REPUBLIC OF KENYA

HYDROLOGISTS REGISTRATION BOARD

DRAFT
RISK MANAGEMENT POLICY FRAMEWORK (RMPF)

(2022 – 2024)

Table of Contents

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

Abbreviations and Acronyms	Meaning
Board	Board of Directors
CEO	Chief Executive Officer
FY	Financial Year
HRB	Hydrologists Registration Board
KRI	Key Risk Indicator
Ministry	Ministry of Water, Sanitation and Irrigation
MWSI	Ministry of Water, Sanitation and Irrigation
RM	Risk Management
RMC	Risk Management Committee
RMPF	Risk Management Policy Framework
Organization	Hydrologists Registration Board

DEFINITION OF TERMS

For a uniform Risk Management System to be implemented, a common language is necessary. As such, below are some definitions of the terms that have been used in the Risk Management Policy Framework document.

TERM	DEFINITION
Committee	Audit, Risk and Compliance Committee
Gross risk	The status of the risk (measured through impact and likelihood) without taking account of any risk management activities that the organization may already have in place.
Impact	The potential loss should the risk materialize.
Likelihood	The probability that an adverse event, which could cause materialization of the risk, may occur.
Residual (net) risk	The status of the risk (measured through impact and likelihood) after taking account of any risk management activities.
Risk	The chance of something happening that will have an impact on the achievement of organizational stated objectives" or the "effect of uncertainty on objectives." An effect is a deviation from the expected positive or negative. The objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).
Risk analysis	The systematic use of available information to determine the likelihood of specified events occurring and the magnitude of their consequences. It is measured in terms of impact and likelihood.
Risk appetite	The level of risk that HRB or management is prepared to live with.
Risk assessment	The overall process of risk analysis and risk evaluation.
Risk Evaluation	The process used to determine risk management priorities by comparing the level of risk against pre-determined standards, target risk levels or other criteria.

Risk Identification	The process of determining what might happen that could affect the objectives, why and how it might happen.
Risk management	The iterative process consisting of steps, which when taken in sequence, enable continual improvement in decision-making. It is the logical and systematic method of identifying, analyzing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process in a way that will enable organizations to minimize losses and maximize opportunities.
Risk management policy	The organization's approach to managing risks and stipulates the standard in respect of risk tolerance. Risk will be measured in terms of impact and likelihood.
Risk Owner	The person primarily responsible for coordinating a response to a particular risk.
Risk tolerance	The extent of variation relative to the achievement of an objective that an organization is prepared to accept.
Strategic Risks	The nature impact on the achievement of the overall objectives of the Board rather than any discrete part of it. They cut across operational and divisional boundaries. These will be high level and strategic by nature. It is associated with a failure to meet HRB's corporate objectives as set out in the Strategic Plan 2022-2026 that cuts across program and operational boundaries.

FOREWORD

The Constitution of Kenya 2010 established the frameworks for governance and accountabilities through Articles 10, 201, and 232. With these Articles, the Constitution is encouraging good governance through accountability. According to Kenya's Vision 2030, it is envisaged that the country will have "transparent, accountable, ethical and results-oriented government institutions" by the year 2030. Furthermore, the Public Financial Management reforms have also identified a need for a more effective Corporate Governance, where risk management should form an integrated part of planning, controlling and reporting procedures.

The Hydrologists Registration Board (HRB) has a primary responsibility of ensuring that all risks facing the organization are identified and appropriate mitigation actions put in place. This can be done through a Risk Management Policy Framework (RMPF) which enables management to focus in a comprehensive and holistic manner on all risks faced by HRB. This RMPF sets out the process to manage and mitigate against present and potential risks faced by the institution. The Policy is intended to provide a framework for managing risk associated with changing roles and responsibilities within HRB.

This Risk Management Policy Framework is an important step in ensuring that Management identifies and manages all risks and that HRB provides oversight as well as policy direction in managing risks. We hereby offer our commitment to its total implementation so as to ensure effective operation and sustainability of the Board.

ANTONY MWENJE
REGISTRAR/CHIEF EXECUTIVE OFFICER

1 CHAPTER ONE

1.1 Introduction

The Hydrologists Registration Board is accountable to a variety of stakeholders and the environment in which it operates is subject to wide range of risks, thus the need for effective risk management has been recognized. This document details both the policy and strategy for continuing to develop the framework to manage risk within, however, it will only be successfully delivered on a day-to-day basis and if staff incorporate it into their daily working practices; otherwise, it will be an exercise in futility.

The Risk Management Policy Framework explains the Board's underlying approach to risk management. It gives key aspects of the risk management process and identifies the main reporting procedures. The policy should be reviewed approximately every three (3) years and amended if appropriate. This policy statement seeks to define the risk management framework within which everyone is expected to operate.

1.2 Background

The Hydrologists Registration Board is a State Corporation established under the Hydrologists Act No. 19 of 2017. HRB was gazetted on 19th July, 2019 and was officially inaugurated on 5th December, 2019. The institution falls under the Ministry of Water, Sanitation and Irrigation (MWSI).

HRB has the overall mandate, guided by the Act, of developing, regulating, coordinating and overseeing the practice of Hydrology in Kenya. This is considered as a key component in achieving water and food security under the country's strategic targets as outlined in the Big Four Agenda, Vision 2030, the Third Medium Term Plan (2018-2022), and the Sustainable Development Goals. Water is considered an important enabler in meeting the targets under all these programs.

The Hydrologists Registration Board has the responsibility of registering and regulating all persons and entities practicing in the field of Hydrology and building capacity for individual hydrologists and hydrology consulting firms, as well as regulating their professional conduct for improved and sustainable performance of the Hydrology profession.

Several restrictions have affected HRB's operations and slowed down its achievements. Chief among these is the delay in approval of its Human Resource and Policy Instruments, which have a bearing on funds allocation from the National Treasury and also on staff recruitment, among others. The minimal funds allocated to HRB in Financial Year (FY) 2020/2021 and 2021/2022 have led to slow rates of operationalization and development.

Other than the Registrar/CEO, all other staff are deployed temporarily to HRB from the Ministry of Water, Sanitation. The Hydrologists Regulations are being developed and have already been subjected to several stakeholder consultations. Once the Regulations are gazetted, the Board will commence the process of registering and licensing hydrologists, implementing programs meant to improve the capacity of its registered professionals, and developing programs for generating funds. HRB has no offices of its own and is currently being housed within the Ministry Headquarters. The Board plan to relocate to more spacious premises once it has adequate funds.

1.3 Mission, Vision and Core Values

1.3.1 Vision Statement

A quality and robust hydrological practice and management.

1.3.2 Mission Statement

To promote good governance in regulation, oversight, coordination of the practice of hydrology.

1.3.3 Core Values

The Hydrologists Registration Board will be guided by the national values as espoused by the Constitution of Kenya, 2010. These are;

a. Sustainable Development;

b. Honesty and Integrity;

c. Human Dignity;

d. Teamwork and Focus on Results;

e. Innovation; and

f. Participatory Approach

1.4 Our Mandate

The Hydrologists Registration Board under Section 19 of the Hydrologists Act, 2017 is mandated with the following functions:

i. To regulate, coordinate and oversee practice of hydrology.

ii. To promote standards of professional competence and practice amongst hydrologists.

iii. To coordinate research, investigations and surveys in the hydrological field.
iv. To recognize institutions that furnish a sufficient guarantee of academic knowledge of practical experience in hydrology.
v. To demand and certify hydrological studies and reports necessary for design of hydraulic structures.
vi. To collaborate with other bodies or organizations in development of programs and facilities for advancement of hydrology and well-being of hydrologists.
vii. To perform any other function that is incidental or consequential to its functions under this Act any other written law.

1.5 Risk Management Policy Framework – Rationale and Scope

1.5.1 Purpose of Policy

The purpose of the policy is to create robust structures, systems and processes that will minimize or eliminate risks where possible, to and from its delivery partners. The statement can be seen as a catalyst for improving awareness and responsibilities for the assessment and the management of risk at all levels of HRB, and with our partners, suppliers and stakeholders. The more specific purposes of the policy are to:

i. Ensure that the Board has an active, structured, and commonly shared knowledge of risks that they have to manage through upward reporting from Management and that the priorities of the Board in respect to the risks are fully communicated down within the Board;
ii. Ensure that management teams at every level share that understanding of risks and priorities;
iii. Ensure responsibility for the management of risks is assigned to all Board staff to ensure that they are managed;
iv. Ensure that the risk management policy framework contributes to the preparation and implementation of internal controls;
v. Ensure that financial, operational and management systems directly support the management of risks that threaten the achievement of Board objectives;
vi. Facilitate Management to deal effectively with future events that create uncertainty;
vii. Foster risk awareness and proactive risk behavior;

viii. Position management to proactively identify opportunities by considering a full range of potential events;

ix. Ensure that the risk management framework is functioning efficiently and effectively integrates with the Board's strategic planning processes; and

x. Ensure that resources are assigned to the management of risks in such a way to optimize value for money.

In addition, the RMPF will support the Board's fulfillment of its mandate and complement existing Government of Kenya regulations including but not limited to:

i. Water Act, 2016;
ii. Hydrologists Act, 2017;
iii. Hydrologists Regulations, 2022;
iv. The State Corporations Act; 2015
v. Public Officers' Ethics Act 2003;
vi. General Public Officers' Code of Conduct;
vii. Public Audit Act, 2015;
viii. Public Procurement and Assets Disposal Act, 2012;
ix. Public Finance Management Act, 2012;
x. Public Service Commission Act; 2017; and
xi. Ethics and Anti-Corruption Commission Act, 2011.

1.5.2 Policy Objectives

The Hydrologists Registration Board's policy is to pursue a structured approach to the effective management of risk in pursuit of its business objectives. This approach and the framework for its achievement is set out in more detail below, covering the continuous process of integrated activities by which the potential impact of risks to the achievement of the Board's objectives are managed.

The Board's policy is to adopt best practices in the identification, evaluation and cost-effective control of risks to ensure that they are eliminated where possible, reduced to an acceptable level or managed and contained; and be embed into the risk management practices within management and planning activities.

The broad objectives of this policy will be to:

i. Identify, measure and control risks that might impact the achievement of the Board's objectives;

ii. Provide a framework for formulation of risk management strategies; identify and harness opportunities; and

iii. Protect and enhance reputation of the Board.

This policy is designed to ensure that the following specific objectives are met:

i. Financial, operational and management systems directly support the management of risks that threaten the achievement of the Board's objectives.

ii. That Management has an active, structured, and commonly shared knowledge of the whole range, and the relative priority, of risks that they have to manage.

iii. Managers at every level share that understanding of risks and priorities.

iv. Staff objectives are set in terms that reflect the Board's strategic and operational risk priorities.

v. Responsibility for the management of risks is assigned to HRB staff to ensure that they are managed.

vi. Resources are assigned to the management of risks in such a way to optimize value for money.

vii. The top Management priorities in respect of risk are fully communicated down to HRB staff

viii. The top Management's view is informed by upward reporting of risks through the Board.

ix. Systems of control are set up support the preparation of the Statement on Internal Control.

x. The risk management system is functioning efficiently and effectively integrates with the Corporate and Business Planning processes.

Principles of best practice in risk management will be used to develop processes of risk management; however, these will be tailored to take account of needs rather than be applied as a template.

The Board's approach recognizes that to advance and thrive, it needs to strike a balance between stability and innovation. In a changing and challenging environment risk management helps to create and seize opportunities in a sustainable way, for example, by considering alternative actions to those originally intended. Some risks will always exist and will be accepted; all staff must understand the nature of risk and accept responsibility for risks associated with their area of operation. HRB focuses to be an innovative organization taking calculated risks, which have been identified and evaluated.

1.6 Scope

This policy is designed to provide a framework for identification and analysis of the risks faced by HRB, to set appropriate risk appetite limits and controls, and to monitor risks and adherence to the limits. It provides the boundaries within which this policy framework will apply, and outlines HRB's approach to risk management, the roles and responsibilities of the Board, the executive, management, employees and external stakeholders.

The policy framework also describes key aspects of the risk management process, defines the main reporting procedures and provides a framework for monitoring and evaluating effectiveness of the policy. It also provides modalities for the management of risk inherent in all activities and operations of the Board. All of the Board's operations shall be subject to this policy.

1.7 Risk Management Policy Framework as a Management Tool

The RMPF will enable the organization to:

i. Anticipate any potential risks that can impact on the achievement of the Board's objectives and propose appropriate risk mitigation measures;

ii. Make informed decisions in an uncertain operating environment and also establish pre-emptive strategies to enhance service delivery;

iii. Remain focused on understanding the nature of risks and steps to mitigate the potential negative consequences.

1.8 HRB's Risk Management Principles

The following guiding principles summarize HRB's approach to risk management and internal Control.

i. The Board of Directors has the ultimate responsibility for the management of risk to ensure HRB achieves its strategic goals and satisfies its major stakeholders.

ii. HRB's risk management structures aim to help all employees make more informed decisions through systematic identification, assessment and management of potential threats and opportunities to business goals to ensure risk exposure remains within the risk appetite limits set by the Board of Directors.

iii. Risk management in HRB encompasses external risks related to stakeholders and the overall business environment, in addition to internal risks.

iv. HRB aims to promote innovation and improvement by taking calculated risks to exploit opportunities associated with its strategic pursuit.

v. HRB's culture encourages learning from both good and poor risk management practice.

vi. Risk management culture will be integrated within existing working policies, procedures and controls of HRB.

vii. HRB will exercise "Do No Harm" practices in all its actions.

2 CHAPTER TWO

2.1 Risk Management Process Overview

Risk management (RM) is an integral part of the strategic management of HRB. The risk management system is dynamic and is designed to adapt to the HRB's developments and any changes in the risk profile over time. Compliance measures are used as a tool to address identified risks. The risk management system is based on a structured and systemic process which takes into account the both internal and external risks. The RM process is depicted in the figure below:

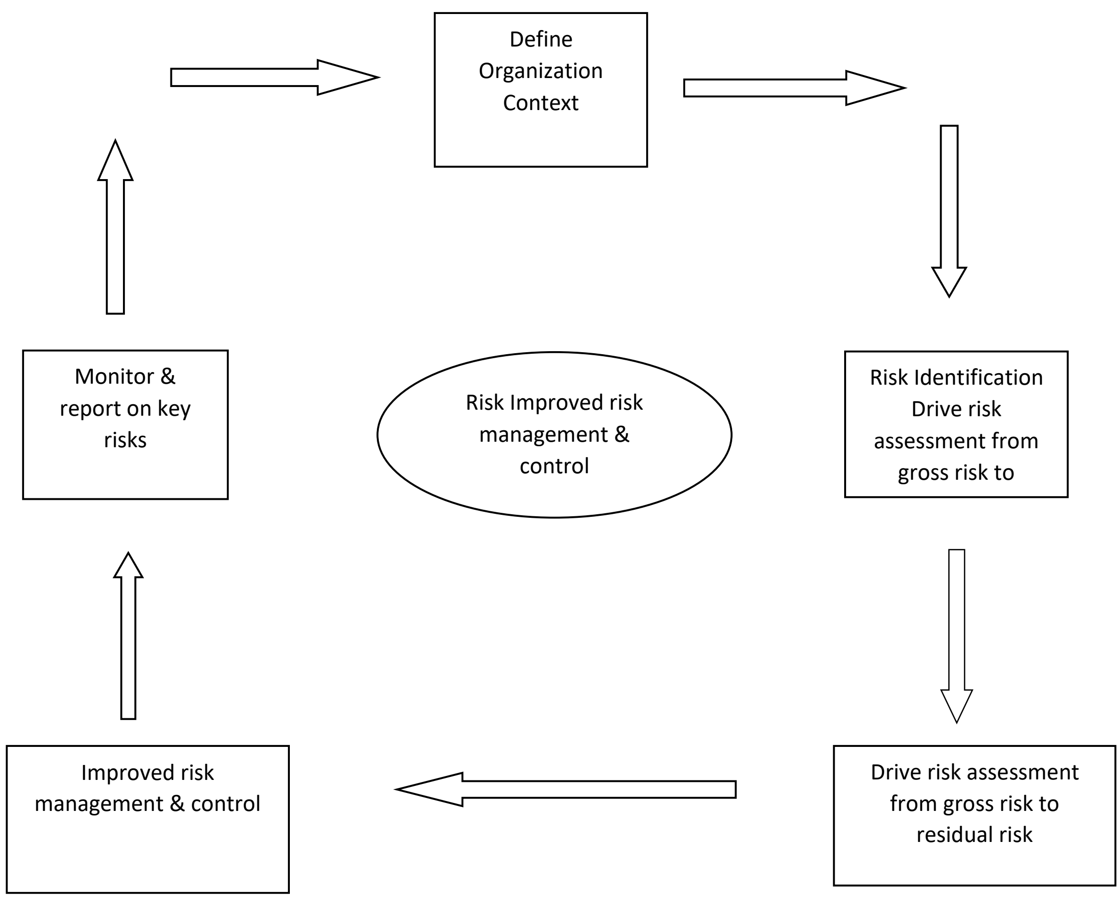

Figure 1: Risk Management Process

2.2 Outline of the Risk Management Process

2.2.1 Defining the Organization context

The Risk Assessment process begins by identifying the departments, sections and processes that will be subjected to the risk assessment process. Key contact persons and risk owners for each risk need to be identified while outlining the process to be followed during the risk assessment. This determination is designed to focus attention on areas of greatest risk by giving consideration to the following:

i. Criticality of the departments, section and processes to HRB's core business, strategy and objectives;

ii. Scale of operational activity;

iii. Regulatory and/or legal requirements; and

iv. The significance of any changes to the organization.

In defining the organizational context, it is crucial to understand the key processes, their respective objectives and the organizational context in which such processes are performed and conducted. The documentation of the critical organization processes needs to be developed at this first step while at the same time matching them to the organizational strategic objectives.

2.2.2 Broad Risk Categories

This policy identifies, defines and describes the broad risk categories in the context of the Board corporate strategic plan and historical occurrences. This RMPF has been aligned to the Board's strategic plan 2022-2026 and the following has been prioritized as the risks categories:

Table 2-1:Risk Categories

Risk Categories	Risk Descriptions	Risk Drivers
Strategic	These relate to HRB's long-term strategic objectives. This category of risk is affected by such factors as availability of funds/capital, global/regional factors, political risks, legal and regulatory factors, reputation, changes in the physical environment, and economic issues.	Internal/External

Operational	These are the day-to-day risks HRB encounters as it strives deliver its core mandate, such as technical risks, process failures, systems failures and people-risks.	Internal/External
Financial	These are related to effective management and control of HRB's finances, and also on the effects of external factors.	Internal/External
Environment, Health and Safety	These relate to issues of health, safety and the environment.	Internal/External
Legal and Regulatory	These relate to legal and regulatory responsibilities of HRB, such as non-compliance to the various legal instruments and their respective regulations.	Internal /External
ICT	This relates to Data and Information Security where key informational assets are damaged due to exploited vulnerabilities.	Internal/External

2.3 Risk Identification, Assessment and Quantification

2.3.1 Risk Identification

This is the identification of risks in the Board process that would affect the achievement of process level achievements. This constitutes the first step in building of the Board risk register. Risk identification and profiling will be a continuous process. The original risk register will be based on the risks identified on the basis of past occurrences and an evaluation of the current and future operating environment. All risks, their causes and information on the risk shall be compiled. All risks identified at departmental level shall subsequently be listed in the Corporate Risk Register, which will be the HRB's risk profile. The Corporate Risk Register will be a live document with opportunities to review and update. Identified risk shall be assigned to a "risk owner" whose responsibility will be to ensure that the risk is managed and monitored over time.

Risks will be identified by management, departments, project teams, risk champions and process owners. The identification methodology can be through structured individual and group interviews, and through workshops.

The identified risks will be reported to the senior management and to the Board of Directors during quarterly meetings. Reviews and reports will be made quarterly to identify levels of intervention made and the results thereof.

2.3.2 Risk Assessment

Assessment of risk starts by performing a root-cause-analysis of the risks identified using the five “whys” analysis and determining the best point of intervention. The five whys analysis is an iterative interrogative technique used to explore the cause-and-effect relationships underlying a particular problem. The primary goal of the technique is to determine the root cause of a defect or problem by repeating the question "Why?". Each answer forms the basis of the next question.

Quantification comes at the heels of assessment of the risk which entails identifying the qualitative and quantitative consequences of the occurrences of each identified risk. For each identified risk, an assessment shall be made of the likelihood of it occurring and the relative impact or probable impact to HRB if it does. HRB’s standardized assessment methodology is applied to assess identified gross risks in terms of likelihood and impact as outlined below. The more unmistakably risks are identified at the identification stage, the more accurately they can be assessed.

The Step-by-Step risk assessment comprises of risk rating, identification of quantitative and qualitative impact, identification of existing controls, and proposal for response and assessment of residual risk. Where possible, past events will be useful input in the risks assessment.

2.3.3 Risk Likelihood

Risk likelihood will involve determining the probability of the event/risk occurring. The following are the five levels of risk likelihood. The risk needs to meet at least one criterion to be aligned to a certain level.

a) **Certain:**

i. The event will occur in most circumstances;

ii. There is a history of regular and or pattern of occurrences;

iii. The event will occur within six months.

b) **Likely:**

i. The event will occur in most circumstances;

ii. There may be a history of frequent occurrences;

iii. The event will occur in 7-18 months.

c) **Possible:**

i. The event may occur at some time;

ii. There could be a history of occurrence;

iii. The event will occur within 19-36 months.

d) **Unlikely:**

i. Not expected, but there is a slight possibility the event could occur at some time;

ii. Divergent opinions on whether or not the risk might occur;

iii. The event will occur within 37-50 months.

e) **Rare:**

i. Highly unlikely, the event may occur under exceptional circumstances;

ii. No experience of a similar occurrence;

iii. Sufficient controls are in place;

iv. The event is likely to occur within 60 months.

2.3.4 Impact Descriptors

The probable effect on the organization if the risk occurs will be outlined in the impact descriptors. On the impact assessment, teams shall be guided by their knowledge and judgment on the subject matter and the criteria given in the table below.

The elements of impact descriptors are depicted in the table below and include impact on financial flows, disruptions on service delivery, reputation and strategic objectives. The risk needs to meet any one description to be aligned to an impact level.

Table 2-2:Impact Descriptors

Impact	**Description**
Catastrophic	Loss of services delivery; High Impact on financial flows; HRB will not meet most of its strategic objectives; Significant reputation damage;

	Litigation is certain; No insurance can be taken against it.
Major	Major disruptions on operations; Significant impact on financial flows; HRB will not meet a significant number of its strategic objectives; Adverse local publicity; Litigation is likely; and Loss of key system data.
Moderate	Moderate impact on financial flows; HRB will not meet some of its strategic objectives; Short term disruption of service delivery;
Minor	Minor impact on financial flows; and Minor impact on the HRB's strategic objectives and operations.
Insignificant	Insignificant impact on financial flows; and Insignificant impact on HRB's strategic objectives and operations.

2.3.5 Risk Ranking and Analysis

The overall ranking of risks will be divided into four broad levels, namely;

i. Extreme

ii. High

iii. Medium

iv. Low

Identified risks will be analyzed on the weights of the likelihood of occurrence and projected consequences to determine if they are extreme, high, medium or low risk as shown in the Heat Map below:

Table 2-3: Risk Analysis Heat Map

Risk Analysis	Insignificant	Minor	Moderate	Major	Catastrophic
Certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	H	H	E
Unlikely	L	L	M	M	H
Rare	L	L	M	M	H

Legend: Color indicating overall risk rating on the Heat Map

Extreme	High	Medium	Low

For purposes of decision making and developing appropriate strategies, it is important to show the relationship between risk likelihood and impact from the table above as follows:

i) Catastrophic or high impact and certain or high probability: these are extreme risks that require immediate attention;

ii) Catastrophic or high impact and rare or low probability: these are high risks that require close attention;

iii) Insignificant or low impact and certain or high probability: these are medium risks and net effect will be as high as in (ii) if left unmanaged; and

iv) Insignificant or low impact and rare or low probability: these are low risks that are generally tolerable.

2.3.6 Driving Risk Assessment from gross to residual risk

Residual risk is the risk remaining after controls have been put in place to mitigate the inherent risks. Key controls and mitigations relative to the gross risk will be identified. The residual risk will be acceptable if it is demonstrated that all measures have been taken. Each of the processes will be assessed with related controls.

2.3.7 Evaluation of existing controls

With every control identified to manage the risks in the Board, it is important to assess and test their effectiveness. The evaluation is a measure of how effective management perceives the identified controls to be working and effectively managing the risks.

The table below shows the classification of controls into five different levels of effectiveness:

Table 2-4: Control Effectiveness Criteria

Control Description	Level of Effectiveness	Rating
Could not be more effectively implemented to mitigate the risk.	Very Good	90%
Most risks are effectively controlled and mitigated.	Good	80%
There is room for some improvement in the control system.	Satisfactory	65%
Some risks appear to be controlled but there are major deficiencies.	Weak	40%
The control system is ineffective.	Unsatisfactory	20%

2.4 Risk Appetite

This policy recognizes that not all risks can be eliminated. Some level of risk will always exist. This level of exposure to risk that remains to exist and is tolerable for the organization to pursue its strategic and operational objectives is referred to as risk appetite. Risk appetite is the level of risk that is acceptable to and can be expressed as a series of boundaries that gives the Board clear guidance on the limits of risk it can take.

A model for the assessment of risk has been developed that enables risks to be evaluated on a consistent basis so that both over-control and under-control can be avoided. This will be periodically reviewed to ensure that it remains current and appropriate. One point to note is that this is not a 'one size fits all' model, it is a norm and the level of risk that is appropriate to take for an individual project or initiative will be determined by the circumstances of the project after due consideration by the appropriate regulatory body.

All risks should be scored in terms of Impact and Likelihood using the following five- point scale: the scores are multiplied together to produce the overall assessment:

Table 2-5: Likelihood of Occurrence of Risk

Impact		Likelihood	
5	Catastrophic	5	Certain
4	Major	4	Likely
3	Moderate	3	Possible
2	Minor	2	Unlikely
1	Insignificant	1	Rare

This model indicates degrees of risk severity, as measured by the combined impact and likelihood of occurrence. Guidance sheets will be made available for staff to assist in assessing scores for impact and likelihood together with lists of suggested risk areas and emergent risks that may be considered for inclusion in the process.

The Risk Appetite model is shown below;

Table 2-6:Risk Appetite Model

Impact Severity	Multiplier					
Fundamental	5	5	10	15	20	25
Major	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Minor	2	2	4	6	8	10
Insignificant	1	1	2	3	4	5
	Multiplier	1	2	3	4	5
Likelihood		Rare	Unlikely	Possible	Likely	Almost certain

Legend

	Key	
Severe	20 - 25	Unacceptable level of risk exposure which requires immediate corrective action to be taken.
Major	12 - 16	Unacceptable level of risk exposure which requires constant active monitoring, and measures to be put in place to reduce exposure.
Moderate	5 - 10	Acceptable level of risk exposure subject to regular active monitoring measures.
Minor	3 - 4	Acceptable level of risk exposure subject to regular passive monitoring measures.
Insignificant	1 - 2	Acceptable level of risk subject to periodic passive monitoring measures.

2.5 Risk Management and Control Processes

2.5.1 Risk Response

Treatment of risks will be part of the risk management process in which decisions are made about how to treat risks that have been identified and prioritized. Options for risk treatment will include: avoidance, reduction, transfer, acceptance, terminate, take opportunity and seeking additional information.

i. **Avoidance:** This risk treatment option involves taking action steps to exit the activities giving rise to risk.

ii. **Reduction/Mitigate:** This involves taking action to contain the risk to acceptable levels through systematic reduction in the extent of exposure to risk and or likelihood of its occurrence.

iii. **Transfer:** One of the best responses to some risks will be to reduce risk likelihood or impact by transferring or sharing part of the risk. Examples to this option include; insurance or paying third parties to take care of the risk.

iv. **Acceptance:** This involves taking an informed decision to accept or tolerate particular risks without taking any further action. This happens when the ability to take action about such risks is limited or the cost of taking any action may be disproportional to the potential benefit gained. In this case, the only response would be to tolerate the existing level of risk supplemented by contingency plans for handling the impacts that will arise if the risk is realized.

2.6 Risk Controls and Treatments/Actions

In the event that the ownership of a risk control or treatment required by the Board to manage a risk lies outside a department, extra departmental controls or treatments will be implemented to ensure that the original control or treatment is effective. Clear inter-departmental communication is crucial in these situations and all relevant stakeholders must be considered and engaged in this process.

Risk controls and treatments can be linked to more than one risk and can be cross departmental.

2.7 Monitoring and Reporting on Key Risks

2.7.1 Monitoring

An elaborate and robust monitoring and reporting regime is necessary in the entire risk management process. Monitoring will ensure that appropriate and timely corrective measures are taken and process-related weaknesses addressed. Risks will be continually monitored at all levels of the Board with their likelihood and potential impacts validated by various information sources, for example, incidents, risk indicator metrics linked to appetite, audit/evaluation findings and management/oversight issues.

All staff have the responsibility of identifying and monitoring risks within their areas of operations and bringing to the attention of their respective supervisors. It is the responsibility of the departmental heads to ensure controls are in place to gain assurance that risks in their areas of jurisdiction are being monitored appropriately.

The Risk Management Policy Framework monitoring process will embrace regular review and update of HRB's Corporate Risk Register and an effective on-going monitoring regime including early-warning triggers or indicators. This process will enable the Board respond to threats progress at an early stage and appropriate actions taken.

Monitoring shall determine whether:

i) Risk measures adopted resulted in what was intended;

ii) Procedures adopted and information gathered were appropriate;

iii) Improved knowledge would have helped to reach better decisions;

iv) There are lessons learnt for future assessments and management of risks.

The monitoring regime involves establishing a metric Key Risk Indicator (KRI) for each risk plus tolerance limits to monitor the risk exposure until risk has been mitigated.

KRI's are quantifiable measurements that reveal the incidence of a risk in an organization. They will differ depending on the activity, section or department. The tolerance limits for risks are established as per what management can accept and it indicates when to escalate or take action regarding the risk. Validated by various information sources, for example, incidents, risk indicator metrics linked to appetite, audit/evaluation findings and management/ oversight issues.

2.8 Reporting

Critical risks with greatest impact and highest likelihood should be measured, monitored and reported. Risk Management reports will be submitted to the Management Team and the Board of Directors periodically or as and when the need arises. The report covers these main aspects:

i. The current rating of the risk;

ii. The performance controls of the risk;

iii. Any losses incurred as a result of the risk during reporting period in question.

The reporting cycle should be reviewed on an annual basis:

i. Predetermined reports should be prepared on a fixed interval as prescribed in the risk management guidelines;

ii. Ad hoc reports will be created as issues develop.

2.9 Risk Registers

Risk registers are an integral part of the process of managing risk. The Board shall maintain a risk register that shall be used to:

i. Record all risks, risk owners, the likelihood and impact of each risk as assessed and measures assigned.

ii. Store information on significant risks in a meaningful way that can be distributed to key stakeholders and used to make better informed decisions.

iii. Rank risks by severity of consequences in order that they may be prioritized for action.

The Hydrologists Registration Board shall adopt a standard format risk register, a sample of which is shown in Annex 1. Each risk should be assessed twice, in the following manner:

i. The Inherent (Gross) Risk, which is the exposure arising from a specific risk before any action has been taken to manage it; and

ii. The Residual Risk, which is the exposure arising from a specific risk after action has been taken to manage it and making the assumption that the action is effective.

The respective manager should update the risk register to ensure that the information is up-to-date. The register will be the source of reporting on the level of risk HRB is exposed to and the actions identified to manage the risk. Risk registers are required whether the issues be strategic, program or operational.

2.10 Risk Management Policy Reviews

The risks facing the Board are likely to change owing to the dynamic nature of the operating environment. The Risk Management Policy Framework and Risk Strategy shall be reviewed on a regular basis to reflect these changes. The review process shall be undertaken through a consultative process involving, departments, the Audit, Risk and Compliance Committee, Senior Management Team and the Board of Directors.

This policy framework will be reviewed every three (3) years or as may be required. Review shall take into account the following factors:

i. Government policy and or circulars;

ii. Changes in the strategic objectives of the Board;

iii. Dynamics in the sector;

iv. Other internal and external factors.

2.11 Interlinkage between the Strategic Plan and the Risk Management Policy Framework

This Risk Management Policy Framework has been developed in line with the HRB's Strategic Plan 2022-2026 and has addressed issues raised in both documents in terms of risks that face the organization.

3 CHAPTER THREE:

3.1 Implementation of the Risk Management Plan

The Risk Management Framework represents the mechanisms and structures that will be used to oversee and manage the risks. The following building blocks are key to successful implementation of the RMPF:

i. Culture and Rules;

ii. Structure and Process;

iii. Resources and Capabilities; and

iv. Tools and Techniques.

For each of the foregoing building blocks, specific elements to be implemented are outlined below:

Table 3-1:Risk Management Plan Building Blocks

Building blocks	Elements
Culture and Rules	• Commitment and support from Board of Directors, Registrar/CEO and Senior Management; • Positive organizational culture of honesty and good ethical behavior; • Definition of risk appetite; and • Effective management oversight including finance and audit committees.
Structure and Process	• Reliable institutional risk identification and mitigation process; • Strong budgetary, accounting and internal control systems; • Policies and processes that promote transparency, accountability, integrity and fairness and delivers value for money; • Effective procurement unit; and • Effective monitoring and evaluation.
Financial Resources and Capabilities	• Effective communication; • Training; • Adequate, qualified, competent and motivated personnel well- versed with risks in their functional areas.

Tools and Techniques	• Disaster recovery plans; • Reporting procedures of risk information; • Adequate social accountability mechanisms; • Risk indicators profile; • Reward/recognition /sanctions measures; • Efficient and sound record management systems and processes on creation, use and disposal of records and • Sanctions.

3.2 Risk Management Structure

The Risk Management (RM) reporting structure will be as follows:

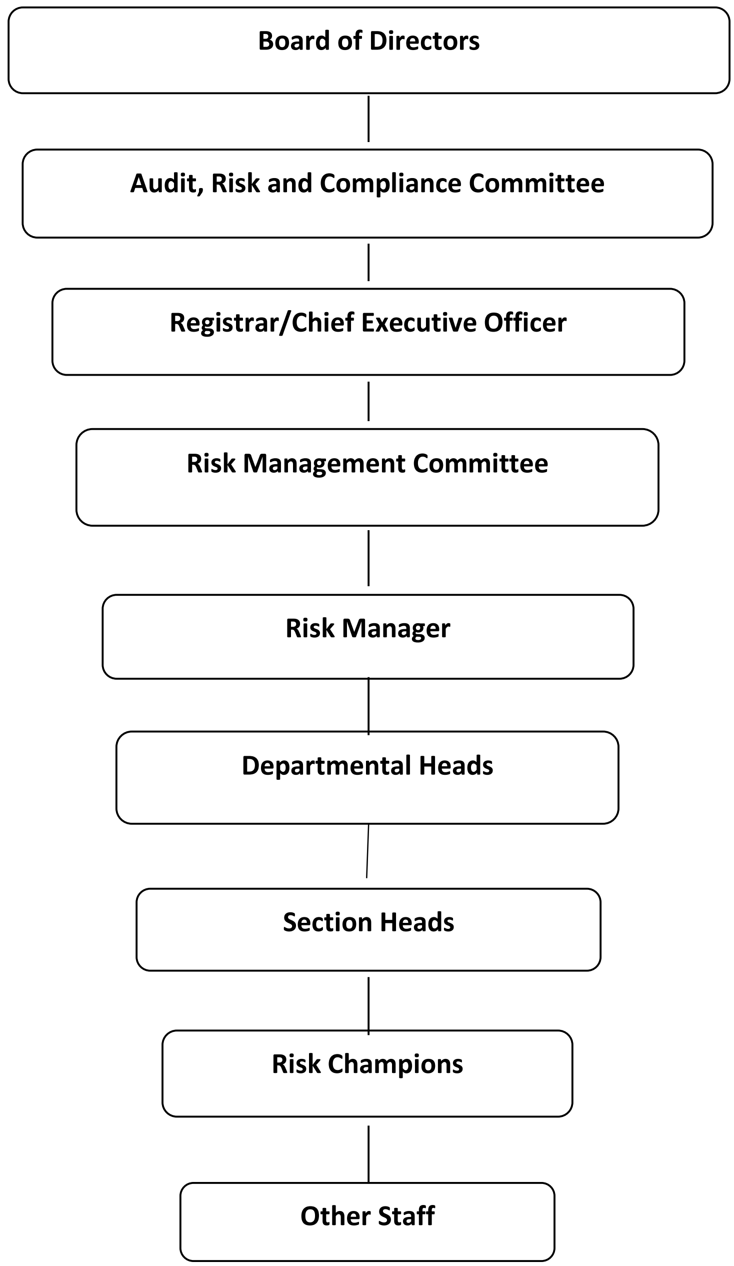

Figure 2: Risk Management Reporting Structure

3.3 Roles and Responsibilities

3.3.1 Functions of Senior Management

Senior Board management will:

i. Set the tone and influence the culture of risk management across the organization;

ii. Determine the appropriate risk appetite for HRB;

iii. Monitor the management of fundamental risks;

iv. Periodically review the Board's approach to risk management;

v. Consider whether risk management continues to be linked to the achievement of the objectives;

vi. Consider the level to which risk management is embedded in the processes and procedures; and consider the effectiveness of the overall approach to risk management

3.3.2 The Board of Directors

i. The Board of Directors bears the overall responsibility and accountability for risk management within HRB.

ii. The Board will provide stakeholders with assurance that key risks are properly identified, assessed, mitigated, and monitored.

iii. The Board will maintain a formal risk policy for HRB.

iv. The Board will formally evaluate the effectiveness of the risk management process once a year.

v. The Board will confirm that the risk management process is accurately aligned to the risk strategy and performance objectives of the Board

3.3.3 Audit, Risk and Compliance Committee

The Audit, Risk and Compliance Committee has responsibility to review and report to the Board that:

i. The Committee ensures that the risk management policy is annually reviewed after every three years and effectively identifies all areas of potential risk.

ii. Adequate policies and processes have been designed and implemented to manage identified risks.

iii. A regular program of audits is undertaken to test the adequacy of and compliance with prescribed policies.

iv. Proper remedial action is undertaken to redress areas of weakness.

v. Report annually to the Board on the organization's systems of internal control and Risk Register.

vi. Monitor the work of internal and external audit in respect of risk.

vii. Oversee regular review of risk management activities.

viii. The Board's Audit, Risk and compliance committee will monitor HRB risk management processes.

ix. The Committee will meet at least four times a year.

3.3.4 The Registrar/Chief Executive Officer

The overall responsibility for developing, coordinating, implementing and assessing the effectiveness of the RMPF is delegated to the Registrar/CEO by the Board. The Registrar/CEO shall also perform the following functions under this policy:

i. Guide the policy implementation process through the issuance of appropriate guidelines.

ii. Define appropriate institutional structures for effective implementation of the RMPF.

iii. Appoint and assign responsibility to the Risk Manager.

iv. Appoint the Risk Management Committee.

v. Demonstrate Management's commitment to the RMPF.

3.3.5 Risk Management Committee

The Risk Management Committee (RMC) will be appointed from among the Senior Management team. The Committee has been given the mandate of overseeing the risk management activities on behalf of Senior Management. The RMC's primary goals and objectives are to:

i. Ensure strong internal controls and a safe working environment.

ii. Monitor the implementation of the risk management policy framework across the Board.

iii. Approve or modify all entries in the Board's risk register.

iv. Monitor and evaluate emerging risks.

v. Approve or modify HRB's risk management training program.

vi. Direct actions to be taken in relation to annual risk management internal audit reports.

vii. Develop and oversee HRB's business continuity recovery program.

viii. In consultation with the Registrar/CEO, develop risk action plans for all risks assessed as high or above and set the time-frame for their implementation.

ix. Approve and monitor the risk action plans once developed.

3.3.6 Role of Risk Manager/Coordinator

The Risk Manager's primary roles are as follows:

i. Develop RM policies, including defining roles and responsibilities.

ii. Promoting an RM competence and awareness throughout the Board, including facilitating development of technical RM expertise and helping managers align risk responses with the Board's risk capacity and developing appropriate controls.

iii. Guiding integration of RM with other organizational planning and management activities.

iv. Establishing a common risk management language that includes common measures around likelihood and impact, and common risk categories.

v. Facilitating manager's development of reporting protocols, including quantitative

vi. and qualitative thresholds, and monitoring the reporting process.

vii. Work with the Board's Risk Committee in ensuring the identification and

viii. prioritization of risks.

ix. Bring to the attention of management any shared risks not owned by process owners.

x. Assist in ensuring that key risks are being managed appropriately by management.

xi. Ensure updated assessments are performed when significant organization changes occur.

xii. Monitor that risk mitigation efforts are progressing as required.

xiii. Monitor implementation of action plans.

xiv. Proactively identify emerging risks.

xv. Reporting to the CEO on progress of implementation and recommending actions as required.

xvi. Consolidating the reports received from the risk champions for presentation to the Board Risk Committee and the RMC.

xvii. Be the secretary to the RMC.

3.3.7 Role of Management

The Board's management consists of the Registrar/CEO, Directors, Departmental and Divisional Heads. These individuals have the primary responsibility of operating the organization in a manner that is consistent within the parameters established by the Board.

3.3.7.1 Directors

The Directorates are responsible for regulating, coordinating and overseeing the development of risk identification and management processes, coordinating the development and implementation of operational policies and procedures that assume the least risk for the Board and review top risks in their Directorates.

3.3.7.2 Departmental Heads

Management is accountable to the board for designing, implementing, and monitoring the process of risk management and integrating it into the day-to-day activities of the Board. Departmental Heads are also required to convene meetings to review top risks in their respective dockets.

3.3.7.3 Division Heads

The day-to-day responsibility for implementation of the Risk Management Policy is delegated to Division heads as "risk owners". Division heads shall manage risks in their respective divisions on day-to-day basis and facilitate departmental risk reporting. Division heads shall convene section risk management meetings for purposes of identifying, analyzing and managing risks as stipulated in the Policy document. The purpose of Division risk management meetings will be to provide the Senior Management with assurance that the major business risks are being identified and consistently assessed and that measures are in place to address risks. The Division heads will be responsible for:

i. Implementation of the principles, actions and requirements of the Risk Policy and regular review of progress against action plans for all risk items.

ii. Regular review of the current list of risk items and making any necessary changes to the risk status of individual items.

iii. Regular reporting of the status of risks.

iv. Appraisal of risk owners' actions taken to manage risk and correction of substandard performance.

v. Internal compliance and control systems for the implementation of the Risk Policy.

vi. Assist in carrying out the internal risk audit as per stipulated guidelines and in compliance with regulatory requirements and best practice.

The Division heads will work with the risk champions to fulfill their mandate. The risk champions will have a delegated responsibility during the RM process, but the ultimate responsibility still lies with the Division heads.

3.3.8 Risk Champions

The Risk Champions will coordinate their respective process areas through the entire RM process. Functions of the Risk Champions will include coordination of employees in:

i. Identification and documentation of the organization's processes;

ii. Risk identification and assessment;

iii. Risk control evaluation and reporting;

iv. Compliance to procedures; and in

v. Implementation of agreed upon improvement action plans.

3.3.9 Other staff

Risk management is the responsibility of each and every member of an organization. The organization's staff are in charge of the day-to-day running of activities and therefore should be fully involved and adequately informed on the risks associated with their daily activities and their responsibilities.

A collaborative approach will be necessary to ensure a quality system for delivery of measurable outcomes. Through training and sound management standards and procedures, the Board and Management will endeavor to develop a disciplined and constructive control environment in which all employees understand their roles and obligations. Staff will therefore be required to comply with any risk management requests as directed by Management and such requests will be channeled through their Risk Champions. Some of the functions of other staff will include;

i. Risk identification and structural reporting;

ii. Implementation of risk controls;

iii. Adherence to procedures; and

iv. Innovation of improved ways of managing risks.

3.4 Role of the Internal Audit Function

Internal Audit Department shall have an oversight role in providing assurance on the adequacy and appropriateness of strategies, policies, procedures and controls to manage risks. Specific functions include:

i. Preparation of periodic Audit Reports on implementation of the risk policy;

ii. Provide an independent and objective opinion on the adequacy an effectiveness of the organization's risk management policy; and

iii. Attend and participate in RMC meetings

Table 3-2: Risk Management Standards

NO	Standard	Responsibility	Frequency
Committee Responsibilities			
1.	The Audit Risk and Compliance Committee should meet at least four times a year.	Chairperson of the Committee/Internal Audit Manager	Quarterly
2.	The RMC should review risk management progress every four (4) months.	Registrar/CEO	Quarterly
3.	HRB's Audit, Risk and Compliance Committee should review risk management progress once a year.	Chairperson, Audit, Risk and Compliance Committee	Annually
4.	The Board of Directors should review risk management progress once a year.	Chairman of the Board/Company Secretary	Annually
Reporting responsibilities			
5.	The Board of Directors should include statements regarding risk management performance in the annual report to stakeholders.	Chairman of the Board/Company secretary	Annually

6.	The RMC with the assistance of the Risk Manager/Coordinator should submit a risk management report to the Registrar/CEO four times a year. The report should focus on the following: The top 10 strategic risks facing HRB; The top 15 risks facing HRB as a whole outside of the strategic risks above; Follow up on implementation of agreed upon actions to improve risk management; Any risk developments or risk incidences; and The report will also include the top 5 risks per department as an appendix.	Registrar/CEO	Quarterly
7.	Each department should prepare a risk management report and submit it to the risk manager/coordinator for consolidation and submission to the RMC. This submission should focus on the following: The top 10 risks facing the department; Progress in implementing agreed upon actions to improve risk management; and Any risk developments or risk incidences.	Departmental managers	Quarterly

Risk assessment responsibilities			
8.	The RMC should arrange HRB key risks to be formally re- evaluated once a year.	Registrar/CEO	Annually
9.	The departmental managers should formally reassess the top 15 departmental risks annually.	Departmental managers	Annually
10.	All risk management committees and forums should review risk registers at each meeting and update the register's contents to reflect any changes without formally reassessing the risks.	All	During each respective risk meetings
11.	The departmental managers should formally reassess the top 15 departmental risks annually.	Departmental managers	Annually
12.	All risk committees and forums should review risk registers at each meeting and update the register's contents to reflect any changes without formally reassessing the risks.	All	During each respective risk meeting
Control Responsibilities			
13.	The Audit, Risk and Compliance Committee should consider management's report concerning the effectiveness of internal controls with regard to the risks identified at least once a year.	Audit, Risk and Compliance Committee Committee Chairperson	Annually
14.	As part of the quarterly report to the Audit, Risk and Compliance Risk Committee, the RMC should report on the performance of internal controls for those risks reported.	CEO	Quarterly

15.	Departmental managers should report to the RMC regarding the performance of internal controls for those risks in the departmental risk registers.	Departmental managers	Quarterly
16.	All risk registers should contain action plans for improving risk controls and risk interventions. Each forum should review progress made with these action plans.	All	In every risk report as above indicated
Governance Responsibilities			
17.	Each risk should have a nominated owner who should be responsible for the following: Updating the risk information. Providing assurance regarding the risk's controls. Coordinating the implementation of action plans for the risk. Reporting on any developments regarding the risk.	Departmental Managers	As scheduled
18.	The Internal Audit Function should use the outputs of risk assessments to compile its audit coverage plan and should investigate the effectiveness of risk controls.	Internal audit	Annually
19.	Each risk owner should review the risks and controls associated with that risk.	Risk Owner	As scheduled

4 CHAPTER FOUR

4.1 Categories and causes of fraud

4.1.1 External fraud

Planned and executed by parties external to the Fund" without any staff' Involvement.

4.1.2 Internal fraud

This is planned and executed by internal staff. However, where internal staff aid an external party to commit fraud; this will be looked at as internal fraud. Internal fraud can be categorised into three:

i. Asset misappropriation - which involves the theft or misuse of an organization's assets.

ii. Fraudulent statements - This is usually in the form of falsification of financial statements in order to obtain some form of improper benefit. It also includes falsifying documents such as employee credentials.

iii. Corruption -This includes activities such as the use of bribes or acceptance of 'kickbacks', improper use of confidential information, conflicts of interest and collusive tendering.

4.2 Causes of fraud

A common model that brings together a number of these aspects is the Fraud Triangle. This model is built on the premise that fraud is likely to result from a combination of three factors listed below:

i. Opportunity

ii. Motive

iii. Rationalization

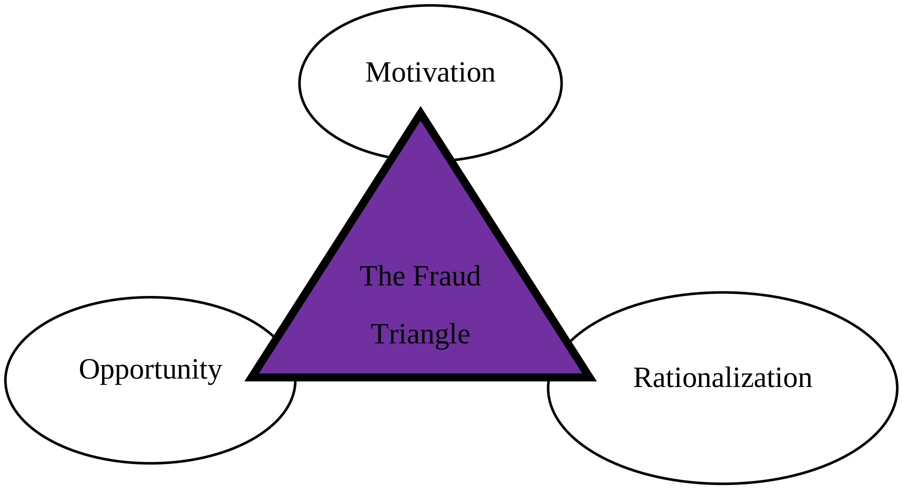

Figure 3: The Fraud Triangle

4.2.1 Opportunity

A fraud opportunity is a situation which provides a favourable environment for commitment of fraud rising from lack of or ineffective controls. Examples of conditions which can provide a fraud opportunity include:

i. Lack of segregation of duties, a single person executing a key process;
ii. Long outstanding entries on the suspense accounts or lack of reconciliation of suspense accounts
iii. Sharing of passwords
iv. Lack of or poor record keeping
v. Lack of inbuilt system controls
vi. Collusion among staff
vii. Lack of or inappropriate verification of customer information
viii. Use of manual systems
ix. Use of inexperienced staff

4.2.2 Motive

Motivation is typically on either greed or need. Seeing the opportunity, a person will develop motive of committing fraud. He/she will evaluate the control environment and the possibility of detection in case he/she commits fraud. If he/she is convinced that the controls are weak and that the possibility of detection is remote, at least in the near future, the person will commit fraud.

4.2.3 Rationalization

Having identified the opportunity and developed a motive of committing fraud, the fraudster will begin to convince him/herself that the act he/she is about to commit is okay and the person starts creating excuses.

4.3 Controlling fraud

Fraud risk is one component of operational risk. Operational risk focuses on the risks associated with errors or events in transaction processing or other business operations. A fraud risk review considers whether these errors or events could be the result of a deliberate act designed to benefit the perpetrator. Managing the risk of fraud is the same in principle as managing any other business risk. The potential consequences of fraud on the organisation need to be understood. Management should then develop and implement an anti-fraud strategy. This is best approached systematically, both at the organisational level, for example by using ethics policies and anti-fraud policies and at the operational level, through introduction of controls and procedures as discussed in the previous section.

The best way to control fraud is to eliminate all fraud opportunities; we cannot fully control the motive and rationalization, because these two exist in the mind of the fraudster. Therefore, HRB shall put in place control measures which are not only adequate but effective, and they will be subject to regular monitoring and assessment by the risk management and compliance unit. Internal audit will also carry out period audits and shall provide reasonable assurance on the adequacy and effectiveness of internal controls in eliminating fraud opportunities. An anti-fraud strategy at HRB should have four main components:

i. Prevention

ii. Detection

iii. Deterrence

iv. Response

4.3.1 Fraud prevention

In the case of deliberate acts of fraud, the aim of preventative controls is to reduce opportunity and remove temptation from potential offenders. Prevention techniques include the introduction of policies, procedures and controls, and activities such as training and fraud awareness to stop fraud from occurring. It is profitable to prevent losses, and fraud prevention activities can help to ensure the stability and continued existence of a business. It is worth bearing in mind though, that fraud prevention techniques, while worth investing in, cannot provide 100% protection. It is difficult, if not impossible, to remove all opportunities for perpetrating fraud.

4.3.2 Fraud detection

As fraud prevention techniques may not stop all potential perpetrators, HRB will have systems in place that will highlight occurrences of fraud in timely manner. This is achieved through fraud detection.

The fraud detection strategy should involve use of analytical and other procedures to highlight anomalies, and the introduction of reporting mechanisms that provide for communication of suspected fraudulent acts. Key elements of comprehensive fraud detection system include;

i. Exception reporting

ii. Data mining

iii. Trend analysis and ongoing risk assessment

Fraud detection may highlight ongoing frauds that are taking place or offences that have already happened. Such schemes may not be affected by the introduction of prevention techniques and, even if the fraudsters are hindered in the future, recovery of historical losses will only be possible through fraud detection. Potential recovery of losses is not the only objective of a detection programme though, and fraudulent behaviour should not be ignored just because there may be no recovery of losses. Fraud detection also allows for the improvement of internal systems and controls. Through detection of such frauds, controls can be tightened making it more difficult for potential perpetrators to act.

Fraud prevention and fraud detection both have a role to play and it is unlikely that either will fully succeed without the other. Therefore, it is important that HRB consider both fraud prevention and fraud detection in designing an effective strategy to manage the risk of fraud.

4.3.3 Responding to Fraud

Reasonable steps or responding to detected or instances of fraud include:

i. Clear reporting mechanisms;
ii. Thorough investigation;
iii. Disciplining of individuals responsible (internal, civil and/criminal);
iv. Recovery of stolen funds or property; and
v. Modification of anti-fraud strategy to prevent similar behavior in future.

4.4 Fraud Monitoring and Reporting

Internally, all cases of fraud, internal or external, attempted or actual, shall be considered as risk incidents which will be reported to the risk management and compliance unit as per the incident reporting guidelines. The risk and compliance manager shall liaise with the internal audit to ensure that reported fraud incidents are investigated.

Internal audit shall conduct a thorough investigation to first of all establish the authenticity of the allegations and then the cause, the parties involved and the actual loss incurred. Internal audit shall report its findings to executive management (and to HRB's Audit, Risk and Compliance Committee). Internal audit shall also recommend improvements to operational controls necessary to prevent future occurrence of fraud.

A fraud reporting framework shall be established and should consist of:

I. An internal reporting structure to facilitate prevention and detection of fraud and corruption;
II. External reporting to government agencies of evidence of illegal acts or suspected corruption as required by law and as a preventive measure; and
III. Publicizing outcomes as a deterrent where inquiries and investigations find fraud and/corruption has occurred.

Everyone in HRB is obliged to report suspected fraud or corruption. This is important so that whatever fraud or corruption may exist can be eradicated. The reporting of a suspicion does not mean that fraud or corruption has in fact occurred. There are more stages to the process before such a conclusion can be reached. For example, staff must be able to provide reasonable grounds for the suspicion.

All supervisors have a duty to address the issue raised and let the reporting officer know the action they have taken. If a supervisor does not take prompt action, an employee can report the information to a supervisor/manager at a higher level. Inappropriate conduct or administrative breakdowns can be revealed as a result of the staff member's initiative in reporting suspicions. This provides an opportunity for corrective of clarifying measures to be taken locally or by the department as a whole. Responses may include re-issuing established guidelines, developing new or better procedures, improving checking and documentation requirements, staff training etc.

For more serious issues, formal counselling, warning or some other staff disciplinary action under The Public Officer Ethics Act, 2003 or other legislation may be warranted. In these instances, the matter must be referred to the management for further action.

Confidentiality is a necessary part of any inquiry or investigation both to protect the staff member making the report and to protect the reputation of innocent people. However, confidentiality cannot be completely guaranteed in every circumstance. Principles of natural justice and procedural fairness may require disclosure of the original report. In some situations, HRB has obligations to inform other agencies including the Ethics and Anti-Corruption Commission, donors or other stakeholders such as the National Treasury.

There are also other alternatives where reporting to a supervisor is not practical of efficient. If this is the case, an employee can report directly to the Accounting Officer. Any employee can also report suspected corrupt conduct directly to the Internal Audit Department.

4.5 Social accountability

The Hydrologists Registration Board and the Board Management should ensure that there is transparency and accountability in all activities. HRB, in accordance with its founding principles, will continue to improve the quality of life of its employees and the communities it serves; conduct its operations ever mindful of its social accountability, respecting applicable laws and with regard for human dignity. HRB will also endeavour to positively Impact and influence its partners in fostering a sense of social commitment for its stakeholders.

5 ANNEX 1: Risk Register

Hydrologists Registration Board

		Department/Section																			
	Ref No	Procedure Objectives				Key Performance Indicators (for monitoring objectives)				Linkage to overall strategy and goals											
Risk Code	Objective Ref	Risk	Root Cause	Qualitative Consequences of Risk	Quantitative Consequences of Risk	Gross Risk Assessment	Controllable			Control to prevent risk occurrence	Control Effectiveness	Residual Risk Assessment			Actions to respond to risk occurrence and manage risk consequence	Key Risk Indicator	Tolerance Limit	Incidents/ actual exposure	Deviation	Improvement action plans	Responsibility and Target Date
						Impact	Likelihood	Overall	(Yes/ No)			Impact	Likelihood	Overall							