

KENYA PIPELINE COMPANY LIMITED



Enterprise Risk Management Policy

23

THE ENTERPRISE RISK MANAGEMENT POLICY

WAS APPROVED BY THE BOARD OF DIRECTORS

DURING IT'S 103rd MEETING HELD ON

20th SEPTEMBER, 2023

For and on Behalf of

KENYA PIPELINE COMPANY LIMITED

Signed:

A handwritten signature in black ink, appearing to read "Joe Sang", is written over a horizontal line.

Joe Sang, EBS

MANAGING DIRECTOR

CONTENTS

CONTENTS.....	i
LIST OF ABBREVIATIONS	ii
DEFINITION OF TERMS	iii
DOCUMENT CONTROL.....	iv
1.0 RISK MANAGEMENT POLICY STATEMENT	1
2.0 PURPOSE	2
3.0 ERMP OBJECTIVES	2
4.0 SCOPE	3
5.0 RISK MANAGEMENT BUILDING BLOCKS	4
6.0 RISK APPETITE.....	5
7.0 ERM DESIGN AND REPORTING.....	8
7.1 ERM Design	8
7.2 ERM Reporting Structure	9
8.0 ROLES AND RESPONSIBILITIES.....	10
9.0 MONITORING & REPORTING	12
10.0 POLICY REVIEW	12

List of Tables

Table 1: ERMP Building Blocks.....	4
Table 2: KPC Risk Appetite	6
Table 3: KPC Roles and Responsibilities.....	10

List of Figures

Figure 1: ERM Reporting Structure.....	9
--	---

LIST OF ABBREVIATIONS

Abbreviation	Definition
ERM	Enterprise Risk Management.
ERMP	Enterprise Risk Management Policy.
KPC	Kenya Pipeline Company.
KRI	Key Risk Indicator.
MD	Managing Director.
RMC	Risk Management Committee.

DEFINITION OF TERMS

Term	Definition
Assurance	An evaluated opinion based on evidence gained from a review that risks are identified, assessed, and effectively mitigated
Controls	Existing processes, devices, practices, or other actions that act to minimize negative risks or enhance positive opportunities.
Corporate Risk Register	The documented and prioritized overall assessment of the principal risks faced by the corporation
Enterprise Risk Management	ERM is an entity wide process for managing the myriad of risks facing the company
Exposure	The consequences as a combination of impact and likelihood, which may be experienced by the organization if a specific risk is realized.
Inherent risk	The risk linked to an activity.
Gross risk	The initial assessment of risk without controls.
Residual risk	The risk remaining after considering the effectiveness of management's risk responses/mitigation measures.
Impact/magnitude of occurrence	Significance of a particular risk to KPC. The significance of a particular risk can range from minor to major. Magnitude of impact is determined with respect to KPC's risk appetite, risk capacity and objectives.
KRI's	A measure used in risk management to indicate occurrence of risk.
Likelihood of occurrence	Probability that a particular risk will occur. These probabilities range from unlikely to likely.
Risk Appetite	The amount of risk the company is willing to take in pursuit for value.
Risk Response	Any action taken by management to enhance the likelihood that established objectives will be achieved by mitigation of risks

DOCUMENT CONTROL

Title: Enterprise Risk Management Policy

Status: Approved

Version: 3.0

Date of Issue: 2023

Supersedes: 2.0

History: Release of version after internal reviews.

Next review date: 2026

Endorsement, Ratification and Compliance

This document is subject to approval by the Kenya Pipeline Company Board of Directors.

Placement

This is one of a range of documents, either in existence or being prepared, forming part of or is related to the Corporate Strategic Plan.

- i. Treasury Circular NO 3/2009 on the Development and Implementation of Institutional Risk Management Policy Framework (IRMPF).
- ii. KPC Risk Management Policy 2009
- iii. KPC Risk Management Policy 2015
- iv. KPC ERM Procedure Manual (annex to the ERM Policy 2023)

In addition to these ERM related documents, there are also in existence a range of other internal controls/procedures, standards, and corporate governance documents within the Company.

1.0 RISK MANAGEMENT POLICY STATEMENT

The Board of Directors and Management of KPC have committed to a process of risk management that is aligned with the principles of best practices in corporate governance. To achieve this:

- i. KPC organization systems, processes and activities will be subject to the Enterprise Risk Management policy (ERMP) and the Enterprise Risk Management procedure manual.
- ii. Risk Management will be applied as a continuous process where risks and opportunities are identified, analysed, and consciously managed to maintain risks within approved risk appetite levels and capitalise on value-enhancing opportunities.
- iii. Risk Management will be integrated with business processes such as strategic planning, operational management, and outsourcing decisions to ensure consistent consideration of risks in all decision-making.
- iv. The ERM procedure manual has been developed to ensure effective implementation of the ERMP. The manual outlines the key steps and all related tasks, provide a description of how these tasks are to be undertaken, and who is responsible for the tasks.

The nature of KPC operations demands that we adopt a prudent approach in the management of our risk portfolio. The ERM processes shall therefore be embedded in our organizational systems and processes so that our response to risk remains current and robust.

KPC is committed to building increased awareness and shared responsibility for risk management at all levels of the Organization. As such, every individual should understand and manage the risk they face in their area of operations. We shall continuously review the ERM framework to ensure that it meets the challenges of a dynamic business environment and best industry practices.



JOE SANG, EBS

MANAGING DIRECTOR

2.0 PURPOSE

Enterprise Risk Management framework is to be applied in strategy setting and across the organization, to identify potential events that may affect the company, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. ERM is therefore a management tool that augments management decision-making process, minimize losses, as well as helps maximize profits. It offers a framework or process for effectively managing uncertainties, responding to risks, and exploring opportunities as they arise to ensure that value is created, protected, and enhanced.

The purpose of the policy is to provide guidance regarding the management of risks to support the achievement of corporate objectives, protect staff and business assets and ensure financial sustainability. The process should be supported by nurturing a strong and organizational culture and effective processes and structures that are directed towards realizing potential opportunities and managing adverse effects.

The nature of KPC operations demands that a prudent approach to risk management is adopted. For this reason, the Enterprise Risk Management Policy is expected to enhance the application of good corporate governance principles and address challenges emanating from both internal and external operating environments.

This Enterprise Risk Management policy therefore sets out KPC's commitment to continual implementation of a holistic risk management framework to aid in the identification, analysis, and evaluation of enterprise-wide risks and opportunities according to ISO 31000:2018 Risk Management Guidelines.

3.0 ERMP OBJECTIVES

The broad objective of KPC's Enterprise Risk Management Policy (ERMP) is to contribute to business sustainability and enhance shareholder value. Key specific objectives are to:

- i. Identify, measure and control risks that might impact the achievement of KPC objectives.

- ii. Provide a framework for the formulation of risk management strategies, identify and harness opportunities.
- iii. Protect and enhance the reputation of the Company; and
- iv. Support the Board and Management to fulfil their mandate as per Mwongozo; which requires KPC to have adequate systems and processes of risk management.

4.0 SCOPE

This ERM policy and ERM Procedure manual (annex) is designed to provide the framework for identification and analysis of the risks inherent in KPC processes and activities, set appropriate risk appetite, outlines KPC's approach to risk management, defines the roles and responsibilities of the Board, Management and Employees. It also outlines the risk response strategies and options, ERM design and reporting and policy review process.

The policy provides a framework for the management of all risks inherent in all KPC processes, activities/operations. It shall be applicable to all its employees, suppliers and third parties interacting with KPC in the execution of its mandate and all KPC working sites and activities.

5.0 RISK MANAGEMENT BUILDING BLOCKS

The enterprise risk management framework represents the mechanisms and structures that will be used to enhance the embedding of enterprise risk management approach. The following building blocks are key to the successful implementation of the Enterprise Risk Management Policy (ERMP) in the company:

Table 1: ERMP Building Blocks

Building blocks	Elements
Culture and Values	i. Commitment and support from Board of Directors, Managing Director and Management ii. Positive organizational culture of honesty and good ethical behavior iii. Definition of risk appetite iv. Effective oversight on effectiveness of internal controls
Structure and Process	i. Reliable institutional risk identification and mitigation process ii. Strong budgetary, accounting, and internal control systems iii. Anchoring ERM actions in the corporate strategy iv. Policies and processes that promote transparency, accountability, integrity, and fairness and delivers value for money v. Effective monitoring and evaluation
Resources and Capabilities	i. Effective Communication ii. Training and development iii. Adequate, qualified, competent, and motivated personnel well versed with risks in their functional areas iv. Allocation of requisite budget for ERM program

Building blocks	Elements
Tools and Techniques	i. Standardized risk matrices ii. Reporting procedures of risk information iii. Automation of risk management processes iv. Adequate social accountability mechanisms v. Risk indicators profile vi. Reward/recognition measures

6.0 RISK APPETITE

The Enterprise Risk Management Policy takes cognizant that not all risks will be eliminated as some level of risk will always exist. The Risk Appetite is the overall level of exposure to risk that is acceptable for the organization to tolerate in pursuit of its strategic and operational objectives. KPC's risk appetite is expressed as the boundary, above which the risk level will not be tolerated, and further actions must be taken to mitigate risk. The risk appetite statement influences, and guides decision making, clarifies strategic intent and ensures choices align with the capacities and capabilities of KPC.

- i. **Low-Risk Appetite** – Areas in which KPC avoids risk or acts to minimize or eliminate the likelihood that the risk will occur because we have determined the potential downside costs are intolerable. These are areas in which we typically seek to maintain a very strong control environment.
- ii. **Medium Risk Appetite** – Areas in which KPC must constantly strike a balance between the potential upside benefits and potential downside costs of a given decision.
- iii. **High-Risk Appetite** – Areas in which KPC prefers disciplined and calculated risk-taking because we have determined the potential upside benefits outweigh the potential costs.

Table 2: KPC Risk Appetite

KPC has looked at its business and defined its risk appetite as follows:

No	Risk Categories	Description	Risk Appetite
1	Strategic	Relate to long-term strategic objectives of the Company. This category of risk is affected by such areas as competition, capital availability, global/regional factors, sovereign and political risks, legal and regulatory factors, reputation, changes in the physical environment and economic issues.	Medium: KPC shall closely monitor its strategic objectives, associated risks and the action plans. KPC shall take calculated risks to take advantage of opportunities to achieve its objectives.
2	Operational	These are the day-to-day risks the organization encounters as it strives to deliver its core mandate, e.g., technical risks, process failures, systems failures, and people risk.	Low: KPC shall ensure continuity of operations in a safe and secure manner and risks that would cause disruptions will not be tolerated.
3	Financial	These are related to effective management and control of the finances of the Company and the effects of external factors (e.g. availability of credit, foreign exchange rates, interest rate movement, liquidity, change in government policy and other market exposures).	Low: Deliberate efforts will be made towards monitoring and ensuring prudent utilization of financial assets. Medium: In pursuit of its overall objective, KPC is willing to take on some risks on Capital Management to positively influence the ability to deliver on our core mandate.
4	Environment Health & Safety	These relate to issues of health, safety, and environment (eg. hazards, fire, product spillage, pandemic, and climate changes).	Low: KPC will have zero tolerance to Environment, Health& Safety related risks and will strive to mitigate both human and

			economic losses arising from accidents, adverse-occupational and environmental hazards.
5	Legal and regulatory	These relate to the legal and regulatory responsibilities of the company.	Low: KPC will adopt zero tolerance in non-compliance to all relevant legal and regulatory requirements to minimize on litigations.

7.0 ERM DESIGN AND REPORTING

7.1 ERM Design

The Risk Philosophy of the Company as articulated in this policy is principally embedding an ERM approach by ensuring that this policy is applied across all company activities and operations to identify potential events that may affect the company and manage the risks to be within the risk appetite, while providing reasonable assurance regarding the achievement of company objectives. The company shall apply an elaborate ERM process that entails, establishing the business context, risk identification & assessment, drive risk assessment from gross to residual risk, continual improvement of risk management & controls and monitoring & reporting of key risks. The risk appetite is operationalized through a determination of the risk tolerance limits for each risk identified. The company is cognizant of the fact that not all risks will be eliminated and that some level of risk will always exist. Hence the company will deploy appropriate the risk response option (risk acceptance, risk avoidance, risk reduction, risk transfer, risk termination, take opportunity and seeking additional information)to each risk as may be assessed and determined.

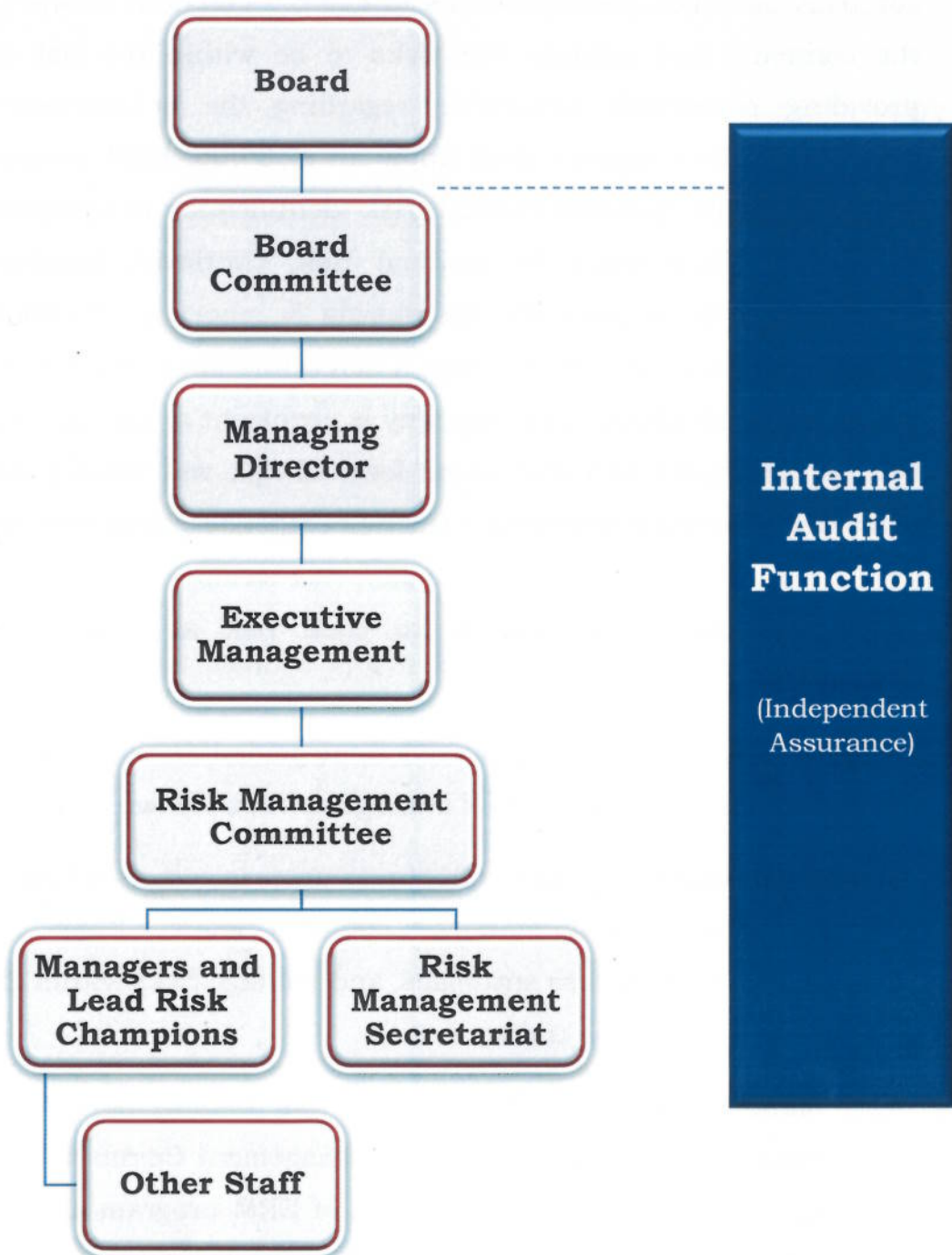
The governance of the enterprise risk management in the company is aligned to the three lines of defense in risk management as follows:

- i. **First Line:** Comprises of business process owners who in KPC structure are departmental managers (Risk Owners). They control budget, implement business strategies, and manage risks within the risk appetite in their respective units.
- ii. **Second Line:** Comprises of the risk management function and top management through the Risk Management Committee (RMC). Ensures coordination and implementation of ERM program as per the approved policies and procedures.
- iii. **Third Line:** This is an oversight role provided by Internal Audit Department. It provides an independent opinion and assurance on effectiveness of risk management processes to the Board of Directors.

7.2 ERM Reporting Structure

In alignment with the ERM design, the ERM reporting structure will be as follows:

Figure 1: ERM Reporting Structure



8.0 ROLES AND RESPONSIBILITIES

Based on the forgoing three lines of defence, the KPC ERM design to risk management has clearly defined roles and responsibilities as outlined hereunder:

Table 3: ERM Roles and Responsibilities

Level	Roles & Responsibility
The Board	• Ensure development and approval of the risk management policy and framework. • Delegate to management the responsibility to implement the risk management plan. • Appoint a committee responsible for risk management in the organization. • Receive from the Internal Audit function, a written assessment of the effectiveness of the system of internal controls and risk management. • Receive assurance from Management that the risk management framework is integrated in the daily activities of the organization.
Managing Director	• Sets the right tone at the top to enhance a positive risk culture in the company • Guide the policy implementation process through the issuance of appropriate guidelines. • Define appropriate institutional structures for effective implementation of the Enterprise Risk Management Policy. • Provide adequate resources for effective risk management • Appoint and assign responsibility to the risk management function • Appoint the Risk Management Committee.
Executive Management	• Support the Managing Director in setting the right tone as lead risk champions in their respective dockets • Implementation of agreed action plans in their dockets • Deep dive and reporting on top risks in their respective dockets to the Board Committee responsible for ERM • Review ERM Risk Management Reports escalated from the Risk Management Committee
Risk Management Committee	• Review quarterly reports received from the ERM secretariat on risk assessment, treatment, and monitoring • Prioritize the principal risks facing the company

Level	Roles & Responsibility
	• Direct actions to be taken in relation to the risk management reports • Escalation of key risks to executive management • Cause amendments to the corporate risk register where applicable • Monitor implementation of the ERM annual program
Risk Management Secretariate	• Coordinates the implementation of ERM Annual program • Coordinate the development and review of the Enterprise Risk Management framework • Building and maintaining relationships with those responsible for managing risks throughout the entity • Preparation of periodic Enterprise Risk Management reports to the Risk Management Committee • Cascade ERM policy, matrices, and related procedures • Monitoring and reporting • Secretary to the Risk Management Committee
Managers	• Accountability as risk owners of their respective business processes • Undertake risk Assessment, monitoring, and updating of departmental risk registers • Implementation of controls and agreed actions • Periodic reporting of status risks, including emerging and evolving risks and opportunities • Ensure risk management is an agenda item during departmental meetings
Risk Champions	• Support their line managers in risk identification, assessment, documentation, design of mitigations, monitoring and reporting
Internal Audit	• Preparation of periodic Audit Reports on implementation of the risk policy • Provide an independent and objective opinion on the adequacy and effectiveness of the organization's risk management policy • Attend and participate in Risk Management Committee meetings
Other Staff	• Support during Risk identifications and reporting • Implementation of risk controls as directed • Adherence to procedures • Innovation of improved ways of managing risks • Incident reporting

9.0 MONITORING & REPORTING

The purpose of risk monitoring and reporting is to create awareness of key risks, improve accountability for the management of risk and the timely completion of risk treatment plans. An elaborate reporting and monitoring regime is necessary in the entire risk management process to ensure that appropriate and timely corrective measures are taken.

The monitoring regime involves establishing a metric i.e. the KRI for each risk plus tolerance limits to monitor the risk exposure until risk has been mitigated. KRIs are quantifiable measurements that reveal the incidence of a risk in an organization. The tolerance limits for risks are established as per the risk appetite and respective risk tolerance levels. Monitoring shall also evaluate implementation status of improvement actions plans designed to mitigate risk and emerging and evolving risks. Top departmental risks and the principal corporate risks are to be monitored and escalated as per policy. ERM reporting requires periodic escalation of ERM reports to Management and the Board of Directors for decision making.

10.0 POLICY REVIEW

The risks facing the Company and the approach to managing the risks is likely to change owing to the dynamic operating environment. The ERM Policy shall be reviewed on a regular basis or at least every two years to reflect these changes. The review process will be undertaken through a consultative process involving departments, the Risk Management Committee, the Management team, and the Board of Directors. A review of the ERMP shall take into account the following factors;

- i. Government Policy and/or circulars
- ii. Changes in the strategic objectives of the company
- iii. Dynamics in the business environment
- iv. Benchmarking policy to industry and best practices
- v. Gap analysis of KPC ERM processes
- vi. Other internal and external factors

