FEDERAL MORTGAGE BANK OF NIGERIA

Enterprise - Wide Risk Management Framework

Contents

1. Introduction

The Federal Mortgage Bank of Nigeria (FMBN) operates as a vehicle for increasing the mobilisation of long-term funds, lending volume and expansion of mortgage lending services to all segments of the Nigerian population. The Bank manages and administers the contributory savings scheme known as the National Housing Fund (NHF) which is a pool that mobilizes long-term funds from Nigerian workers.

The Bank's statutory mandates are to mobilise deposit liabilities through National Housing Fund collection, creation of quality risk assets for revenue generation, facilitation of affordable home ownership for qualified NHF contributors and provision of Home Renovation Loan to Nigerians. To achieve this, the Bank finances mortgages created by Primary Mortgage Banks (PMB) under the NHF scheme and also gives Estate Development Loans (EDL) at soft interest rates to contributors.

We are aware that we must maintain a critical balance between the pursuit of growth and the need to have a firm control of the risks facing the business. Therefore, this Enterprise-wide Risk Management Framework ("the Framework" or "this Framework") reflects the commitment of the Board and Management to establish and maintain good risk management practices in the Bank.

1.1. Purpose of the Enterprise-wide Risk Management Framework

This Framework articulates the broad guidelines to ensure consistency in the actions taken by the Board, Management and staff of the Bank to manage the risks that could impede the achievement of the Bank's statutory objectives. The issues covered in the framework are fundamental to the process of identifying, measuring, controlling, monitoring and reporting the risks facing the Bank.

More specifically, the framework:

- Sets out clearly how risk is viewed and addressed in the Bank to ensure that the actions and activities of management and staff with respect to risk management are consistent with the need to meet stakeholders' expectations;
- Creates the platform through which risk management is integrated into the business practices and decision making activities of the Bank;
- Provides the means to communicate the Bank's risk management philosophy, principles, policies, strategy and governance structure to staff and other stakeholders in order to promote a good risk culture;
- Ensures the Bank's compliance with regulatory requirements;
- Enables the Board and Management to understand the key risks facing the Bank and the process for managing them in order to optimise the risk-return trade-off; and
- Ensures the Board and Management have reasonable assurance that risks faced by the Bank are being managed effectively.

1.2. Ownership of the Document

The ownership of the framework lies with the Board of Directors of the Bank. The Head, Risk Management Group, has the responsibility for implementing the framework across the Bank under the supervision of the Managing Director and shall establish and communicate the detailed procedures for managing risk to staff from time to time to enable the effective monitoring for compliance with the framework.

1.3. Review of the Framework

This framework shall be subject to continuous review and update at least every two years. The Group Head, Risk Management shall assume responsibility for the review and update of this framework. The various Group Heads may also propose changes based on the outcome of the risk management review. However, any proposed changes must receive the approval of the Managing Director.

The periodic review and update shall be to ensure the appropriateness and robustness of the Risk Management Framework given the nature, scope and complexity of the Bank’s activities.

The outcome of these reviews and other monitoring activities shall influence the decisions to enhance this framework and the approach for the management of risk within the Bank.

The final approval for the revision of this framework rests with the Board of Directors.

2. Risk Management in the Bank

2.1. Enterprise-wide Risk Management

Enterprise-wide Risk Management (ERM) is defined as a structured and disciplined approach to the management of risk that considers the strategy, assets, liabilities, process, people, technology and resources within the business with the purpose of continually evaluating and managing risks to business strategies and objectives on an enterprise-wide basis.

It is a continuous process that seeks to aggregate and integrate risk management activities across all risk types in order to maximise the risk-adjusted returns.

2.2. Risk and Risk Management

Risk is defined by FMBN as the likelihood that an event would occur that will affect the achievement of the Bank's objectives. This event can be induced by internal and external factors. The internal risk event may arise from operational failures, fraud, people-related issues such as non-compliance with internal policies and procedures. External risk events, on the other hand, may arise from unexpected regulatory changes or natural disasters. Risk is integral to the way of doing business, and we recognise that risk can result in either better- than-expected or worse-than-expected outcomes.

In FMBN, we acknowledge that 'risk is risky' but also accept that 'disregarding risk is even riskier'. We shall therefore seek to understand risk, how it is caused and what influences it so that we will be able to change the things that cause and influence risk in our favour. In so doing, we will be in a position to achieve our objectives more efficiently.

Risk management is simply the coordinated activities to direct and control the Bank with regard to risk. It is the comprehensive process of identifying, assessing and responding to risk. Effective risk management will bring about comfort that we can deliver desired results, manage risks and threats well, and make informed decisions about opportunities that come up in the course of business.

2.3. Risk Philosophy, Principles, Culture and Objectives

2.3.1. Risk Philosophy

Our risk management philosophy and culture are the set of shared beliefs, values, attitudes and practices that govern how we consider the risk inherent in our business activities, from points of strategy development to our day-to-day implementation of same. We believe that an efficient risk management system across all lines of our business will ensure more efficient use of capital and resources and reduce the likelihood of operational and financial losses. We consider risk management to be a Bank wide imperative and a key driver towards the effective and efficient delivery of our mandate and the attainment of our strategic objectives. As such, we are committed to:

> Building a strong risk culture, sound corporate governance and a proactive risk management process while creating value for our stakeholders.

Maintaining an integrated enterprise-wide approach to risk management using clearly defined standards, guidelines, policies, limits and procedures;

Giving due consideration to risk issues in decision making across the

Bank; Building a shared perspective on risk within the Bank;

Making risk management an integral part of job and performance appraisals of our staff;

Ensuring that risk controls do not constitute an impediment to the achievement of our strategic objectives;

Continually reviewing our activities to determine the level of inherent risks, and the controls to mitigate the risks. Our decisions are based on careful analysis of the implications of such risks to our strategic objectives and operating environment; and

Ensuring that our risk management program will equip our people with the tools and capabilities to overcome the barriers that arise in striving to exceed expectations.

2.3.2. Risk Management Principles

Embedding – ERM shall be fully embedded within the major functional and operational processes just as strategic planning and performance measurement system.

Consistency – We shall adopt a consistent method for the identification, assessment, mitigation, control, monitoring and communication of risks associated with all of our activities, functions, processes, and events in an effort to efficiently and effectively achieve our corporate objectives.

Risk Awareness – A result driven and risk awareness culture shall be nurtured to move the Bank to a position where decisions are taken with full consideration of relevant risks and their implications.

Ownership – Specific risk owners within the Bank's workforce as well as the members of the Board shall have sound understanding of the risk impacting their operations or areas of responsibility and be able to respond with appropriate strategies and mechanisms to identify, assess, monitor, and control those risks.

Accountability – Risk owners within the Bank's workforce shall be accountable for the risk management actions in their respective areas of responsibility. The Board shall provide adequate oversight, control, review and approve risk strategies, plans and budgets prepared by management.

Authority – Risk owners must have the required level of authority and flexibility to determine and execute the proper course of action to manage the risk in their respective areas of responsibility.

Communication – Our information system will be continually updated to accommodate data output necessary for proper assessment and monitoring of risks.

2.3.3. Risk Culture

Consequent to our risk management philosophy, we will strive to entrench the following attributes as guiding principles of our risk culture:

The Board shall set the tone for enterprise-wide risk management across the Bank with a view to promoting an appropriate risk - aware culture.

We shall institute a sound risk governance structure that enables us to manage all major aspects of our activities through an integrated planning and review process.

The Board and management of the Bank shall establish and promote a strong culture of adherence to limits in managing risk exposure.

Risk management shall be governed by formally documented and defined policies and procedures, which are clearly communicated to all staff.

We shall avoid investments that we do not fully understand or for which we cannot reasonably and objectively measure or manage the associated risks.

We shall strive to maintain a balance between risk/opportunities and revenue consideration with our risk appetite. Thus, risk-related issues will be considered in all our business decisions.

Our risk officers shall be empowered to perform their duties professionally and independently within clearly defined authority.

Staff will be encouraged to disclose inherent risks and actual losses openly, fully and honestly.

We shall create a process for institutionalising the lessons learned from a risk event and will frown at any reoccurrence.

We shall carry out extensive risk assessment and analysis before operational and strategic decisions are taken.

2.4. Risk Management Objectives and Strategy

2.4.1. Risk Management Objectives

Our risk management objectives are as follows:

To ensure that our business growth plans are consistent with our risk appetite and supported by an effective and efficient risk management function;

To identify any real and perceived risks exposures that may impact or be associated with the effective and efficient management and co-ordination of the Bank's activities;

To integrate risk management into the culture and strategic decision making processes of the Bank;

To optimize our risk and return trade-offs by ensuring our business units act as primary risk managers while establishing strong and independent review and assurance structures;

Ensure that top management as well as individuals responsible for risk management possess the requisite expertise and knowledge to accomplish their functions;

To comply with appropriate regulations and leading industry practices.

2.4.2. Risk Management Strategy

Our strategy for managing risks is to implement and continuously improve the Enterprise- wide Risk Management framework. To ensure the successful implementation of our risk management strategy, we shall maintain an independent risk management function which shall be responsible for implementing this Framework. The function shall promote the establishment of a sound risk culture that is commensurate with the Bank's mandate and risk appetite.

In order to protect its reputation, the Bank shall actively engage its stakeholders and disclose relevant risk information within its annual reports. These disclosures would cover qualitative information on risk policies and practices as well as quantitative information.

To achieve a holistic and regular risk analysis and reporting, we shall also maintain an enterprise data warehouse that captures, disseminates and stores internal data inputs. The data warehouse shall include daily or weekly feeds of external market data from providers such as Bloomberg, Reuters and external credit rating agencies such as Fitch, Standard and Poor's and Moody's Investors.

2.5. Risk Appetite and Tolerance

Our risk appetite articulates the amount and types of risk we are prepared to pursue, accept or reject to achieve our strategic objectives. The Bank shall use the risk appetite statement to set the tone, quantum and direction of its risk-taking activities. The risk appetite shall be central to embedding a risk culture in business decision making, day-to-day risk management and risk reporting.

Management shall define and recommend to the Board for approval a process for setting the risk appetite and allocating the appetite among the business units.

In general, we shall adopt a moderate approach to risk taking in pursuance of our mandate. However, in times of stress where this is not realistic, we may refine the risk tolerance upward. We shall apply principles which govern lending to protect our credibility but with due regard to preventing moral hazard.

The risk appetite will apply to the Bank's reputation, financial position, key stakeholders, regulatory and Health, Safety and Environment.

Risk limits that are consistent with the Bank's mandate and strategy shall be set to reflect the Bank's overall risk appetite. These limits shall be defined in financial (loss) or operational (exposure) terms at lower thresholds than the quantitative measures of risk appetite such that they act as triggers for action.

3. Risk Management Governance Framework

3.1. Introduction

This section of the framework explains the structure for managing risks within FMBN. It describes the risk governance structure as well as the roles and responsibilities of staff in the management of risks.

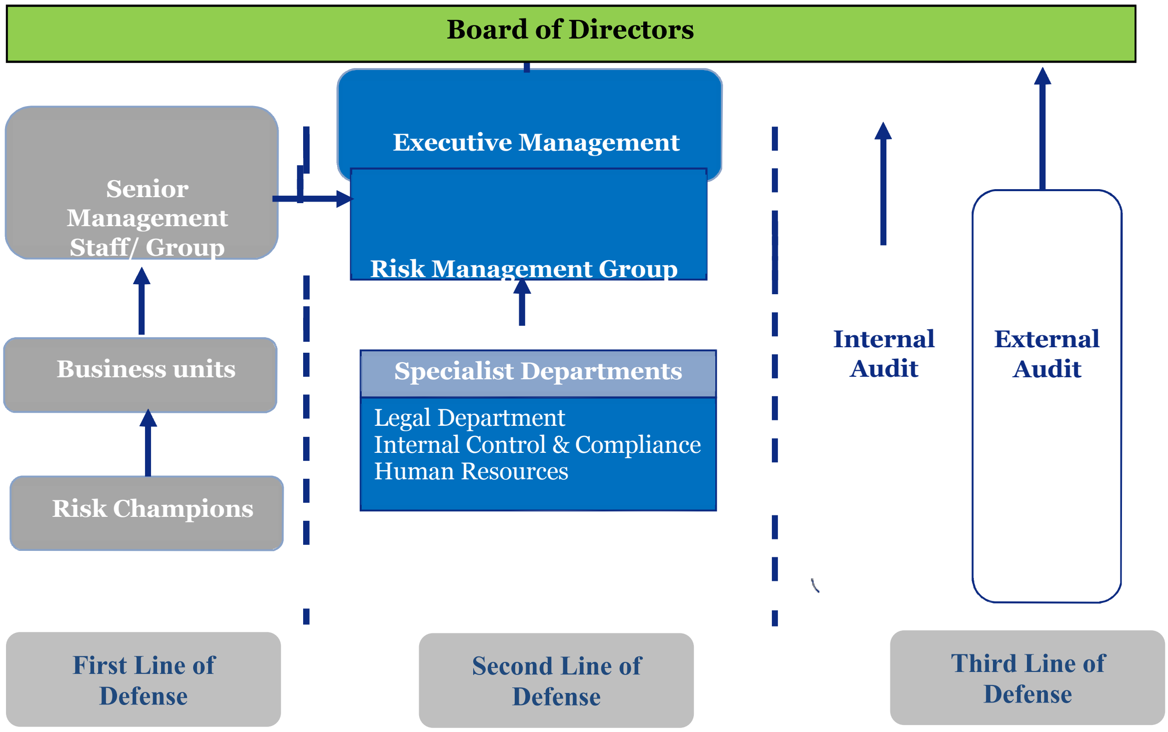


Figure 3.1: Risk Management Lines of Defence

The Board sets the tone for the management of risks across the Bank. It has primary responsibility for ensuring that an effective system of risk management and controls exist across the Bank. The Executive Management and the Risk Management Committee have delegated authority from the Board.

3.2. Risk Management Governance Structure

In order to properly govern and operationalise our risk management strategy, we shall adopt the industry standard 'three lines of defence' model, as shown above, in which the role of the Risk Management Department is to advise, challenge and oversee the 'first line' in relation to the type of risks that they are exposed to and how they are managed.

3.2.1. First line of defence – Risk management and ownership

The first line of defence is made up of the Bank's business units with primary responsibilities. Each group shall own the risks associated with their activities and have first line responsibility for managing these risks. Most preventive controls are implemented at this level as this is where business processes are initiated, recorded and executed. Detective controls help to manage control breaks at the transaction level.

The primary responsibilities and objectives of the first line of defence are to:

Identify emerging risks at the transaction/business case level;

Execute risk assessment and support the development of the risk register;

Develop and implement procedures, practices and lines of authority that translate the Board's goals, objectives and risk appetite/tolerance into operating standards that are well understood by the staff;

Ensure that appropriate controls are embedded in each activity to mitigate the risks associated with the business units' processes;

Create adequate awareness to promote a risk aware culture within their respective the business units;

Promptly address weaknesses in the business units' controls;

Promptly report material risk events including near misses; Incorporates risk consideration into all major decisions;

Include the consideration of risk management events/issues as a standing item in management meetings;

Promptly deliver periodic reports to the second and third lines of defence.

3.2.2. Second line of defence – Risk oversight

The second line of defence consists of all risk and control functions responsible for developing and implementing a uniform approach to risk management across the Bank. These functions provide independent risk oversight & monitoring and evaluating the effectiveness of the Bank's risk management processes. The second line of defence is responsible for the following:

Develop and coordinate the implementation of the Bank's Risk Management Framework and policies.

Providing oversight over key risks to which the Company is exposed.

Establish systems and procedures relating to risk identification, measurement and control.

Monitor across the Bank the current status of risk parameters and limits established by the Board.

Assist the business units to proffer remedial measures to address identified risks.

Provide risk advisory and report to the Board and stakeholders as appropriate.

Conduct risk profiling and facilitate business units risk self-assessments.

The Risk Management Group is responsible for leading and coordinating the implementation and maintenance of the Bank's Enterprise Risk Management (ERM) Framework. The Group is responsible for providing risk advisory to all other groups and Management as well as promoting risk management best practices through the provision of a suite of risk mitigating policies, procedures, tools and templates.

3.2.3. Third line of defence – Assurance functions

The third line of defence consist of all functions with primary responsibilities for assessing and providing independent assurance on the adequacy, appropriateness and effectiveness of the Bank's overall risk management framework, policy and risk plan implementation. It provides independent perspectives on the overall control framework and tests the adequacy of the control's design and effectiveness. The main duties of those in this line of defence include:

Providing oversight on the risk management process;

Performing internal control reviews based on a rationalised and systematised approach that allows for risk assessment and governance reporting;

Reporting to the Board on:

- The state of the control environment;
- Gaps in the controls or monitoring environment;
- The status of remediation plans; and
- Potential current and future risks.

3.2.4. The lines of defence

In summary, the primary responsibility for controlling and mitigating risks on a day-to-day basis rests with the Group heads. All employees are to imbibe the practice and culture of proactive enterprise risk management in carrying out their respective roles. The Group heads should see to it that emphasis is placed on the careful analysis and control of risk as a vital part of each business process.

Employees at all levels across the Bank are required to comply with the Bank's ERM Framework and the risk related policies. Bank staff are responsible for ensuring compliance with this Framework and other risk policies, procedures and guidelines.

Unit heads own the risk management process within their respective business units. As a result, they are responsible for ensuring that risk events are duly identified and reported in a timely manner. They shall ensure that adequate resources are allocated to carry out risk management activities at all times and that risk consideration is a key factor in decision making.

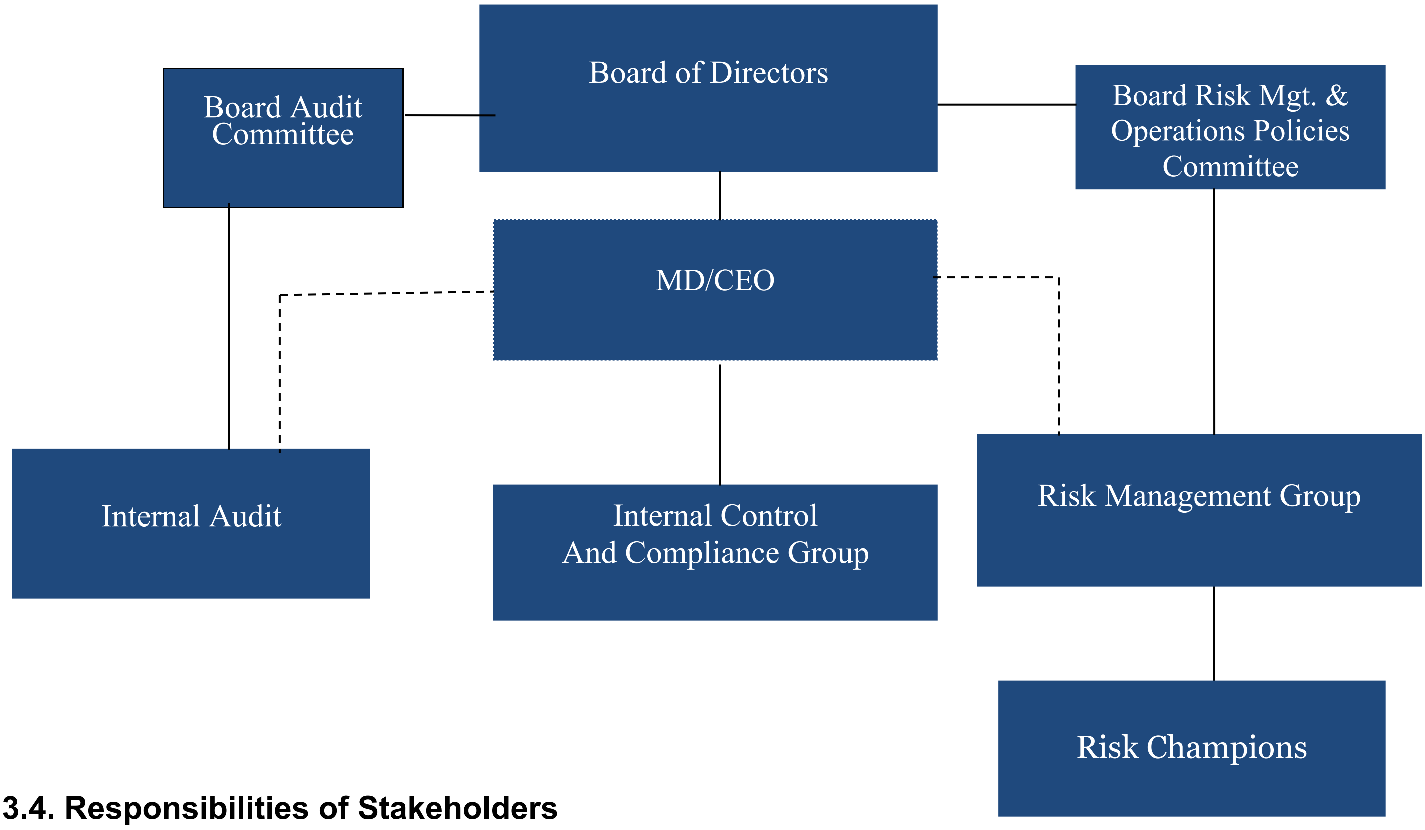
Risk Champions are representatives from each group who act as the conduit between their respective groups and the Risk Management Group.

Finally, Internal Audit is in the third line of defence and so carry out independent check to ensure adherence to approved policies and procedures.

3.3. Enterprise-wide Risk Management Structure

The enterprise-wide risk governance structure outlines the roles, authorities and responsibilities in relation to managing material risks in the Bank.

Figure 3.2: Risk Management Structure



3.4. Responsibilities of Stakeholders

The Bank's risk governance structure shall be supported by a clear and explicit articulation of the ownership, accountability and responsibilities for the different components of ERM within the Bank. The key elements to the Bank's risk governance structure are as follows:

3.4.1. Responsibilities of the Board

a. Sets the tone for the management of risks across the Bank.

b. Approves the risk strategy and appetite for the Bank, based on recommendations from the Board Risk Management Committee.

c. Sets the risk parameters and tolerances within which the Bank conducts its activities.

d. Reviews and approves the ERM framework and risk policies as well as ensures they are appropriate for the achievement of its strategic objectives.

e. Sets the parameters for the approval of waivers and exceptions to the provisions of the ERM Framework and associated risk policies.

f. Monitors the Bank's enterprise-wide risk profile, risk exposures, and risk management initiatives.

g. Approves risk systems to facilitate the management and monitoring of the Bank's risk profile.

h. Reviews risk reports and directs remedial and / or mitigating actions as appropriate.

i. Institutes appropriate reward and sanction system in line with the Bank's risk appetite.

j. Provides oversight of the Bank's risk management and ensures adequate resources are allocated to risk management activities.

3.4.2 Responsibilities of the Board Risk Management and Operations Policies Committee

The Committee shall assist the Board in its oversight of risk management. The Committee's responsibilities are as follows:-

a. Review and recommend on an annual basis or as may be required an appropriate risk strategy and appetite to the Board for approval.

b. Assist the Board in fulfilling its oversight responsibilities with respect to risk management across the Bank.

c. Determine the Bank's risk appetite and monitor the risk profile against the risk appetite.

d. Ensure that roles and responsibilities for risk management activities are clearly defined.

e. Monitor the Bank's risk profile, risk exposures, and risk management initiatives and make recommendations to the Board.

f. Recommend risk systems and solutions to facilitate the management and monitoring of risks bank-wide.

g. Create an atmosphere of open communication between the Internal and External Auditors and the members of the Executive Management.

h. Review risk reports and make appropriate recommendations to the Board.

3.4.3. Responsibilities of Executive Management Committee

The Executive Management shall be responsible for the following:

a. Documenting the Bank's risk management policies and strategy and on approval by the Board carry out the implementation.
b. Ensuring there are policies and procedures for identifying, measuring, controlling, monitoring and reporting risks.
c. Reviewing the findings from risk assessment and making appropriate recommendations.
d. Superintending over the implementation of risk treatment plans.
e. Ensuring that the quality and quantity of staff deployed to risk management activities are adequate.
f. Ensuring the timely consideration of risk events.
g. Monitoring the Bank's risk profile to ensure that it does not fall out of the agreed risk appetite by way of the activities undertaken.

h. Reviewing and recommending risk limits.
i. Reviewing and monitoring business units key risk indicators.

3.4.4 Responsibilities of the Risk Management Group.

The Risk Management Group shall provide technical assistance and advice to business units on the identification, evaluation, control, monitoring and reporting of risks within their units.

The following are important elements of the Group's responsibilities:

a. Develop risk strategy and appetite for Executive and Board consideration.

b. Champion the implementation of the Enterprise-wide Risk Management Framework across the Bank.

c. Recommend waivers or exceptions to the provision of this framework and related risk policies to the appropriate Board Committees.

d. Articulate and recommend risk management strategies.

e. Coordinate the implementation of risk management strategies, initiatives, policies and key risk indicators.

f. Monitor risk limits and make recommendations as appropriate.

g. Facilitate risk assessments and make recommendations to the appropriate Board and Management committees.

h. Recommend appropriate reward and sanction system with a view to embedding an appropriate risk aware culture across the Bank.

i. Recommend and obtain approvals for risk limits.

j. Custodian of the ERM framework, risk register, risk policies.

k. Ensure proper documentation to ensure consistency of actual control descriptions, control registers, flow charts and related procedures.

l. Ensure that controls, skills and systems are in place to enable compliance with the Bank's policies and standards.

m. Provide the Management with practical, cost effective recommendations for mitigating risks.

n. Promote risk awareness and provide education and training on risk management

o. Provide assurance on the effectiveness of risk treatments and related control activities.

p. Drive the annual review and update of the Bank's risk management policies and procedures.

3.4.5. Responsibilities of Group and Unit Heads

Group and unit heads are responsible for the first line of defence in the management of risk. They are expected to put in place preventive and detective controls in the business "frontline" and make recommendations to mitigate identified risks. Other responsibilities of unit heads include ensuring:

a. The development and implementation of risk management policies and procedures that address individual unit objectives and ensure consistency with corporate objectives;

b. That operational activities are carried out according to risk management policies and procedures for individual units; and

c. That recommendations are made from time to time about the appropriateness and adequacy of risk management policies and procedures for their respective units.

3.4.6. Responsibilities of Every Employee

Risk management is the responsibility of everyone at FMBN and therefore shall constitute a critical aspect of every employee's job description. The following shall include the responsibilities of staff:

a. Perform their duties in accordance with risk management policies and procedures (Including the code of ethics).

b. Report to their Unit Heads instances where they consider risk management procedures inadequate or inefficient enough to address the risk under consideration.

c. Identify and evaluate risks towards the achievement of the strategic objectives.

d. Capture, monitor and report risk events.

e. Provide information for updating the risk register and implement risk treatments.

f. Collaborate with Risk Management Group to develop, monitor and report on key risk indicators.

3.4.7 Internal Audit Unit

Internal Audit Unit shall have the following responsibilities:

a. Independently assess and evaluate the adequacy and effectiveness of the Bank's Risk Management Framework.

b. Perform periodic review to determine compliance with the Bank's risk policies.

c. Assess the adequacy of the Bank's risk assessment and measurement methodology.

d. Assess the effectiveness of the Bank's risk monitoring and reporting process.

e. Collaborate with the Risk Management Group and business units to ensure that emerging risks are effectively identified, measured, mitigated, monitored and reported.

3.4.8. Specialist units - Legal Department, Internal Control & Compliance and Human Resources

a. Work with the Risk Management Group to perform periodic risk assessments of related control activities across the Bank.

b. Perform assessments of new and existing laws, regulations and best practices affecting the Bank in order to identify and mitigate potential areas of non- compliance and other emerging risks.

c. Provide copies of assessment reports to the Risk Management Group to ensure emerging risks identified during assessments and reviews are captured on the Enterprise Risk Register.

3.4.9. Risk Champions

a. Serve as an interface between the 1st and 2nd lines of defence and represent their respective BUs in the Risk Champion Network.

b. Assist in promoting a risk aware culture.

c. Assist in identifying emerging risk trends.

d. Support the implementation of risk mitigation.

e. Facilitate training and awareness for members of their respective groups.

f. Report risk events.

3.4.10. Other Stakeholders

a. Imbibe a risk culture that emphasizes the careful analysis and control of risk as a vital part of the Bank's business.

b. Comply with the Bank's ERM Framework and associated policies, procedures and guidelines.

3.4.11. Risk Management Group – Relationship with Business/Support units

The relationship between the Risk Management Group and other business units are highlighted below:

a. The Group shall set risk limits for other Groups in the Bank.

b. The Group shall perform risk monitoring and reporting in the Bank.

c. Other group heads shall provide relevant data to the Risk Management Group for risk monitoring and reporting and identify potential risks in their Groups.

d. The Risk management Group shall provide the framework for monitoring and managing the risks identified

e. The Risk Management Group shall be involved in the design and development of new products and services.

f. The Group shall co-ordinate activities to provide a holistic view of risks across the Bank.

g. Information Technology shall provide relevant user support to the Group in respect of all risk management systems used in the Bank.

4. Risk Management Stakeholders

4.1. Introduction

Our risk management stakeholders are individuals or entities (internal and external) who can affect, be affected by or perceive themselves to be affected by our decisions or activities. They are individuals and entities who are involved or interested in the affairs of the Bank. In FMBN, we shall communicate and actively consult with our stakeholders to ensure the success of risk management in the Bank.

4.2. Stakeholder Identification

Stakeholder identification is an important element of our risk management process.
Risk management stakeholders identification will help the Bank:

a. Develop the relevant communication plan;

b. Ensure that the interest of the stakeholders are understood and considered;

c. Bring together different areas of expertise for identifying and analysing risk;

d. Ensure that risks are adequately identified;

e. Manage reputational risk;

f. Secure the endorsement and support for the risk treatment plan.

In evaluating potential stakeholders, the Bank will consider the following:

a. Capacity to contribute to the risk assessment process;

b. The effect a risk treatment plan would have on the perceived value of the stakeholder;

c. The effect an adverse risk occurrence would have on the perceived value a stakeholder places on the Bank.

It is important to state that stakeholders change over time and therefore the identification of stakeholders in the Bank's risk management process is an on-going one.

4.3. Determination of Stakeholders Expectations

In determining stakeholders' expectations, the following approaches shall be adopted:

a. One-on-one discussions;
b. Administration of questionnaires;
c. Literature review;
d. Combination of all methods.

4.4. Communication and Consultation Plan

Communication and consultation are an important consideration at each stage of the risk management process. We shall develop a communication plan for both internal and external stakeholders at the earliest stage of the process and this plan would address issues relating to both the risk itself and the process to manage it.

The communication plan shall contain the following:

a. Information: Stakeholders;

b. Communicators;

c. Responsibility for preparing communication;

d. Purpose/objective of communication;

e. Content/message;

f. Method of delivery;

g. Timing/date;

h. Frequency of communication.

The important components of our communication and consultation plan would include the following:

a. Awareness and understanding about a particular issue;
b. Information from stakeholders;
c. Information that would influence the target audience and achieve attitudinal or behavioural shift concerning a particular matter;
d. The context of risk, the risk criteria, the risk, or the effect of risk remediation from the stakeholders' perspective.

4.5. Participants in Communication Process

The purpose of the communication will determine which of the Bank's stakeholders will receive its communication or participate in the consultation. For instance, where the purpose of the communication is to learn from stakeholders, participation would be limited to stakeholders with expertise in the area of discussion. The Risk Management Group shall be responsible for identifying the participants in our communication process.

4.6. Means of Communication

Communication with our stakeholders would take any of the following forms:

a. annual financial reports;
b. memoranda;
c. intranet and internet;
d. e-mails;
e. bulletin;
f. board notices;
g. Press releases.

5. Risk Management Process

5.1. Introduction

The Bank's risk management process involves a set of tasks to support decision making by senior management within the Bank. This process entails the identification, evaluation, control and monitoring of risks.

We shall conduct a comprehensive risk evaluation and assessment of all material risks to which the Bank is exposed. The evaluation and assessment shall form the basis for determining our risk profile and updating the Risk Register. We shall conduct periodic reviews of this risk profile to ensure that it remains up to date, thereby allowing for the recognition and reporting of emerging risks. These activities shall be coordinated by the Risk Management Group to ensure risks are appropriately prioritised and managed across the Bank.

5.2. FMBN's Risk Management Process

The Bank's risk management process is depicted in the diagram below.

Figure 5.1: Risk Management Process

5.2.1. Operating environment

The Board sets the tone for risk taking and management across the Bank through the establishment of an appropriate risk appetite, ethical values, and internal structures for effective and efficient risk management in the Bank. In defining its operating environment, the Bank shall consider both internal and external factors. Internal factors include issues such as corporate governance, risk profile and internal controls. External factors could include the legislative framework for the Bank's operations, the political climate and domestic/global economic developments.

5.2.2. Strategic objective Setting

Strategic objectives, which are derived from the mandate of the Bank and management priorities, provide an appropriate context for the management of the Bank's risk in line with its risk appetite. The Board shall set financial, operational and other objectives which should be cascaded to business units and individual levels.

Activities designed to achieve the strategic objectives need to include adequate risk mitigants or controls to increase the likelihood of attaining set objectives.

5.2.3. Risk Identification

This activity seeks to identify the risks associated with business decisions made by the management of FMBN. It attempts to provide an answer to the question, 'what can happen and why'? The purpose of risk identification is to identify what might happen or existing situations that might affect the achievement of the Bank's objectives. The sources of risks may be internal or external. The external factors include liquidity issues, negative political trends (poor brand perception), natural disaster and inability of some PMBs to meet recapitalization targets.

Groups are primarily responsible for identifying and reporting the risks inherent in their activities as they pursue and implement the mandate and strategic objectives of the Bank.

The Risk Management Group shall set standards, deploy appropriate tools and coordinate risk identification to ensure that risk identification performed across the Bank is comprehensive and at the same level.

5.2.4. Risk Assessment

The risk assessment is aimed at analysing the risks to arrive at a level that describes FMBN's exposure. Quantitative and qualitative methods shall be adopted to conduct assessments of material risks. Groups in collaboration with the Risk Management Group shall determine the appropriate risk rating for existing and potential risk events, based on the impact and likelihood of occurrence.

In this regard, the levels of risk are ranked as high, medium or low.

5.2.4.1. Techniques for Assessing Risks

We shall adopt a combination of the following approaches to assess risks within the Bank:

a. **Desktop Based Assessment:** This approach would be used on a frequent basis (daily, weekly, monthly, etc.). It involves identifying key risk indicators (KRIs) for each risk and setting thresholds for these KRIs. The threshold would be defined for medium and high risk levels.

b. **Facilitated workshop**: A facilitated workshop at which staff knowledgeable in the processes and activities to be assessed, identify and evaluate the risks and controls associated with it. Risk and Control Self-Assessment (RCSA) workshop is a key component of risk identification and assessment in the Bank. RCSA for strategic objectives, groups and key cross functional activities shall be conducted at least once every 18 months to ensure the current risks associated with the relevant activities are identified and mitigated (See Appendix 2). RCSA shall be performed more frequently for activities and business units designated as high risk or when significant changes are made to or occur in the activity, group or related environment. Other risk assessment approaches such as Independent Risk Assessment may be used to update the risk profile and register in between the RCSA cycle.

c. **Interviews**: Structured interviews with key personnel to obtain their opinions on the risks categories being assessed. The outcomes of individual interviews are then aggregated to present a comprehensive view of the risk in question. This approach is desirable where it is difficult to get relevant personnel and other stakeholders into a workshop session. It is commonly used to obtain a top down view of the risk associated with the activities of a business unit, directorate etc.

d. **Questionnaires**: Structured questionnaires are developed and distributed to key personnel or focus groups to obtain a comprehensive view of the activity or group vis-a-vis its risk profile. This approach is desirable where the people required are in diverse locations and there is time constraint to concluding the exercise.

e. **Field observations**: A method of capturing risk events from the locations where they naturally occur by observing the process. Risk Management Group shall conduct independent assessments of key processes across the Bank to ensure that controls captured in the risk assessment operate as described. Field observations may be conducted to ascertain the nature, level of exposure, probability and magnitude of risk events emanating from external sources.

f. **Risk Modelling:** Quantitative risk assessment methodologies shall also be used as appropriate. Regardless of the approach adopted, the focus shall be geared towards assessing each risk, based on the following two components:

- Likelihood (probability) of occurrence; and
- Impact (consequence) of occurrence.

Before the risk assessment, the risk ranking criteria to be utilised shall be agreed. The Bank standard risk ranking shall be used except where it is impossible to do so

5.2.4.2 Risk Ranking

The Bank shall develop criteria for evaluating/agreeing the level of risks required to achieve its objectives. The risk levels are as follows:

HIGH	Risks that would significantly threaten the continued existence of the Bank as a going concern and significantly impede the Bank's ability to fulfil its mandate. This includes any event that is highly likely to occur with major impact on the Bank. Such risks would require Management's involvement in managing them.
MEDIUM	Risk that would result in the material loss of assets, risk that violates, harm, or impedes operations, or risk that may cause injury. This may include an event that could result in significant reputational damage or major financial loss that is highly likely to occur.
LOW	Risk that would result in the loss of some assets or may noticeably affect operations of the Bank. These risks are expected to happen in the normal course of business. The effect of such risks on the Bank's goals or objectives is usually minimal.

Table 5.1: Risk Ranking

The above three levels of the risks shall be determined by considering the following risk rating factors:

- The magnitude of the impact of the risks; and
- The probability that the risks might occur.

The following chart forms the basis for risk classification; it takes consideration of the probability and impact rating to arrive at a composite risk rating for each risk item. The risk matrix below can be used for both determining the level of inherent or residual risk.

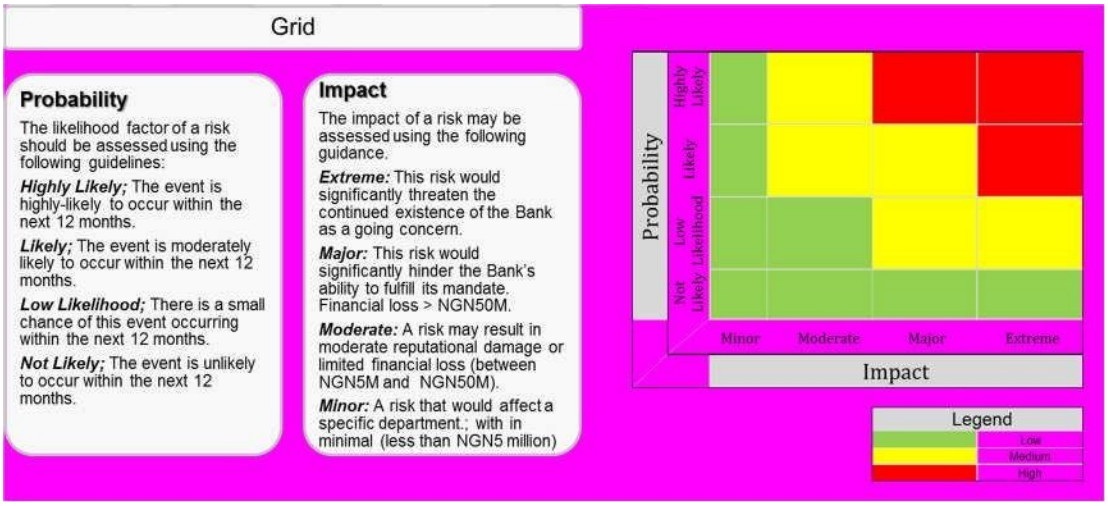


Figure 5.2: Probability/Impact matrix

5.2.4.3 Risk Rating Criteria

Magnitude of Impact of the Risk

The magnitude of impact of the risk is defined using a five-point scale with five (5) being the highest and one (1) the lowest as shown in table the below.

Table 5.2: Magnitude of impact

	Insignificant	Minor	Moderate	Major	Catastrophic
Scale	1	2	3	4	5
Implication	Could be written - off	Requires corrective action	Significant disruption – recovery Takes < X years	Severe disruption – recovery Takes > 1 year	Could lead to termination of business
Business	Less than NX million	Greater than NX million but less than NX million	Greater than NX million but less than NX million	Greater than NX million but less than NX million	Greater than NX million
Reputation	No impact on reputation	Potential impact on reputation	Reputation is impacted in the short term.	Serious diminution in reputation with adverse publicity	Sustained serious loss in reputation
Strategy					
Human Resources					
Customer/Client	No impact on customer satisfaction/retention	Minor negative impact on customer satisfaction/retention	Moderate negative impact on customer satisfaction/retention	Serious negative impact on customer satisfaction/ retention	Severe negative impact on customer satisfaction/retention resulting in negative referral
Regulatory Compliance	Verbal warning from regulatory authorities	Written warning from regulatory authorities but no penalty	Written warning from regulatory authorities	Penalty from regulatory authorities and partial suspension of production	Withdrawal of operating license to produce which threatens the Company's ability to continue as a going concern.
Fraud					
Health & Safety	Little or no injury	Moderate injury	Multiple injuries/some environmental damage	Single fatality/major environmental damage	Multiple fatalities/environmental disaster

Likelihood of Occurrence

Some events happen once in a lifetime; others can happen almost every day. The analysis of risk requires an assessment of their frequency of happening. The following table provides broad descriptions to support likelihood ratings.

Description	
The event is expected to occur in most circumstances, i.e. 80% or higher chance of occurring in the next 12 to 36 months.	Almost Certain
The event would probably occur in most circumstances, i.e. between 60% and 79% chance of occurring in the next 12 to 36 months.	Likely
The event might occur at some time, i.e. between 20% and 59% chance of occurring in the next 12 to 36 months.	Possible
The event might occur at some time, i.e. between 5% and 19% chance of occurring in the next 12 to 36 months.	Unlikely
Event may occur only in exceptional circumstances, i.e. lower than 5% chance of occurring in the next 12 to 36 months.	Rare

Table 5.3: Likelihood of occurrence

In order to estimate likelihood on a consistent basis, we will periodically determine a reasonable timeframe/period to use in assessing likelihood.

Level of Risk/ Risk Map

The level of risk is based on a combination of the magnitude of impact and the likelihood of occurrence of risks to form a matrix. The matrix formed (the Risk Map) from this combination provides a graphical illustration of the level of risk, that is, Low, Medium or High as shown in the figure below:

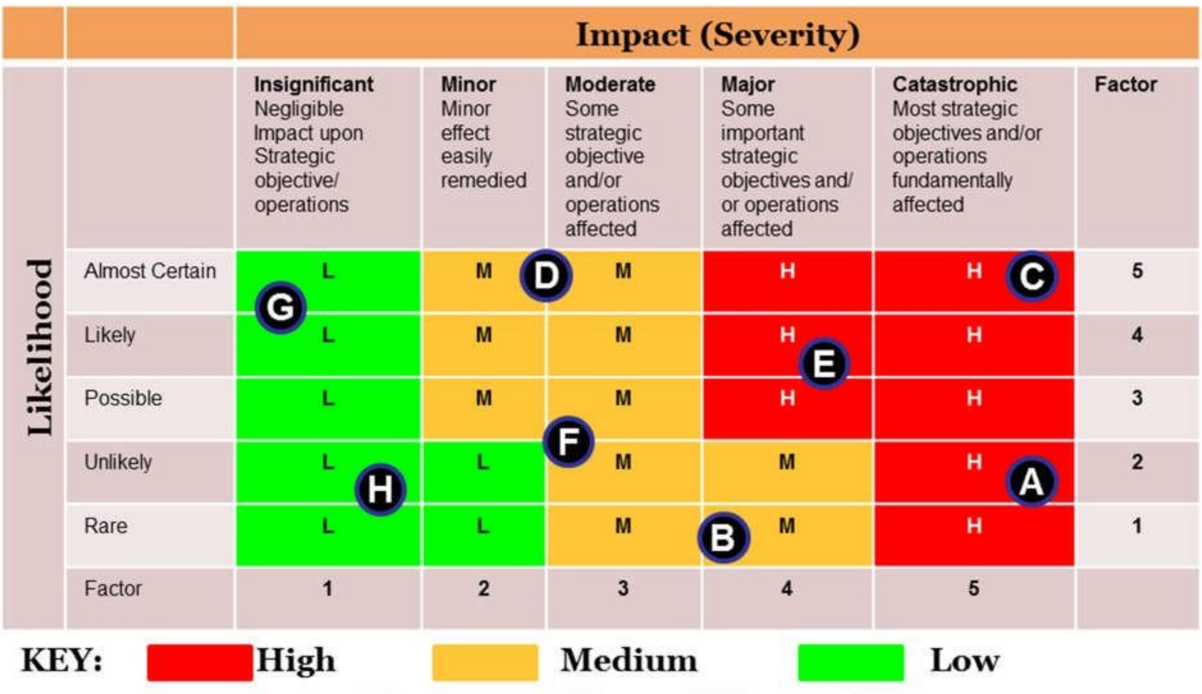


Figure 5.3: Risk Map

The High risks, (in the areas marked “H” on the risk map), require active management participation. The source of these risks must be identified, understood and actions formulated to treat or terminate the risk. Medium risks (in the areas marked “M”) also requires senior staff action to eliminate or minimise the risks. Low risks will usually require monitoring by lower level staff.

5.2.4.4 Risk Prioritization/Ranking

After identifying and assessing the risks, we shall proceed to prioritise the risks in order of significance as shown on the Risk Map. The risks outside FMBN’s risk appetite will be ranked as most significant. Conversely, risks on the bottom left hand corner of the risk map would be given the least priority, since they are within the Bank’s risk appetite.

For example, we shall rank the risks identified in the above risk map as follows (note that a description of the risks should be included in the ranking):

Ranking	Risk	Rating	Description
1	Risk C	High	
2	Risk E	High	
3	Risk A	High	
4	Risk D	Medium	
5	Risk F	Medium	
6	Risk B	Medium	
7	Risk G	Low	
8	Risk H	Low	

Table 5.4: Risk Raking Format

In order to determine the Residual Risk Level, we shall evaluate the effectiveness of the existing controls. Major risks that are not subject to effective controls may cause catastrophic consequences. To assess control practices, the following questions apply:

a. Are all appropriate controls present?

b. Does the control address the risk effectively?

c. Is the control officially documented and communicated?

d. Is the control in operation and applied consistently?

e. Is the control reviewed by anyone independent of the person performing the control procedure?

To help describe and attribute a control rating, the following indicative ratings are used:

Control Rating	Description
Poor	The Control is not documented, there is limited awareness of its existence, employees lack the skills to implement it, independent reviews are not performed, tools and resources for implementing the controls are unreliable and/or the report from the process is inadequate or unsatisfactory.
Fair	The Control is not documented, there is limited awareness of its existence, employees lack the skills to implement it, independent reviews are not performed, tools and resources for implementing the controls are unreliable and/or the report from the process is inadequate or unsatisfactory.
Good	The control is automated and documented, there is an awareness of its existence, employees have the skills to implement it, independent reviews are performed, the tools and resources for implementing the controls are reliable, and the report from the process is adequate. However, control is detective.
Excellent	The control is automated, documented and preventive. It effectively addresses the risk. There is an awareness of its existence, employees have the skills to implement it, independent reviews are performed, the tools and resources for implementing it are reliable, and the report from the process is adequate and satisfactory.

Table 5.5: Effectiveness Ratings for Existing Controls

The matrix below indicates how residual risk shall be determined from the relationship between the gross risk level (level of risks determined prior to control evaluation) and the control rating. The table shows that as controls improve, residual risk reduces.

Gross Risk Level	Control Rating			
	Poor	Fair	Good	Excellent
High	High	High	Medium	Medium
Medium	Medium	Medium	Low	Low
Low	Low	Low	Low	Low

5.2.5 Risk Response/Treatment

Groups shall adopt appropriate response strategies to mitigate risks evaluated as being higher than the Bank‘s appetite for such risks. The response options available to group are to avoid, reduce, transfer or accept the risk.

5.2.5.1. Risk Treatment Approaches

FMBN will apply any or a combination of the following four approaches to treat risks:

Risk Avoidance/Elimination

In this approach, we shall make decisions that isolate us from further contact with such risks. The decision could affect a new or existing strategy, PMB or product. Some instances of risk avoidance include opting out of, declining to transact with certain mortgage banks because of failure to meet certain criteria.

Risk Acceptance/Retention

Under this approach, we will acknowledge the risk, but we may not take measures to halt the likelihood of such situation occurring or to minimise the risk associated with it. We shall adopt this approach where the cost of mitigation exceeds the benefit or loss incurred should the risk occur.

Risk Reduction/Mitigation

Under this approach, we will acknowledge the risk and take steps to reduce the risk's likelihood and/or impact. Some of the steps that may be taken to mitigate the impact or likelihood of risk occurrence include the following:

a. Formulate or enhance policy.
b. Define authority limits.
c. Improve processes.
d. Strengthen/implement new controls.
e. Continuous education and training program.
f. Obtain expert advice.

Risk Transfer/Sharing

Under this approach, we shall attempt to transfer our risks to other sources. Some common practices involved in risk sharing include:

a. Purchasing various forms of insurance;
b. Hedging risk in the foreign exchange market; and
c. Out-sourcing risky functions to third parties.

The choice of the treatment option to use depends on the outcome of a cost benefit analysis. That is, we shall weigh the cost of implementing that option and the benefits derivable from using the option. FMBN shall consider all direct and indirect costs and measure all benefits whether tangible or intangible before reaching a decision.

5.2.5.2 Risk Treatment Plan

The purpose of the risk treatment plan is to document how the chosen risk treatment option will be implemented. The risk treatment plan identifies responsibilities, resource requirements, timing, proposed actions, expected outcome of treatments, performance measures, reporting and monitoring processes.

When risk treatment plans are implemented and plotted on the Risk Map, they should have the effect of moving risks towards the bottom left hand corner of the grid.

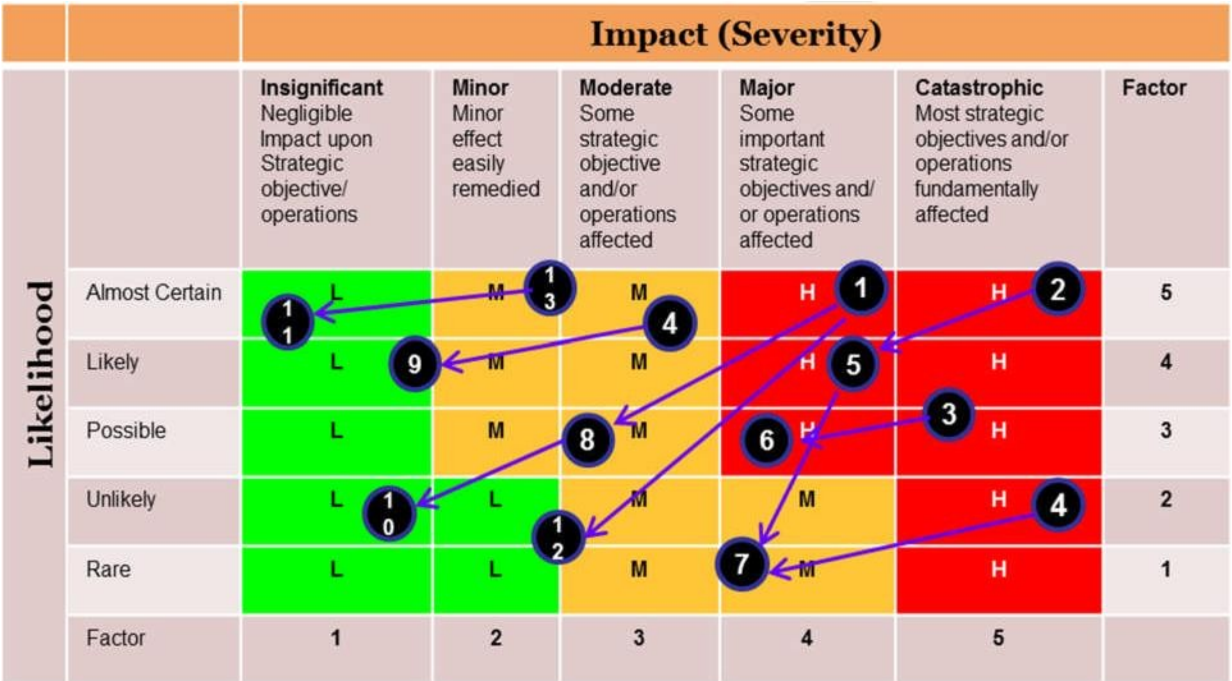


Figure 5.4: Risk Implementation plan plotted on a Risk Map

FMBN shall carry out a re-assessment of the new level of risk after the implementation of each risk treatment plan with a view to determining whether further treatment is required.

5.2.6 Control Activities

Policies and procedures shall be implemented bank-wide to ensure that risk responses are properly executed in accordance with the Bank's risk appetite. All Bank policies shall be approved by the Board and/or Management.

5.2.7 Information and Communication

Information that supports the implementation of the Framework shall be timely, relevant, accurate, and effectively communicated across the Bank.

5.2.8 Risk Monitoring and Review

Responsibility for the on-going monitoring of risks that are inherent in the Bank's various activities carried out across the Bank resides with the activity / process owners. Groups are therefore responsible for monitoring their risks albeit at exposure, portfolio or process. Data and reports are expected to be used to justify its risk positions and mitigation tactics. Groups shall communicate the current status of key risk indicators and any significant risk events to Risk Management Group as they occur for aggregation, remediation and reporting. The Risk Management Group shall draw from internal and external information sources to establish early warning indicators using approved Key Risk Indicators (KRIs).

FMBN shall monitor and review risks and controls on a regular basis to ensure that:

a. Assumptions made about risk, including the basis of the risk assessment remain valid.
b. Projected outcomes and expected results are being achieved.
c. Risk management plan remains relevant.
d. The outcomes of risk assessment are in tandem with actual experience.
e. Risk assessments techniques are being applied as desired.
f. The right mix of risk treatment is being used and that risk treatment used is effective.

Regular reviews of the risk management process shall be done to:

a. Evaluate the risk identification and assessment process;
b. Evaluate the effectiveness of implemented controls and the quality and appropriateness of all risk treatment action plans.

Internal/External Audit Reviews

Internal audit and external audit shall perform regular reviews of the risk management process to:

a. Evaluate the risk identification and assessment process;
b. Assess the effectiveness of implemented controls and the quality and appropriateness of all risk treatment action plans. This will form part of the updates into the risk treatment plan. Risk actions and any associated risk budget shall be reviewed every financial year and updated in the risk treatment plan.

5.3. Risk Reporting

A holistic and forward looking view of the Bank's risk profile relative to its appetite shall be provided to the Bank's Board and Management as appropriate. The reports shall contain a mix of quantitative and non-quantitative risk issues and shall be provided frequently.

In the event of a breach of risk appetite or risk limit, predefined escalation paths specific to the nature and scale of the breach will be followed.

Risk disclosures shall comply with relevant risk reporting standards such as the International Financial Reporting Standard.

The Risk Management Group shall co-ordinate the risk reporting process.

Risk management information may be summarised in many ways – for the Bank as a whole, by group, by business unit, by risk segment etc. The objective is to enable decision-makers to evaluate risk management performance monthly, weekly, daily or even in real time, as the nature of the risks and circumstances dictate.

5.4. Risk Register

The risk register is a comprehensive record of all risks affecting the business of FMBN. All the risks identified from the risk identification process will be documented in the risk register. The register is updated any time the Bank carries out a risk identification process. For the time being, our risk register will be documented using Microsoft Excel. At a minimum, it would contain the following information:

a. Description of the risk, its causes and its impacts;

b. Type of risk and the likelihood that it would occur; level of risk (risk rating);

c. Mitigating controls in place to manage the risk;

d. Mitigation options and risk accountability.

6. Embedding ERM within the Bank

6.1. Guiding Principles

The Bank is committed to embedding ERM best practices into its governance and business practices. The guiding principles for doing this are as follows:

a. The deployment of appropriate risk policies, standards, procedures, guidelines and tools to guide risk behaviour and serve as the bedrock for the Bank's risk management culture;

b. The Board and Executive Management shall take the lead in expressing the norms of the Bank's risk culture and demonstrating good practice;

c. The Board, Executive Management and Risk Management Group shall provide clear, consistent and appropriate risk communication;

d. Executive Management and Risk Management Group shall provide relevant and timely management information on enterprise and group risks and compliance that will drive the right risk behaviours and decision making;

e. Executive Management, Risk Management Group and Human Resource Group shall ensure appropriate risk awareness training is provided to educate and drive the appropriate risk culture across the Bank;

f. Executive Management and Human Resource Group shall ensure that the Bank's performance management and appraisal system: rewards appropriate risk behaviours; and sanctions inappropriate or risky behaviours;

g. Executive Management, Strategy and Performance management group, Risk Management Group and Financial Control Group shall ensure that risk considerations are incorporated into the strategy and budgeting process of the Bank.

In order to embed these principles within the Bank, the Bank shall consider the following key enablers:

S/N	KEY ENABLERS FOR PEOPLE DEVELOPMENT AND REWARD MANAGEMENT	
1.	People and communication	a. Appropriately developed job descriptions. b. Commitment to excellence by staff as outlined in the Bank's core values. c. Employee competence, training and development at all levels. d. Adequate communication, top-down, bottom-up and across processes/departments on the Bank's strategy, objectives and ERM policies, procedures and risk appetite. e. Full and timely disclosure of risk incidents. f. Sanctions for failure to report risk events. g. Deployment of independent incident blowing function. h. Incorporate risk management targets as part of balance score card for all staff.
2.	Performance Management	a. Competency frameworks aligned to strategy, objectives and business processes. b. Reward and recognition to incentivise behaviours that support effective and efficient enterprise risk management. c. Competitive salary and compensation structures to motivate staff and reduce the likelihood of fraud. d. Risk management considerations as a yardstick for evaluating staff performance. e. Sanctions for violating risk policies and operating outside the Bank's risk appetite, including termination in the event of repeated or grave violations. f. Adherence to limits. g. Implementation of an effective and fair performance management system, based on meritocracy. h. Timely resolution of internal and external audit exception.
3.	Management Succession Planning	a. Management succession planning to ensure the continuity of the Bank's operations during times of disruption. b. Support for outstanding managers who have the necessary ability, knowledge and experience for higher-level management responsibilities. c. Definition of detailed qualifications of persons to take up management positions and the required training programme

Table 6.1 – Key Enablers for Embedding Enterprise Risk Management within the Bank

7. Training in Risk Management

7.1. Introduction and Objectives

This section of the framework outlines the core risk management training that staff of the Bank shall be required to undergo to enable them understand the risk management philosophy, principles, culture, appetite, assessment methodologies, process and framework.

The objectives of the training plan are to:

a. Educate staff on FMBN’s risk management framework and process;

b. Educate staff on the fundamentals of risk management;

c. Provide an understanding of methods and tools for identification, analysis, planning, tracking, controlling, and communicating risks;

d. Provide staff with concepts, methods and techniques for successful ERM Promote a risk awareness culture.

7.2. Risk Management Awareness

It is important to communicate recent trends, changes and developments in the global and local economy as they relate to risk management. Thus, a risk awareness programme shall be established to ensure that members of staff are continually educated on recent developments and findings in risk management in the Financial Services industry. This will help to increase awareness of FMBN’s risk management policy and processes as well as enable staff to appreciate their roles and responsibilities better.

The awareness process shall be designed in a way that staff can readily learn with minimum disruptions to their duties. Options for this type of training include:

a. Induction manuals for new hires;

b. Short presentations during normal office meetings;

c. Short video clips;

d. Computer based training/e-learning programme;

e. Workshops and seminars;

f. Special briefings;

g. Newsletters.

7.3. Risk Training Plan

The Risk Management Group shall develop a comprehensive training plan on an annual basis. This plan shall form part of our annual training calendar. The training plan shall include courses that:

a. Provide our staff with specific training on our risk management framework covering all the key risks we manage;

b. Discuss trends and industry practices in ERM process;

c. Discuss the fundamentals of risk management and ERM concepts and approaches;

d. Assist participants to understand and implement risk management policies and procedures;

e. Provide an efficient methodology for evaluating risks in the business environment;

f. Assist participants to understand the use of information systems put in place to manage risks;

g. Give practical insights into the relationship between ERM and other organizational systems;

h. Provide understanding of important quantitative techniques used in risk management;

i. Provide understanding of how ERM can be used to gain a competitive advantage;

j. Provide an understanding of the Risk Management decision process.

Appendix A. - Job Responsibilities

A.1. Job Responsibilities for the Enterprise Risk Management Function

POSITION	Group Head, Risk Management
GRADE LEVEL	General Manager
REPORTS TO	BOARD
SUPERVISES	Risk Management Officers

The Head of Enterprise Risk Management Department reports functionally to the Managing Director/CEO on all enterprise risk issues. He has primary responsibility for coordinating the enterprise-wide risk management and compliance functions of the Company.

The Head, Enterprise Risk Management department has the responsibilities to:

- Assist in drafting Company's risk management strategy, risk appetite and tolerance statements and endorse to the Managing Director for review and approval.
- Manage the process for developing risk management and compliance policies and procedures and risk limits.
- Establish work standards for risk management and compliance staff and implement approved policies and procedures.
- Integrate the considerations of risk into strategic decision-making and ensure alignment between business strategies of line management and the Company's risk policy.
- Conduct a company-wide risk and compliance assessment on an on-going basis.
- Ensure that the Company's organisational structure and defined roles and responsibilities support the overall risk governance framework.
- Ensure that the Company has the required risk management skills to support the Company's business strategy.
- Prepare, monitor and evaluate the budget allocation and costs incurred by the department on an ongoing basis and develop short and long-term risk management strategic plans in alignment with the Company's goals.
- Evaluate the design and operating effectiveness of risk controls within the Company's products and processes, with a view to validating and/or effecting changes as may become necessary.
- Provide regular risk and control reports to the Board (through the relevant Board committees) on significant risk issues.
- Prepare periodic reports on compliance related matters, including progress against plan, findings from monitoring activities and recommendations, for the MD/CEO

- Establish and maintain a risk awareness culture in the Company and provide the appropriate opportunities for organisational learning, including lessons learnt from previous problems, ongoing communication, training and development.

- Ensure line management monitor compliance with laws, regulations and supervisory requirements as part of their normal operational duties.

- Ascertain skills gap of risk management personnel on an on-going basis, develop and update the annual training plan incorporating skills gap noted for all levels of risk management personnel and communicate to the Human Resources department for implementation.

- Prepare performance evaluations for all risk management personnel in accordance with the Company's performance appraisal system.

- Act as the point of contact between the Company and Regulators with reference to risk management and compliance issues and familiarize the shareholders, regulators and rating agencies with the Company's Enterprise Risk Management programme.

- Liaise with the external auditors and other assurance providers in the Company as required.

- Establish a risk and compliance culture that supports the overall objectives of risk management in the Company.