risk Management is necessary to enable the GMO to be able to categorise risks that the Office may face, rank them in order to prioritise and mitigate key risks.

Methodology of Preparing the Policy

This policy was developed through reference to applicable laws and regulations, guidelines, standards, consultative engagement with the GMO Management and the Risk Management Committee.

3. Objectives, Scope and References of GMO Risk Management Policy

3.1 Objectives of the Policy

The specific objectives of this policy are to establish:

i. effective risk management practices in all aspects of GMO activities;
ii. a framework of early identification and alignment of risks to the respective GMO's objectives they are affecting;
iii. objective tools of assessing, measuring and monitoring of all GMO's risks;
iv. a risk criteria and tolerance levels against which GMO risks will be evaluated;
v. a methodology of developing risk treatment strategies that are cost effective and efficient in reducing GMO's risks to acceptable levels;
vi. a process of providing accurate risk information through timely reporting for effective decision making;
vii. an appropriate risk governance and management structure for supporting the risk function in GMO.

3.2 Scope of the Risk Management Policy

This policy shall cover:

i. High Monitoring Council, Executive Secretary Office; Unit, Staff and processes within GMO operations;
ii. Planning, Reporting & decision-making processes.

3.3 References for the Risk Management Policy

The policy has been framed in line with the following risk management and governance standards, directives and guidelines:

i. Most current Ministry of Finance and Economic Planning Risk Management Guidelines: provides risk management guidelines for the public sector in Rwanda,
ii. Most current ISO 31000, Risk management – Principles and guidelines: provides principles, framework and a process for managing risk,
iii. Organic law on Public Finance Management,
iv. Most current Public Finance Management laws and Ministerial Order,

4. Principles of Risk Management at GMO

The Risk Management practices at GMO are based on the following principles.

4.1. Integration

GMO adopts a risk-based management approach that will cut across and integrate all its activities including but not limited to:

a. Offices, Unit, Functions, Staff, processes and programmes/projects within GMO operations;

b. Planning, Reporting & decision-making processes.

4.2. Structured

GMO shall adopt a systematic approach to risk management that contributes to consistent and comparable results.

4.3. Comprehensive

GMO shall adopt a complete and exhaustive approach to risk management that shall be applied in all areas under the scope.

4.4. Customized

GMO Management shall customize risk management framework and processes to fit the organization, in particular, its risk profile, culture and risk criteria taking into consideration its external and internal context related to its objectives.

4.5. Inclusive

GMO shall adopt a decentralized approach to risk management that advances appropriate and timely engagement of all staff, stakeholders and partners by enabling their knowledge, views, and perceptions to be considered. The institution recognizes that risk management is the responsibility of everyone in the institution.

4.6. Dynamic

GMO recognizes that risks can emerge, change, or disappear as an organization's external and internal context changes. As such, the institution shall develop a risk management

framework that anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.

4.7. Best available information

The inputs to GMO risk management approach are based on the best available historical and current information, as well as on future expectations. GMO's Risk Management Framework shall clearly take into account any limits and uncertainties associated with such information and expectations. GMO shall also ensure information is timely, clear, and available to relevant stakeholders and partners.

4.8. Human and cultural factors

GMO recognizes human behaviour as an essential aspect of organizational culture that significantly influences risk management at all levels and stages; hence it shall consider the effects of such aspects in GMO risk management processes.

4.9. Continual improvement

GMO commits to a continuous learning, review and improvement of its risk management framework and processes, so as to maintain a strong, relevant and best practice risk management framework.

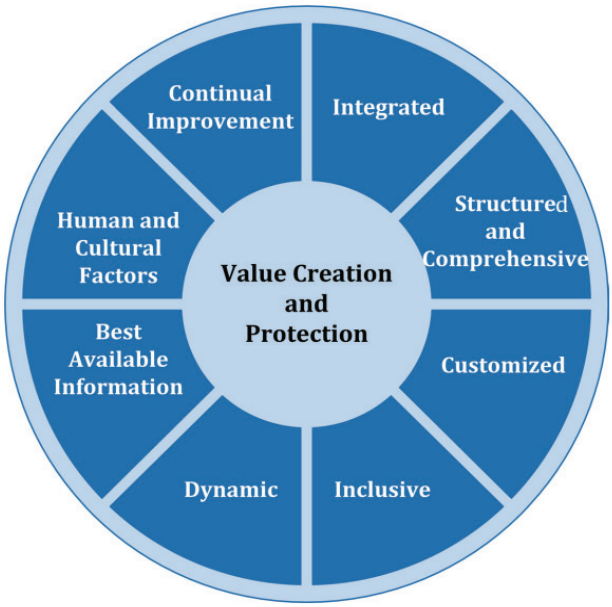


Figure 1. GMO Risk Management Principles

5. Risk Management Framework

The purpose of the risk management framework is to assist GMO to integrate risk management into its processes, activities and functions. The effectiveness of risk management depends on its integration into the governance of GMO including decision-making which requires support from stakeholders.

5.1 Risk and Risk Management as it applies to GMO

5.1.1 Risk

Risk is the effect of uncertainty on GMO objectives.

An **effect** is a deviation from the expected. It can be positive, negative or both and can address, create or result into opportunities and threats.

Uncertainty: is the state, even partial, of deficiency of information related to understanding or knowledge of an event, its consequence and likelihood.

Objectives: can have different aspects (such as financial management, public service administration, employment promotion goals) and can apply at different levels (such as strategic, department, unit, project or process).

5.1.2 Risk Management

Risk Management is coordinated activities to manage the effect of uncertainty on GMO's objectives.

Risk Management and Enterprise Risk Management (ERM) shall be used interchangeably at GMO.

5.2 GMO Risk Management Framework

GMO risk management framework is anchored on Leadership and Commitment based on ISO 31000: 2018 Risk Management Standard. This is to ensure its integration into the governance of GMO including the decision-making process. The components of GMO framework shall encompass integrating, designing, implementing, evaluating and improving risk management across the organisation as depicted in figure 2 below.

Figure 2. GMO Risk Management Framework

5.2.1 Leadership and Commitment

GMO High Monitoring Council (HMC) shall ensure that risk management is integrated into all GMO's activities and shall be accountable for overseeing risk management.

GMO Executive shall demonstrate leadership and commitment by:

i. Issuing a policy that establishes a risk management approach, plan or course of action;
ii. Ensuring that the necessary resources are allocated to managing risk;
iii. Assigning authority, responsibility and accountability at appropriate levels within GMO;
iv. Ensuring that risks are adequately considered when setting the GMO's objectives; and
v. Understanding the risks facing the GMO in pursuit of its objectives.

GMO Management is accountable for managing risks.

GMO Management shall demonstrate leadership and commitment by:

i. Customising and implementing all the components of this framework;
ii. Ensuring that systems to manage such risks are implemented and operating effectively;
iii. Ensuring such risks are appropriate in the context of the GMO's objectives; and
iv. Ensuring that information about such risks and their management is properly communicated.

5.2.2 Integration

Integrating risk management into GMO shall be a dynamic and iterative process, and shall be customized to GMO's needs and culture. GMO Risk management shall be a part of, and not separate from, GMO purpose,

governance, leadership and commitment, strategy, objectives, programs, projects, services and operations.
Risk Management shall be integrated into GMO organisational structure and be integral to accountability and oversight roles in its governance processes.

5.2.3 Design

GMO risk management framework shall be designed by thorough examination and understanding its external and internal contexts such as contractual relationships, interdependencies, organisational structure, information flow among others.

GMO HMC shall ensure the design of GMO risk management framework is documented in the risk management policy with clear assigned roles, authorities, responsibilities and accountabilities at all levels of GMO management. Individuals who have accountability and authority to manage risks must be identified.

GMO Executive Secretary shall develop and adopt a Risk Communication and Consultation plan to ensure timely and relevant risk information collection, collating, synthesising and sharing as appropriate and that feedback is provided and improvements made.

GMO Executive shall ensure allocation of appropriate resources for risk management every year through budgetary allocation to cover:

i. Development of people, skills, experience and competence in risk management;
ii. Tools, Information and knowledge management system to support risk management;
iii. Professional development and training of core team.

5.2.4 Implementation

GMO Management shall implement the risk management framework by:

i. Developing an appropriate plan including time and resources;
ii. Identifying where, when and how different types of decisions are made across the GMO, and by whom;
iii. Modifying the applicable decision-making processes where necessary;
iv. Ensuring that the GMO arrangements for managing risk are clearly understood and practised.

5.2.5 Evaluation

GMO Management shall evaluate the effectiveness of the risk management framework by:

i. Periodically measuring risk management framework performance against its purpose, implementation plans, indicators and expected behaviour;
ii. Determining whether the Risk Management framework remains suitable to support achieving GMO objectives.

5.2.6 Improvement

GMO Management is committed to maintaining a robust, relevant and good practice risk management principles adapting to internal and external changes. As such, GMO Management is committed to continually improving the suitability, adequacy and effectiveness of the Risk Management Framework and the way risk management processes are integrated.

Through a Plan–Do–Check–Act model of continual improvement, GMO Management shall be undertaking, gap analysis, benchmarking exercises, routine reviews and comparative analysis to enhance efficiency and effectiveness of risk management in the Ministry.

5.3 GMO Risk Management Process

GMO risk management process as illustrated in figure 2, shall involve systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context, risk assessment, risk treatment, monitoring & review and recording & reporting. The risk management process shall be an integral part of management and decision-making that shall be integrated into the organisation structure, all operations and all processes of GMO either at strategic, operational, programme or project levels.

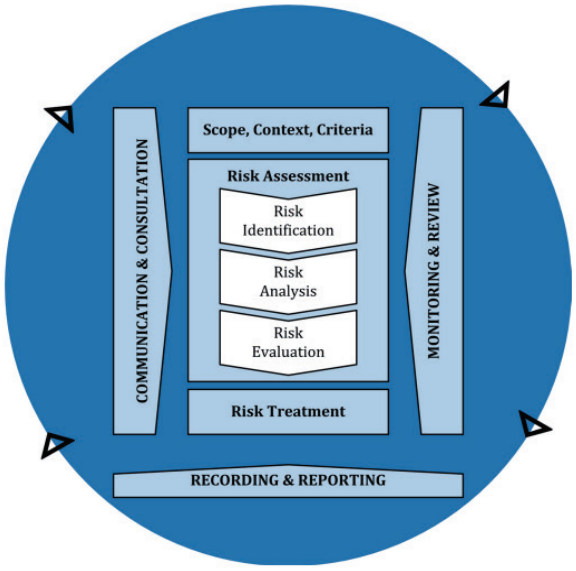


Figure 3. GMO Risk management process

5.3.1 Communication and consultation

GMO risk management process shall involve communication and consultation with stakeholders. Communication shall seek to promote awareness and understanding of risk, whereas consultation shall be obtaining feedback and information to support decision making.

GMO risk management process of communication and consultation shall:

i. Bring different areas of expertise together for each step of the risk management process;
ii. Consider different views when defining risk criteria and when evaluating risks;
iii. Provide sufficient risk information to facilitate risk oversight and decision-making;
iv. Involve all those affected by risk to build sense of inclusiveness and risk ownership.
v. Shall enhance risk management knowledge transfer to relevant stakeholders through training and capacity building.

5.3.2 Scope, Context, Criteria –

GMO Management shall establish scope, context and criteria so as to customize and structured risk management process in all activities.

In defining the scope, the Management shall consider different levels of application such as strategic, operational, programme, project or other levels and clearly define relevant objectives at the various levels while ensuring their alignment with organizational objectives.

The context of GMO risk management process shall be established from understanding the external and internal environment in which it operates and shall reflect the specific environment of the activity to which the risk management process is being applied.

GMO risk management process shall specify the amount and type of risk that GMO may or may not take relative to its objectives and shall define the criteria to evaluate the significance of risk to support decision making process. This shall be defined in GMO Risk Criteria. The Risk Criteria shall be customized GMO and shall reflect its values, objectives and resources taking into consideration its obligations and views of stakeholders.

5.3.3 Risk assessment –

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

i. **Risk identification** –

GMO shall identify where, when, why, and how events could prevent, degrade, delay, or enhance the achievement of the corporate's objectives. Risk identification shall cover all risks whether or not their sources are under GMO control or not.

ii. **Risk analysis** –

GMO shall analyze risks identified to comprehend their nature, characteristic and level of risk. Risk analysis shall entail:

a) Risk sources,
b) Consequences,
c) Likelihood,
d) Events and Scenarios,
e) Controls and their effectiveness.

Risk analysis shall be undertaken with varying degree of detail and complexity depending on the purpose of the analysis, availability and reliability of information and resources available.

iii. **Risk evaluation –**

GMO shall evaluate risks in order to support decisions by comparing the results of the risk analysis with the established risk criteria to determine where additional action is required.

The decisions available to the risk owners are:

a) Do nothing further,
b) Consider risk treatment options,
c) Undertake further analysis to better understand the risk,
d) Maintain existing controls,
e) Reconsider objectives.

The outcome of risk evaluation shall be recorded, communicated and validated at appropriate levels of the organization.

5.3.4 Risk Treatment –

GMO shall apply risk treatment to select and implement options of addressing risk. Selection of the most appropriate risk treatment option(s) shall involve balancing the potential benefits derived in relation to the achievement of the objectives against costs, effort or disadvantages of implementation.

Options available to GMO risk owners for risk treatment are:

a) Avoid the risk by deciding not to start or continue with the activity that gives rise to the risk;
b) Taking or increasing the risk in order to pursue an opportunity;
c) Removing the risk source;
d) Changing the likelihood;

e) Changing the consequences;
f) Sharing the risk;
g) Retaining the risk by informed decision.

GMO Management shall ensure adequate monitoring and review of risk treatment implementation to give assurance that the different forms of treatment become and remain effective and shall monitor any new risks that may arise from treatment. This shall be achieved by preparing and implementing a Risk Treatment Plan. The Risk Treatment Plan shall specify how the chosen treatment options will be implemented and shall be integrated into the management plans and processes.

5.3.5 Monitoring and Reviewing –

GMO Management shall implement a monitoring and review process including planning, gathering and analyzing information, recording results and providing feedback throughout all the stages of the risk management process.

The results of monitoring and review shall be incorporated throughout GMO performance management, measurement and reporting activities.

5.3.6 Recording and Reporting –

GMO Management shall implement an appropriate management system of recording and reporting risk management process and outcomes. The system shall:

i. Communicate risk management activities and outcomes across the organization;
ii. Provide timely information for decision-making;
iii. Improve risk management activities;
iv. Assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

6. Risk Criteria

GMO High Monitoring Council shall specify the amount and type of risk that it may or may not take, relative to the objectives and define criteria to evaluate the significance of risk to support decision making process. The risk criteria shall reflect the GMO's values, objectives and resources and be consistent with policies and statements on risk management.

The risk criteria will be determined for each major risk category. The risk criteria shall be dynamic and shall be continually reviewed and amended if necessary.

The risk criteria of GMO shall use a combination of Likelihood and Consequence of risks in a 5x5 matrix (heat map) and risk indicators of major risk categories. The impact and likelihood are each assessed on the scale of 1 to 5 by referring to the descriptions shown on the GMO risk matrix while the risk level of these two numbers will range from 1 to 25.

The Risk Criteria shall be developed as a separate detailed document, and shall be read/ applied together with Risk Management Policy.

The components of the Risk Criteria document are:

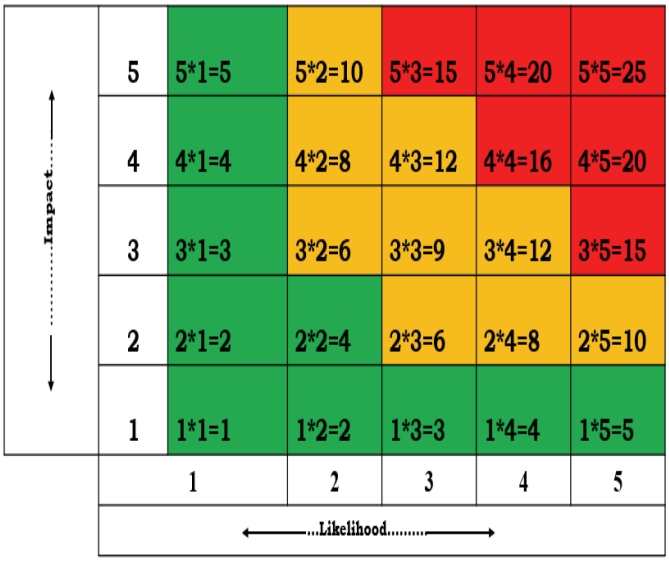
i. Define 3 colour codes of Red, Amber, Green (RAG), which will be used to determine whether a risk at GMO is acceptable or not, whether it will be treated and to what level it should escalate.
ii. **Likelihood scale** which is a tool to measure and rank the probability of a risk occurring at GMO, on a scale of 1 to 5.
iii. **Impact scale** which is a tool to measure and rank the impact a risk would have if it occurred at GMO, on a scale of 1 to 5.
iv. **A 5x5 matrix** which displays and positions GMO risks in terms of likelihood and impact.
v. **Risk tolerance** which is articulated by way of key risk indicators for each of the major GMO

risk categories. GMO Management shall set quantitative triggers for acceptable (tolerated) levels for each risk indicator, and unacceptable levels that cannot be tolerated.

vi. Maximum acceptable variation on expected performance levels or targets.

6.1 GMO Risk Matrix

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.

6.2 Factors to be considered in setting risk criteria

When setting the risk criteria for GMO, the High Monitoring Council shall consider the following:

i. **The nature and type of uncertainties that can affect outcomes and objectives:** this shall be done by defining and categorizing the various risk types GMO is exposed to;

ii. **Consequences and likelihood of risks:** this shall be done by using and considering appropriate scaling tools and levels to determine and measure the impacts and probabilities of risks;

iii. **Time-related factors:** the age, periods, cycles, frequencies, shelf-lives, seasons, past, present and future aspects of risks and its associated treatment controls shall be considered in the Risk Criteria;

iv. **Consistency in use of measurements:** to ensure

reliability and uniformity when reporting on risk matters, a consistent measurement approach shall be adopted, and any exemptions and exclusions shall be expressly stated;

v. **Determination of risk levels:** the risk levels shall be determined by defining the appropriate risk zoning / ranking rules and appropriate risk matrix.

vi. **Multifaceted risk approach:** a compound approach, interlinking and combining various risk sources and risk effects shall be considered to define the overall risk levels;

vii. **GMO's capacity:** the risk criteria shall consider GMO's overall capacity on its ability to manage risks and this shall not be limited to financial, staff, policies, processes and equipment.

6.3 Steps for setting risk criteria

When setting the risk criteria for GMO, High Monitoring Council shall consider the following:

Step 1: Risk Zones:

GMO shall adopt Red, Amber and Green colour codes to describe risk zones and define the escalation and response for risks in each zone.

Step 2: Setting a boundary on the risk matrix (likelihood and consequence):

GMO shall use a 5 x 5 matrix to identify risk ratings. The Red, Amber and Green areas in the matrix shall be established and this shall determine the risk boundary based on colour zone (as described in clause 6).

Step 3: Likelihood scale:

GMO shall articulate meaning and representative measures to a scale of 1 to 5 to reflect the ranking of probability of a risk occurring. The likelihood of the risk occurring will be described as rare, unlikely, possible, likely, or almost certain.

Step 4: Impact scale:

GMO shall articulate meaning and representative measures to a scale of 1 to 5 to reflect the ranking of a risk impact if it occurred at GMO. Therefore, the consequences or potential impact if the risk event occurred shall be described in

GMO as insignificant, minor, moderate, major or catastrophic.

Step 5: Risk Categories Tolerable limits:

GMO shall articulate this by way of Key Risk Indicators for each of the major risk categories identified in the Risk Management Policy. GMO shall set quantitative triggers for the lowest acceptable (tolerated) level for each risk indicator, and the unacceptable levels that cannot be tolerated.

Step 6: Performance indicators:

The performance indicators of GMO shall be scaled by setting quantitative triggers for lowest acceptable (tolerated) performance level, and the unacceptable performance levels that cannot be tolerated. Alternatively, this can be by defining the maximum acceptable variation on strategic objectives of GMO.

6.4 Risk Criteria Zones

GMO shall use the 3-colour concept, Red, Amber and Green (RAG) for measuring and monitoring risks and determining levels of escalation and the urgency of actions that are required.

The required escalation and actions required for each zone are as follows:

Table 1. Risk Actions and Escalation Points

Risk Actions and Escalation Points				
Risk Zone	**Zone Description**	**Meaning**	**Action required for risk**	**Risk Escalation**
15-25	**Red-High/ Extreme**	**Unacceptable Risks** that require urgent or immediate attention	**Immediate/Urgent action** required. Investigate and take steps to mitigate or avoid within a specified **short-term** period, i.e. **1 Month**	All Red risk matters are escalated to the **Risk Management Committee by CBM and Risk Owners**. Risk Management Committee deals with risks in both red and amber risks

				escalated from Risk Owners. Those that are not resolved satisfactorily are escalated to the High Monitoring Council by **Chairperson of the Risk Management Committee**.
6-12	**Amber-Medium**	**Tolerable Risks** but action required to avoid a red status	**Weighted action** required- Risks will be treated as long as the costs do not outweigh the benefits. As Low as Reasonably Practicable (ALARP)* Investigate and take steps to mitigate or avoid within a specified **medium-term** period, i.e. **3 Months**	Must be addressed by the risk owners (**Heads of assessed unit**) and escalated to the **Risk Management Committee** where there are no sufficient mitigations.
1 – 5	**Green – Low**	**Acceptable risks**	**No actio**n required. May only require periodic **monitoring.**	Monitoring within the Office, unit, function or a programme

*ALARP stands for 'As Low as Reasonably Practicable' refer to ISO 31010 (Risk Assessment)

7. GMO Risk Categorisation

GMO principle on integration of risk management requires that risk management be integrated in all management practices. Whereas this overall policy provides the risk methodology to be applied in each of the risk categories, the uniqueness of risks requires that each risk category be addressed considering specific best practices standards and guidelines but within the overall methodology.

Figure 4 below provides the policy framework for GMO.

Each of the risk categories shall be assigned a function to integrate in their management practice. The management function shall develop a stand-alone policy or incorporate the specific risk management methodology in its already existing policies and take into consideration best practice standards and guidelines to address the specific risk category.

GMO is exposed to a wide range of risks, which can fit into any of the risk categories below:

Figure 4. GMO Risk Management Policy Framework

i. **Operational Risk**: – It is the risk of loss resulting from inadequate or failed internal process, people, system, technology or from external events.

ii. **Strategic Risk**: - The risk of a) Choosing and continuing to follow sub-optimal strategies to meet objectives, b) Not executing the strategies successfully, and c) Changing the business-as-usual risks differently from expected.

iii. **Political Risk: -** is the risk arising from political decisions, events, or conditions that significantly affect the GMO.

iv. **Fraud/corruption Risk:** - the risk that a perpetrator commits an act using deception and/or acts contrary to the interest of GMO and abuses position of trust in

order to achieve some personal gain.

v. **Compliance risk**: is the exposure to legal penalties, financial forfeiture and material loss that GMO faces when it fails to act in accordance with laws, regulations & standards, internal policies or prescribed best practices as set forth by the competent authority. Includes contract risks (negative outcomes arising from agreements or contracts between parties).

vi. **Information Security Management Risk**: - is the potential that a given threat will exploit vulnerabilities to cause loss or damage to an information asset or group of information assets directly or indirectly to GMO or public sector entities. This risk includes Cybersecurity risk (the potential for unauthorized use, disclosure, damage or disruption to assets through the use of technology) and Data protection risk (threats or vulnerabilities that could compromise the confidentiality, integrity, or availability of sensitive data) and personal data.

vii. **Occupational Safety & Health risk:**- is the risk of harm or adverse health effects on workers/employees as a result of workplace hazards leading to injuries, illnesses, and even fatalities.

viii. **Gender-Based Violence (GBV) Risk -** refers to a classification of risks related to acts of violence directed at individuals based on their gender, gender identity, or gender expression. These risks include the threat, attempt, or actual use of physical, sexual, psychological, or economic harm that disproportionately affects women, girls, and gender-diverse individuals.

ix. The **Gender Mainstreaming Risk -** refers to a classification of risks that arise when gender considerations are not properly integrated into the planning, design, implementation, and evaluation of policies, programmes, or projects. These risks can result in unintended gender inequalities, exclusion of certain groups, or ineffective outcomes due to the failure to account for different needs, roles, and impacts based on gender.

NB: The precise slotting of individual factors under each category is less important than the recognition that Risk Management covers all categories and all material risk factors that can influence the organization's value.

8. GMO Risk Management Methodology

GMO Risk Management methodology seeks to operationalise the GMO Risk Management process as adopted under ISO 31000: 2018 Risk Management standard. It also seeks to achieve the structured, comprehensive and customised principles of Risk Management in GMO by developing standard and practical tools that provide the how to implement GMO Risk Management process.

The Risk Coordinator in liaison with the process owners shall operationalise risk management by applying the following risk management tools:

1. Risk and Controls Self-Assessment (RCSA)
2. Key Risk Indicators
3. Incident Management
4. Action Tracking
5. Compliance Management
6. Risk-based Internal Audit

These tools are explained in section 9.1 below. The frequency of review of RCSA outcomes will be risk-driven, responsive to business change and consider any regulatory or GMO specific requirements. GMO will review RCSA outcomes and monitoring tools at least annually, with Quarterly review and Periodic review depending on major emerging risks or requests or new significant projects.

Steps followed in risk management process through applying the RM tools:

1. Risk champions will conduct risk assessments by applying Risk Management tools for documentation, through a systematic process;
2. Risk Owners who have accountability and authority to manage risk, will review the output of what is developed to validate, and sign off on the risks identified, key risk indicator monitoring levels, compliance monitoring, action plans, implementation timelines and assigned responsibilities;
3. Once the Risk register and monitoring tools are

adopted, all staff with an assigned monitoring responsibility will be required to provide the actual data or status for the item being monitored. The data will be collected through template or through system alerts (if automated).

4. Risk monitoring reports will be sent to the Risk Coordinator for review and consolidation.
5. The Risk Coordinator will generate a **quarterly** GMO Risk Management Report (Appendix 1: 7 Risk Management Report) and by Directorate General/Unit.
6. The Risk Coordinator will present the GMO Risk Management Report on a **quarterly basis** to the CBM.
7. The CBM shall provide the GMO Risk Management Report to the Risk Management Committee to deliberate on top risks and thereafter produce the Executive Risk Management Report to be submitted to the High Monitoring Council and Audit Committee by the Chairperson of the RMC on **quarterly** basis and present the report in the next Senior Management meeting.
8. The CBM will present Annual Risk report to the Audit Committee annually for input to the annual risk-based audit plan.

8.1 Risk Management Operationalisation Tools

GMO shall apply the following tools to operationalize the risk management process:

8.1.1 Risk and Control Self-Assessment (RCSA)

See Appendix 1:1. Risk Register

RCSA is used to conduct adequate risk assessment consistent with the Risk Assessment (Identification, Analysis and Evaluation) and Treatment stage of the risk management process. The risk and control self-assessment specific steps will be designed to suit the risk category under consideration and shall apply the overall risk assessment and treatment process. These steps shall be included in the respective risk management sub-policies.

8.1.2 Key Risk Indicators

See – Appendix 1: 2. Key Risk Indicators

Key risk indicators shall be used to operationalise the Monitoring and review stage of the ISO31000 Risk management process. Key risk indicators shall be developed for all risks that require monitoring consistent with the risk criteria and results applied in decision making.

8.1.3 Incident Management

See Appendix 1: 5. Sample Incident register

Incident management shall be used to operationalise the monitoring and review stage of the risk management process. The Incident management tool shall act as a central system to record and manage risk incidents for detailed analysis, follow up and as a basis of data for future analysis across all functions of GMO.

8.1.4 Action Tracking

See Appendix 1: 6. Action tracking

Action tracking shall be used as central systems to record, analyse and monitor all risk management actions in GMO. This includes but not limited to:

a) Risk treatment actions;
b) Key risk indicators actions;
c) Non-compliance actions;
d) Audit actions;
e) Incident corrective actions,
f) Management actions etc.

8.1.5 Compliance Management

See Appendix 1: 3&4. Internal & External Compliance

GMO Compliance Management is a proactive system to monitor Internal Compliance (compliance with internal controls) and External Compliance (compliance with laws and regulations). It shall be used to empower risk owners to monitor compliance with risk mitigation strategies within their function.

8.1.6 Risk-based Internal Audit (RBIA)

Risk-based internal audit shall be used to operationalise the Review stage of ISO 31000 Risk management process.

RBIA shall provide **assurance** to the High Monitoring Council and Audit & Risk Committee that risk management processes are managing risks effectively, i.e. risks are being managed to be within GMO's **risk criteria**. The RBIA shall:

i. Give assurance that the **processes** used by management to **identify** all significant risks are effective;

ii. Give assurance that risks are **correctly assessed** by management, in order to prioritize them;
iii. Evaluate risk management processes, to ensure the **response** to any risk is appropriate and conforms to the GMO's policies;
iv. Evaluate the **reporting** of key risks, by Management to the High Monitoring Council;
v. Review the management of key risks by managers to ensure **controls** have been put into operation and are being **monitored**.

9. Risk Management Governance, Roles & Responsibilities

Risk governance is the system for directing and controlling the management of risk at GMO. It sets out the risk management structure and defines clear responsibilities and expectations for risk for GMO Management and staff.

9.2 Risk Management Governance Structure

Risk Management Governance consists of a 3-Lines of defence concept, as follows:

(i) **First line of defence** involves Culture, Management, Risk Champions, Staff and Internal controls. Management and staff operate GMO's business processes and therefore hold primary responsibility for the risks that the business/functional unit faces. Risk is managed in each business unit by a range of controls and risk treatments. The tone of leadership influences GMO culture and positions each of the lines of defence to function effectively.

(ii) **Second line of defence** is comprised of the Risk Management Coordinator who coordinates Risk Management for the first line to ensure risks are being appropriately identified, analysed, evaluated, treated, monitored and reported. This line is strengthened by establishing a Risk Management Committee comprised of senior management.

(iii) **Third line of defence** dedicated to Risk Governance and Auditing undertaken by GMO Internal Auditor, Audit Committee and the High Monitoring Council. Internal audit through application of Risk-based internal audit shall provide assurance to the High Monitoring Councils on effectiveness of Risk Management. The High Monitoring Council risk oversight comprises the last line of defence, as significant issues are escalated upwards and should therefore ensure appropriate reporting and review structure is

established in order to ensure that risks are effectively identified, assessed and appropriate controls and responses put in place. The GMO Audit Committee shall ensure an effective risk management function is in place and obtain independent assurance on its effectiveness from Internal Audit.

The figure below illustrates GMO's Risk Management governance structure. The detailed roles and responsibilities are documented in Section 9.3 of this policy.

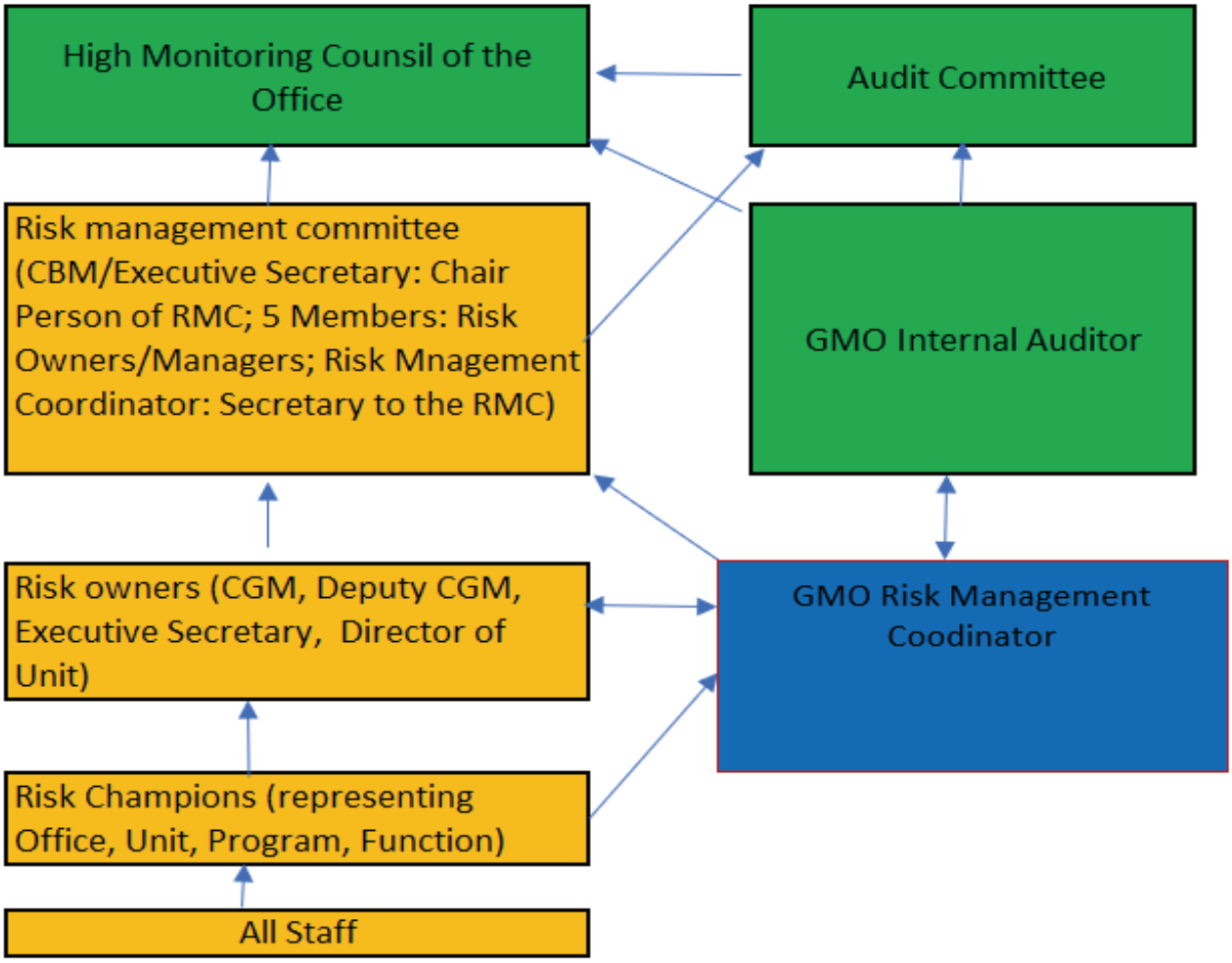


Figure 5. Risk Management Governance Structure

9.3 Risk Management Roles & Responsibilities

9.3.1 High Monitoring Council

The High Monitoring Council recognizes that it has the ultimate responsibility for the sound and judicious management of GMO and ensuring that an adequate and effective system of risk management and internal controls are established and maintained.

Specifically, the responsibilities of the High Monitoring Council include:

i. Ensure the development of a policy on risk management;
ii. Set out responsibilities for risk management;
iii. Approve the risk management policy and the risk management framework;
iv. Delegate to the senior management the responsibility to implement the risk management plan;
v. Receive and review the risk management report from RMC and Audit Committee on a quarterly basis;
vi. Establish a risk management function within GMO;
vii. Shall appoint Risk Management Committee Members;
viii. Ensure that risk assessment is carried out on a continuous basis; and
ix. Evaluate the performance of the Risk Management Committee and the Audit Committee once a year.

9.3.2 The Audit Committee

The Audit Committee shall meet at least once every **quarter** of the financial year to review the adequacy of the risk management processes in place and report on Risk Management to the High Monitoring Council. The Audit Committee should also meet on a need basis to address an urgent matter arising.

Key Risk Management related roles and responsibilities of the Audit Committee include but not limited to:

i. Provide oversight of risk management process through receiving quarterly risk

management reports from the Chairperson of the RMC.

ii. Report and propose recommendations to the High Monitoring Council for implementation;

iii. Communicate any concerns when deemed necessary to the Chairperson of the RMC,

iv. Reviewing the risk management policy framework and effectiveness of getting management assurance that material risks are identified and appropriate risk management processes are in place, including formulation and subsequent updating of appropriate GMO policies;

v. Advocate of sponsorship for risk management initiatives and support the communication of the risk management approach adopted by the organization;

vi. Ensure that GMO's risk management and corporate governance practices are in line with best practice and meet good practice requirements.

Key audit related roles and responsibilities of the Audit Committee include but not limited to:

i. Provide oversight of risk management process through receiving assurance reports from the entity's Internal Auditor on effectiveness of risk management, governance and internal controls;

ii. Review and approve annual risk-based audit plan and monitor its implementation;

iii. Communicate any concerns when deemed necessary to the CBM and the High Monitoring Council;

iv. Ensure that the GMO's risk-based internal audit practices are in line with best practice as defined in the Global Internal Audit Standards issued by the Institute of Internal Auditors (IIA).

9.3.3 Chief Budget Manager (CBM)- Executive Secretary

The CBM/ES of GMO, is responsible for:

i. Developing and implementing the risk management framework in compliance with the Risk Management guidelines for Public Entities and applicable standards;
ii. Providing the required resources for risk management efficiency;
iii. Embedding risk management in GMO processes in such a way that risks are effectively managed;
iv. Systematically reviewing the underlying risks and assigning appropriate accountability to RMC;
v. Actively promoting and being an advocate of a Risk Culture in GMO;
vi. Appointing Risk Champions representing each assessed unit;
vii. Issue a report to the High Monitoring Council and Audit Committee that oversights risk on quarterly basis.

9.3.4 Risk Management Committee (RMC)

The High Monitoring Council shall appoint at least 5 members to the Committee among Senior Management team. The Committee shall be chaired by the Executive Secretary and the Risk Coordinator acts as the Secretary.

The RMC should meet at least once every **Quarter** of the financial year to review the adequacy of the risk management processes in place and approve reports to the High Monitoring Council on a **Quarterly** basis. The RMC should also meet on a need basis to address an urgent matter arising.

The following are the main responsibilities of the Risk Management Committee:

i. Developing and reviewing the risk management policy and framework, and implementation plan for approval;

ii. Reviewing the entity's risk criteria.
iii. Ensuring that the entity has appropriate risk identification and assessment methodologies, arrangements and tools;
iv. Developing risk treatment plans to address the significant risks of the entity;
v. Assessing implementation of the risk management policy and framework, and integration of risk management within the entity operations;
vi. Review and approve **Quarterly** risk reports from the Risk Management Coordinator.

The Risk Management Coordinator is the Secretary of the Risk Management Committee. The Committee shall develop and adopt a Risk Management Committee charter to govern its operations consistent with this policy.

9.3.5 Risk Management Coordinator

The risk management function coordinates risk management activities across GMO. The risk management function shall be assigned to a senior member of staff – Risk Management Coordinator, with appropriate knowledge, experience and relevant skills.

The Risk Management Coordinator shall report to the CBM and the RMC.

The Risk Management Coordinator shall be a senior management position that is able to provide 'frank and fearless' advice about risks and how they are managed.

The Risk Management Coordinator facilitates the GMO's 1st line of defence and oversees the risk management processes by:

i. Building GMO's risk capability and defining risk management practices and framework;
ii. Developing and implementing the risk management plan;
iii. Providing guidance and training on risk management processes;
iv. Supporting Risk Owners in identifying trends and emerging risks and assessment;

v. Assisting Risk Owners in developing processes and risk treatment action plans;
vi. Monitoring the adequacy and effectiveness of risk treatment plans, and accuracy and completeness of reporting;
vii. Assisting Risk Owners and staff in recording risk data for risk monitoring and reporting;
viii. Escalating identified or emerging risks exposures to the Chair Person of RMC and the Audit Committee in line with the Risk Criteria;
ix. Monitoring compliance with the risk management policy;
i. Issue a report to the Audit & Risk Committee that oversights risk on quarterly basis; and
ii. Administering the National Risk Management Information System.

9.3.6 Senior Management (Risk Owners)

These are the risk owners and required to ensure compliance with the GMO risk management policy/framework with the departments they are in charge of.

The roles and responsibilities are as follows:

i. Implementing the risk management framework;
ii. Own risks and controls in their respective offices, directorates, finance and administrative unit thus ultimately accountable for the management of risk;
iii. Integrate risk categories relevant for the responsibilities in their day-to-day management practice and develop appropriate policies/framework.
iv. Ensure that all corrective actions against any areas of weakness are effectively and are expeditiously implemented;
v. Ensure that required risk information is reported

and that it meets all established standards for timelines and integrity;

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

vii. Ensuring compliance with all relevant legislation, standards, policies, procedures and controls;

viii. Fostering a risk management culture in their respective responsibilities;

ix. Taking appropriate measures to manage risks consistently and proactively;

x. Review, validate and consolidate reports on risk management activities in their respective responsibilities and share with the risk coordinator for RMC presentation;

xi. Propose risk champions under their assessed units for appointment by the CBM.

9.3.7 GMO Internal Audit

The roles and responsibilities of Internal Audit include:

i. Independent assessment and evaluation of the GMO Management compliance with the risk management policy and framework;

ii. Assessing adequacy and effectiveness of the risk management and control process for risks;

iii. Review the assigned risk levels, overall risk and control ratings and risk management methodology and systems;

iv. Reviewing the management of key risks by risk owners to ensure controls have been put into operation and are being monitored;

v. Evaluating risk management processes, to ensure the response to any risk is appropriate and conforms to the organisation's policies and framework.

vi. Evaluating the reporting of key risks, by Risk Owners;

vii. Report the result of its assessment to Audit & Risk Committee, Management and Risk Coordinator; and

viii. Ensure that the GMO risk policy and framework is working as designed, and

noting any shortcomings thereon to the High Monitoring Council and Audit Committee.

9.3.8 Risk Champions (RCs)

RCs are typically functional staff who assume responsibility for designing, implementing, and/or monitoring risk treatments.

RCs are responsible for the following:

i. Assist the Risk Owner in managing risks within their area of responsibility;
ii. Oversee the recording of risk data on a frequency established by GMO;
iii. Promote risk discussions and awareness within the assessed unit;
iv. Identify where current control deficiencies may exist;
v. Update risk information pertaining to the risk;
vi. Escalate the risk where the risk is increasing in likelihood or consequence;
vii. Provide information about the risk whenever it is requested;
viii. Carryout risk assessment for their assessed unit;
ix. Preparing risk report under their assessed unit on quarterly basis for review and validation by risk owner.

9.3.9 All Staff Members

All staff are responsible for:

i. Recording and reporting risk incidents;
ii. Providing information appropriate for risk data collection and recording as may be applicable;
iii. Contributing to and being responsible for risk management and internal control processes in their respective areas;
iv. Supporting the development and updating of the documentation of risks, identifying and assessing risks in their areas, and contributing to risk mitigation; and
v. Effective management of risk including the identification of potential risks.

10. Risk Management Performance Review

Risk Coordinator in liaison with the CBM will at least annually identify and reward Risk Champion of the year. A policy will be developed and communicated to all staff on that regard.

The Senior Management shall implement basis of integrating risk management into annual performance review for all staff.

Risk Management shall be incorporated in the annual performance for review of staff. All staff will be expected to demonstrate their role in Risk Management and overall understanding of the subject matter.

11. Interpretation of the Policy

The overall responsibility for interpreting this policy/framework lies with the CBM Risk Management Coordinator at GMO.

12. Applicability and Adoption

This risk management policy and framework will be applicable upon approval by the High Monitoring Council.

The policy shall be reviewed every three (3) years or when changes in the environment require such changes.

13. Policy Approval

This policy is subject to review in order to ensure that it meets the evolving needs of GMO and changes in the corporate governance environment. Any changes to the contents of this document will require the approval of the High Monitoring Council.

This risk policy and framework was considered and approved by the High Monitoring Council in its session of ..../..../2025

SIGNATURE.....

DATE.....

UMUTONI GATSINZI Nadine
Chief Gender Monitor

Appendix 1: GMO Risk Management Implementation Plan

#	Activity	Due date	Responsible person
1)	Presentation of Risk Management Policy and Implementation Plan to the High Monitoring Council for approval	15/12/2025	CBM
2)	Communicate with MINECOFIN the approved policy and request for implementation support	22/12/2025	Risk Management Coordinator
3)	Establish context and risk criteria with Risk Owners (2days) workshop	07-08/01/2026	RMC/Risk Coordinator/ MINECOFIN
4)	Nomination of risk champions	09/01/2026	CBM/Risk Owners
5)	Train and conduct risk assessment with Risk Champions (5days).	12-16/01/2026	CBM/Risk Management Coordinator /Risk Champions/MINECOFIN
6)	Validate risk registers	19-23/01/2026	Risk Owners/Risk Management Coordinator /Risk Champions
7)	1-day workshop for risk management awareness sessions across GMO	Mid Feb 2026	RMC/HR/Risk Management Coordinator
8)	Train and conduct risk data recording, monitoring & reporting as per the risk management policy (5days).	13-17/04/2026	Risk champions/Risk Management Coordinator/MINECOFIN
9)	RMC inaugural meeting	28/04/2026	CBM/Risk Management Coordinator/RMC/MINECOFIN

Appendix 2: ERM Templates

Assessed Unit	Objectives	Critical success factors	Risk event	Risk source	Risk effect	Inherent risk level	Controls	Residual risk level	Improvement action

2. Key Risk Indicator monitoring

Business Unit	Objectives	Risk event	Residual risk level	Key Risk Indicator	Green/ Amber	Amber/ Green	Month/ Qtr 1	Month/ Qtr 2	Month/ Qtr 3

3. Internal Compliance monitoring

Business Unit	Objectives	Risk event	Residual risk level	Compliance Question	Green/ Amber	Amber/ Green	Month/ Qtr 1	Month/ Qtr 2	Month/ Qtr 3

4. External Compliance monitoring

Business Unit	Objectives	Risk event	Residual risk level	External Compliance Question	Green/ Amber	Amber/ Green	Month/ Qtr 1	Month/ Qtr 2	Month/ Qtr 3

5. Incident Management

Business Unit	Date of incident	Location	Incident detail	Risk event	Control that failed	Root cause	Corrective action	Status of action taken

6. Action tracking System

Business Unit	Objectives	Risk event	Residual risk level	Improvement action	Due date	Responsibility	Status Month/ Qtr. 1	Status Month/ Qtr. 2

7. Risk Management Report

Q1 2024-25															
					Sept	Sept	Sept	Sept	Sept	Sept	Sept		Sept		
Risk events	**Aggregate ranking June Qtr 1**	**Movement**	IRL	RRL	Key Risk Indicator	Corrective action status	Compliance	Corrective action status	Incidents	Corrective action status	Risk Treatment Plan	No. of Audit findings	Status of corrective actions	Risk Owner Comments - *Summary of key issues, actions being taken and conclusion on the risk rankingin relation to each risk in Red and Amber.*	Risk Management committee comments/resolutions
Risk no. 1	1	↑	12	4	2	**WIP**	**No**	Overdue	3	WIP	WIP	2	Overdue	xxxx	xxxx
Risk no.2	2	↔	12	4	50%	**WIP**	**Yes**		1	Completed	WIP			xxxx	xxxx

Appendix 3: Risk maturity assessment

	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	Audit Test
Key characteristics	No formal approach developed for risk management	Scattered silo-based approach to risk management	Strategy and policies in place and communicated. Risk appetite defined	Enterprise approach to risk management developed and communicated	Risk management and internal controls fully embedded into the operations	
Process						
The organization's objectives are defined						Check the organization's objectives are determined by the board and have been communicated to all staff. Check other objectives

	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	Audit Test
						and targets are consistent with the organization's objectives
Management have been trained to understand what risks are, and their responsibility for them						Interview managers to confirm their understanding of risk and the extent to which they manage it
A scoring system for assessing risks has been defined						Check the scoring system has been approved, communicated and is used

	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	Audit Test
The risk appetite of the organization has been defined in terms of the scoring system						Check the document on which the controlling body has approved the risk appetite. Ensure it is consistent with the scoring system and has been communicated
Processes have been defined to determine risks, and these have been followed						Examine the processes to ensure they are sufficient to ensure identification of all risks. Check they

	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	Audit Test
						are in use, by examining the output from any workshops
All risks have been collected into one list. Risks have been allocated to specific job titles.						Examine the Risk Register. Ensure it is complete, regularly reviewed, assessed and used to manage risks. Confirm that risks are allocated to managers
All risks have been assessed in accordance with the defined						Check the scoring applied to a selection of risks is consistent

	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	Audit Test
scoring system						with the policy. Look for consistency (that is, similar risks have similar scores)
Responses to the risks have been selected and implemented						Examine the Risk Register to ensure appropriate responses have been identified
Management have set up methods to monitor the proper operation of key processes, responses						For a selection of responses, processes and actions, examine the monitoring control(s) and ensure

	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	Audit Test
and action plans ('monitoring controls')						management would know if the responses or processes were not working or if the actions were not implemented
Risks are regularly reviewed by the organisation						Check for evidence that a thorough review process is regularly carried out
Management report risks to directors where responses have not						For risks above the risk appetite, check that the board has been

	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	Audit Test
managed the risks to a level acceptable to the HMC						formally informed of their existence
All significant new projects are routinely assessed for risk						Examine project proposals for an analysis of the risks which might threaten them
Responsibility for the determination, assessment, and management of risks is included in job descriptions						Examine job descriptions. Check the instructions for setting up job descriptions

	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	Audit Test
Managers provide assurance on the effectiveness of their risk management						Examine the assurance provided. For key risks, check that controls and the management system of monitoring, are operating
Managers are assessed on their risk management performance						Examine a sample of appraisals for evidence that risks management was properly assessed for performance

	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	Audit Test
Internal Audit approach	Promote risk management and rely on alternative audit planning method	Promote enterprise-wide approach to risk management and rely on alternative audit planning method	Facilitate risk management/liaise with risk management and use management assessment of risk where appropriate	Audit risk management processes and use management assessment of risk as appropriate	Audit risk management processes and use management assessment of risk as appropriate	