



Home Afrika Limited | 5th Floor, Morningside Office Park | Ngong Road, P.O. Box 6254 – 00100, Nairobi. Tel: +254 (0) 20 272000
info@homeafrika.com | www.homeafrika.com

RISK MANAGEMENT POLICY

AUGUST 2024

A. INTRODUCTION

Home Afrika Limited (the Company) is a Nairobi Securities Exchange (NSE) listed company established under the Companies Act, CAP 486 of the Laws of Kenya whose main service offering is to address the housing need in Africa.

B. RISK MANAGEMENT STATEMENT

The Company recognizes its responsibility to shareholders and has therefor committed to a process of risk management that is aligned to the principles of best corporate governance national and internationally and various regulations. Risk Management processes are embedded in the company's systems and processes to facilitate a risk response that is current and dynamic.

C. PURPOSE OF THE RISK MANAGEMENT POLICY

The objective of the risk management policy is to ensure that risks are managed in line with the company's criteria for risk management to ensure the Company meets its strategic and business objectives.

1.1 Definition of Terms

Risk means the quantifiable likelihood of loss or less than expected returns.

Risk Identification is the process of finding, recognizing and describing risks.

Risk Estimation is the process of estimating the risk value and its likely impact on the Company.

Risk Analysis is the process of determining the source and cause of risk and likelihood of occurrence and resultant impact.

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

Risk Treatment is the actionable process undertaken on identified risk to mitigate the exposure to acceptable levels.

Risk Management is the logical and systematic process of identifying assessing, managing and reporting all risks associated with the Company's business activities to minimize losses and maximize opportunities to pursue strategic goals.

Residual Risk is the remaining risk after the process of risk treatment.

Risk Evaluation is the process of comparing the results of risk analysis against the risk criteria to determine whether the risk is acceptable or tolerable.

Risk Owner is the person who has the responsibility to manage the identified risk.

D. RISK MANAGEMENT FRAMEWORK

1. The group's risk management is all inclusive and tasks various categories of its internal stakeholders with responsibilities that ensure that risk management is a continuous business action. The company relies on the 'three-line defense' approach to risk management. These support more effective risk management by introducing structured governance and oversight that clarifies and segregates roles and responsibilities based on the following:

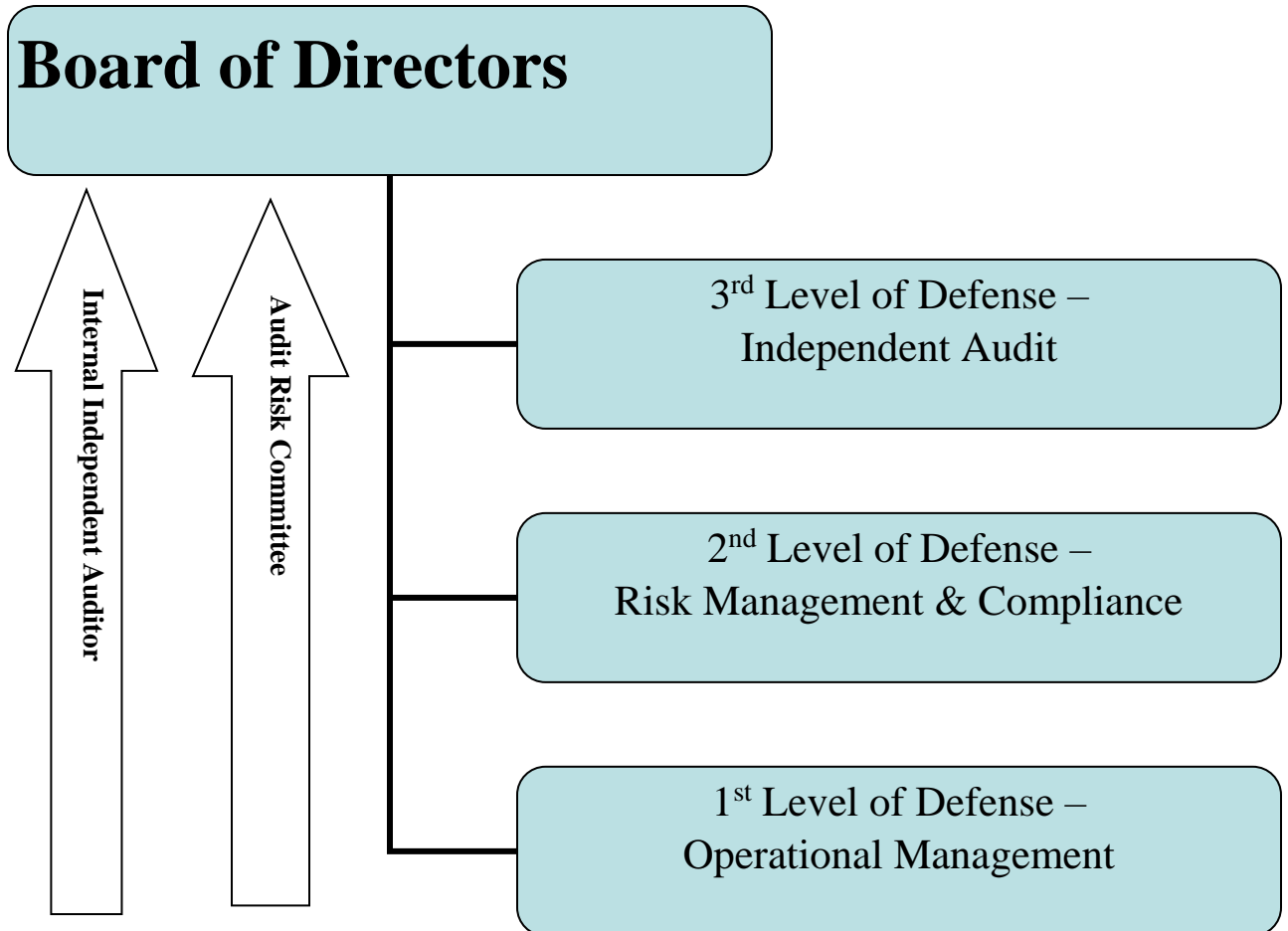
- a. **First Line of Defense - operational management:** this level is made up of frontline staff and operational management that are responsible for carrying out the daily business operation of the company. The systems, internal controls, the control environment and culture implemented by these business units is crucial in anticipating and managing operational risks. Operational management is also comprised of managers, departmental heads and unit leaders. Their functions are designed to implement detailed procedures that serve as controls and supervise execution of those procedures by their employees.
- b. **Second Line of Defense – Risk Management and Compliance:** this level of is made up of functions that provide the oversight and the tools, systems and advice necessary to support the first line in identifying, managing and monitoring risks.

Risk management and compliance in the company is comprised of managers and compliance personnel whose roles may include one or all of the following functions:

- Company functional goal setting;
- Identification of known and emerging risk factors in the company business;
- Identification of shifts in the company's risk appetite;
- Assisting the board in developing process controls to manage existing risks and arising issues;
- Facilitating compliance with all legal compliance and financial reporting requirements and standards;
- Monitoring the adequacy and effectiveness of internal control, accuracy of reporting and timely remediation of deficiencies.

2. **Third Line of Defense - Independent audit:** the functions in this level provide a level of independent assurance that the risk management and internal control framework is working as designed. It consists of the independent internal audit and the audit risk committee.

RISK MANAGEMENT DEFENSE MODEL



2. Role of the Board of Directors

The Board shall have the responsibility of establishing an effective risk management framework for the Company. The Board shall determine the Company’s level of risk tolerance and actively identify, assess and monitor key business risks to safeguard shareholders’ investments and the company’s assets. The identified risk criteria will be cascaded to Management

3. Role of Management

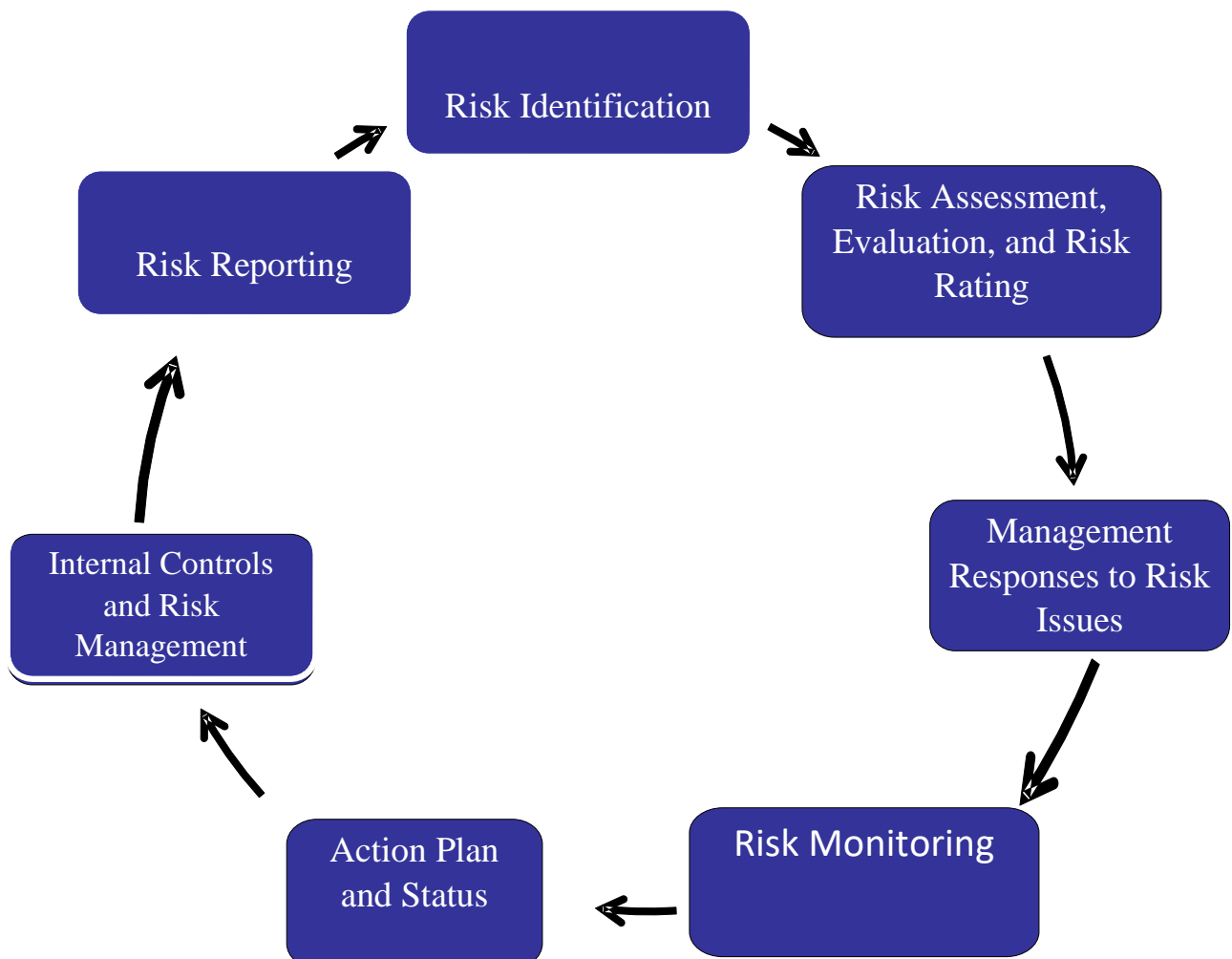
Management has the responsibility of implementing the company strategy as approved by the Board and developing policies and procedures for risk management. Risk Management reports are reviewed by the Board Audit Committee (BAC). Management is responsible for:

- a. Identifying and prioritizing risk within the Company;
- b. Assigning risk management responsibilities to managers;
- c. Reporting on risk responses and related risk control activities;
- d. Ensuring information pertaining to risk is effectively communicated to staff; and
- e. Defining adequate risk mitigation and acceptance of residual risk.

4. Role of the Risk Owner

The Risk Owner is responsible for embedding risk management objectives and making risk management a daily occurrence. Risk Owners also ensure that risks emanating from business processes are assessed at regular intervals in accordance with the Company’s management framework.

1.2 Risk Management Process



1.2.1 Risk Assessment

Risk assessment is a process that entails risk identification, analysis and evaluation.

1.2.1.1 Risk Identification:

To facilitate the creation of the Company risk register, risk will be identified companywide and listed in the Company risk register. The top ten (10) identified risks will then be allocated to respective “risk owners” who will be responsible for ensuring the risk is managed and continuously monitored. It is the responsibility of all staff to identify risk within their areas of operations and escalate this to their respective line managers for appropriate monitoring.

The group risk management framework categorizes risks as follows:

Type	Description
Strategic	Related strategic mission and objectives.
Financial	Related to economic impact (costs, revenues, budgets).
Regulatory (Compliance)	Related to legal and contractual obligations.
Management	Related to decision making, resources, policies, etc.
Operational (Technical)	Related to ICT delivery, support or management services.
Sustainability	Related to the overarching principles of protecting the environment, human rights and promoting good corporate governance.
Ethical	Related to the ability of the organization to live up to its ethical values and standards.

a) Strategic risks

These are risks that the group may not achieve its business objectives and goals. They arise from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes e.g. changes in general economic situation, customer consumption behaviors, competitors, legislation and technological developments.

The purpose of assessing strategic risks and opportunities is to identify the business operations which can be deployed to attain the objectives taking into account manageable risks, and also avoiding those business operations which involve unreasonably high risks. A failure to identify or leverage opportunities in the market is also considered a strategic risk by the group.

b) Operational risks and Compliance risks

These are risks resulting from weaknesses in internal control processes, people, inadequacies in system and processes, human error, fraud, legal issues and physical or environmental processes through which the group operates. The aim is to avoid or reduce operational risks, taking into consideration the cost of controls measures in relation to the scope of risk.

c) Credit risks

Credit risk refers to the risk that the group customers will default on the debt by failing to make required payments. The risk is primarily that of the group and includes lost amount of receivable, disruption to cash flows, and increased collection costs.

d) Liquidity Risks

The risk arising out of the possibility that the group will not be able to meet its financial obligations as and when they fall due. It arises when the group is unable to generate sufficient cash flows to enable it meet its financial obligation as and when they fall due. It's mainly results from mismatches in the maturity patterns of the group's assets and liabilities.

e) Reputation Risks

Risk of loss resulting from damages to the group's reputation, in lost revenue, increased operating costs or destruction of shareholders' value, consequent to an adverse event. Adverse events typically associated with reputation risk include ethics, safety, security, sustainability and quality of goods and services supplied.

f) Market Risk- Interest Rate and Foreign Currency Exchange Risks

Market risk is the risk of losses in earnings arising from movements in market prices i.e. interest rates, foreign currency exchange rates, commodity prices etc.

Interest rate and foreign currency exchange risks are the risks that the earning / profits of the group will be negatively affected by adverse movement in interest rates and foreign exchange rates respectively.

g. Sustainability Risks

Sustainability risks are the potential challenges that arise from environmental, social, and governance (ESG) factors. ESG entails:

- a) **Environmental Risks**-Environmental risks involve climate change, resource depletion, pollution, and biodiversity loss. For businesses, these risks can manifest as regulatory penalties for non-compliance with environmental standards, increased operational costs due to resource scarcity, or disruptions caused by climate-related events such as floods.
- b) **Social Risks**- Social risks pertain to how a company manages its relationships with employees, communities, and consumers. Poor labour conditions, human rights violations, or neglecting employee health and safety can result in labour strikes, legal action, and a damaged reputation.
- c) **Governance Risks**- Governance risks arise from inadequate corporate governance practices, including corruption, lack of transparency, and poor decision-making. These risks often result in legal actions, financial mismanagement, and erosion of stakeholder confidence.

h. Ethical Risks

Ethics risks refers to risks that could affect the ability of the Company to live up to its ethical values and standards, undermining trust and reputation and threatening financial and operating performance. Ethical Risks include conflict of interest, fraud, corruption and anything that prevents progress with regards to social, environmental, and economic outcomes. This risk occurs when there is departure from the set Company code of standards and ethics.

1.2.1.2 Risk Analysis

Risk Analysis involves the identification of causes and sources of risk. It provides a key input to risk evaluation and respective risk treatment. Generally identified risk in term of likelihood and impact are categorized into critical, high, medium and low risk as follows:

- a. **Critical Risk**- Has potential to create severe negative impact to the Company and must be reported to the Board of Directors and the Board Audit Committee. Any recommendation made on risk treatment must be implemented immediately.
- b. **High Risk** – Has potential major impact to the Company but can be managed and mitigated and is therefore reported to the Management. Any recommendation made on risk treatment must be implemented immediately.
- c. **Medium Risk**- Exposure had moderate impact to the Company. Any recommendation made on risk treatment must be implemented within the agreed timelines.
- d. **Low Risk**- Exposure has no significant impact to the Company however as best practice any recommendations made must be implemented in due course

1.2.1.3 Risk Assessment, Evaluation & Rating

The risks identified are evaluated/assessed and prioritized on the basis of their significance by assessing the impact and probability of their occurrence and the quality of risk management procedures in place.

The impact and probability of occurrence is categorized as low, medium or high while the quality of risk management is defined as weak, acceptable or strong. Aggregate risk exposure is low, moderate or high for each risk category.

Risk Register

The chief finance officer prepares an aggregated risk register capturing the key risk, mitigating controls and any additional details in the prescribed format.

The following parameters are used for rating the risk scales.

Impact	Description	Insignificant	Minor	Moderate	Major	Extreme
Financial	Loss	None	KES 20,000 to KES 50,000	Kshs.50,000 to Kshs.100,000	KES 100,000 to KES 200,000	Above KES. 200,000
Reputation	Letters /Press complaint from customers and business associates	One off complaint by customers/business associates/Stakeholders	Series of complaints by customers/business associates/Stakeholders	Series of articles or complaints in press business associates/Stakeholders	Extended negative coverage & short-term disruption of customer/business associate confidence	Extended negative coverage and disruption of customer/business associate confidence
Regulatory	Penalties to business closure	No penalties	No penalties	Minor penalties	Major penalties	Major censure
Business Disruption/Operational Risk		No business disruption	One off/short term business disruption leading to minor loss.	One off/short term business disruption leading to minor loss.	Medium term business disruption leading to moderate loss.	Business disruption leading to major loss.
		Junior staff required to resolve	Middle level management required	Middle level management required	Business head effort required	MD effort required

Table (b) Risk Register

Likelihood parameters

Quantification criteria for likelihood					
Likelihood	Rare	Unlikely	Possible	Likely	Almost Certain
	Event may occur only in exceptional circumstances	Event could occur at some time	Event should occur at some time	Event will probably occur in most circumstances	Event is expected in most circumstances
	0-15%	15-30%	30-50%	50-90%	>90%
Quantification of Criteria of impact					
Impact Rating	1	2	3	4	5
	Insignificant	Minor	Moderate	Major	Extreme
	No injuries low financial loss, no risk to reputation.	Minor First aid treatment, on-site release immediately contained, medium financial loss, some customer dissatisfaction.	Medical treatment required, on-site release contained with outside assistance, high financial loss and public visibility.	Major extensive injuries, loss of production capability, invocation of disaster recovery with no detrimental effects, major financial loss.	Death, off-site with detrimental effect, huge financial loss.

Table (c) Likelihood Parameters

Once the above risks are analyzed they are plotted on a heat map and shared with audit committee as per below color codes.

	Consequences				
	Insignificant	Minor	Moderate	Major	Extreme
Likelihood	1	2	3	4	5
A (almost certain)	H	H	E	E	E
B (likely)	M	H	H	E	E
C (possible)	L	M	H	E	E
D (unlikely)	L	L	M	H	E
E (rare)	L	L	M	H	H

Key	Description
E	Extreme Risk: Immediate action required to mitigate the risk.
H	High Risk: Action should be taken to compensate for the risk.
M	Moderate Risk: Action should be taken to monitor the risk.
L	Low Risk: Routine acceptance of the risk.

Table Risk Heat Map

1.2.1.4 Risk Treatment

Risk Treatment is undertaken to select one or more options for managing risk and implementing chosen options. When selecting the most appropriate risk treatment consideration should be made for costs and

effort against the benefits that will be derived to the Company with regards to compliance. For each risk identified by evaluation the following options are available:

- a. **Risk Acceptance-** This is generally used for low risks which are acceptable to the Company and are contained in the Company risk register.
- b. **Risk Avoidance-** By adopting risk avoidance the Company will implement appropriate changes to the business to ensure the risk is eliminated.
- c. **Risk Mitigation-** For this option both technical and non-technical options are implemented to reduce the threat and risk impact.
- d. **Risk Transfer-** This involves transfer of the existing risk to other companies affiliated with the Company.

1.2.2 Risk Communication and Consultation Reporting and Risk Calendar

1.1. Risk reporting

Most of the internal reporting and day to day interactions between senior management and business functions ensures that senior management is aware of key risks and unusual incidents or loss events.

Formal risk reporting has been developed by the company to highlight key risks and effectiveness of risk management systems

The following is a summary of the risk management reporting that communicates the risk profile and risk mitigation efforts.

a) Company and Business Risk profile

Key risk dashboards are implemented to review risk levels at a company level as well as at business function levels.

b) Risk monitoring and risk calendar

As the risk exposure of any business may undergo change from time to time due to continuously changing environment, the updating of the risk matrix will be done on a regular basis

The Chief finance officer shall maintain a risk calendar that outlines the frequency of performance of various risk management initiatives.

The risk calendar is presented on the table below;

Risk Management Activity	Responsible person	Reporting to	Frequency
Updates to current Action Plan	Unit head	Execute action items identified in the action plan. Review and update the action plan regularly	Regularly/ As needed
Updates to current action plan	Chief Finance Officer	Take updates from all units and update the companywide action plan	Monthly
Risk Heat Maps	Chief Finance Officer	Develop departmental heat maps and report as Risk Dashboard Audit Committee representative	Quarterly
Summary of Incidents Occurred	Chief Finance Officer	Compile a summary of risk/loss incidents and present to management	Quarterly
Review of risk register	Chief Finance Officer	Update risk register and share with unit heads and audit committee	Half yearly
Review and revision to Risk management policy	Chief Finance officer/Audit Committee	Update Policy	Annually

Table: Risk Monitoring Calendar

c) Quarterly Review of Risk Management Framework

Progress on implementation of risk management systems is reviewed by the Audit and Risk Committee on a quarterly basis and submitted to the Board as part of the Board reporting Package.

The purpose of risk management communication and consultant is to allow Management to:

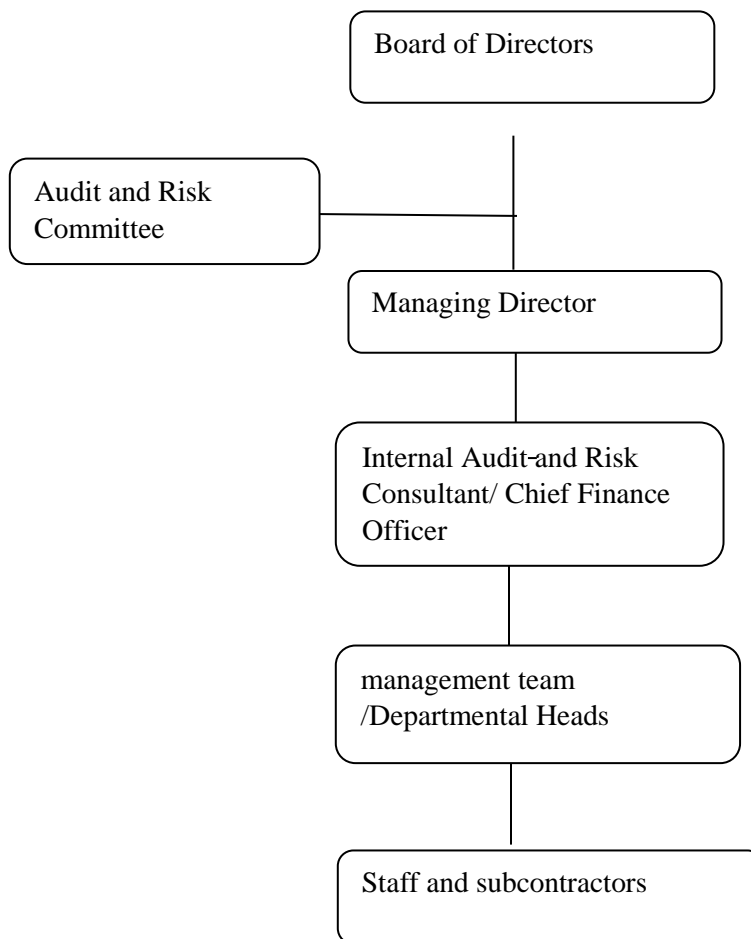
- a. Understand the risk profiles;
- b. Report on risks within the guidelines issued by the Board;
- c. Develop a baseline for early detection of critical or major risks
- d. Identify unfavourable risk trends to permit corrective actions to minimize organization risk.

Generally, risk reports within the Company will be shared with (1) the Board of Directors, Managing Director and Board Audit Committee (2) Management and (3) Staff designated as the risk owners. Risk Assessment for the Company will be executed annually or upon significant business changes or the addition of new business processes or assets.

RISK MANAGEMENT STRUCTURE AND RESPONSIBILITIES

The company’s ability to conduct effective risk management is dependent upon having an appropriate risk governance structure and well defined roles and responsibilities.

Figure below: Risk Management structure



INTEGRATION OF AUDIT AND RISK MANAGEMENT

The system of internal control incorporates risk management. It encompasses effective and efficient operations enabling the company to respond to a variety of operational, financial and commercial risks. These elements include

1.1. Policies and procedure

Policies and procedures are the foundation for an effective internal control framework that then supports a strong risk management framework. Written procedures support the policy where appropriate.

Individual business units are responsible along with support from business excellence and chief finance officer for establishing effective internal controls within various business processes. Effective design and implementation of the internal control framework is validated by regular internal audits and test of controls for these units.

1.2. Business planning and budgeting

The business planning and budgeting process is used to set objectives, agree action plans and allocate resources. Progress towards meeting business plan objectives is monitored regularly.

1.3. Independent internal audit function

A risk based internal audit approach is adopted by the company to ensure adequacy and effectiveness of internal control and policy framework.

1.4. Audit committee


The Audit committee reports to the board on internal controls and risk matters including any emerging issues.

2. RISK MANAGEMENT POLICY REVIEW

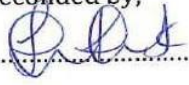
The Chief Finance Officer shall have the ownership of the risk management policy and shall be responsible for implementation of all its aspects across the business units. This policy framework will be reviewed at least annually by the audit and risk committee and the Board to assess its effectiveness and to ensure continued application and relevance.

Team	Responsibilities
Board of directors	i. Provided oversight and review of the groups risk management policy and process
	ii. Reviews most significant risks and responses to manage them as presented by the audit and risk committee
	iii. Assesses the efficiency and effectiveness of the group risk management process.
Audit and risk Committee	The Audit committee assists the board to carry out its oversight responsibilities relating to financial risk management and reporting as follows
	i. Reviews the risk register to assess the risk status of the group
	ii. Reviews and endorses the risk strategy for the group
	iii. Reviews the risk register and risk management framework of the group as presented by the audit and risk consultant
	iv. Ensures that management monitors the effectiveness of internal control system
Managing Director	i. Ensures that the risk is managed across all the group activities through review of risk management reports presented by the Chief Finance Officer
	ii. Drives the culture of risk management at the top
Chief Finance Officer	i. Develop and communicate organizational policy and information about the risk management program to all staff and where appropriate to the relevant business associates
	ii. Undertaking risk assessment and maintenance of an up-to-date companywide risk register
	iii. Work with risk owners to ensure that the risk recommendations are implemented in accordance with the policy of the risk management
	iv. Review the risks rating of each department
	v. Conducting risk management reviews regularly to ensure they are in line with the group risk management policy and conduct workshops on risk identification
	vi. Presenting to the audit and risk committee on significant risks affecting the group on a quarterly basis
Management team	i. Responsible for implementing risk management policies across their respective areas of operations.
	ii. Regularly review and manage risks within their units
	iii. Identify any risk deficiencies in terms of controls within their units
Staff and contractors	i. Comply with all risk management procedures
	ii. Identifying, managing and monitoring risks within their areas of accountability
	iii. Communicating these risky issues to their managers
	iv. Taking measures to ensure their safety and that of other employees, customers and third parties.

Approved by the Board of Directors on the^{31st}..... Day of AUGUST..... 2024


.....
Chairman of the Board

31st AUGUST 2024
.....
Date

Seconded by;

.....
Director

31st AUGUST 2024
.....
Date