RISK MANAGEMENT MANUAL

RISK MANAGEMENT MANUAL

FIDELITY LIFE MUTUAL BENEFIT ASSOCIATION, INC.

Table of Contents

Chapter 1 4
OBJECTIVE 4
I. Objective 4
A. Risk Management Objectives: 4
Chapter 2 4
RISK MANAGEMENT SCOPE 4
I. Risk Management Roles and Responsibilities 5
A. Board of Trustees 5
B. Senior Management 5
C. Board of Trustees thru Risk Management Committee 5
1. Role 5
2. Authority 6
3. Composition 6
4. Frequency of Meetings 6
5. Duties and Responsibilities 6
D. Risk Management and Audit Officers (RMAOs) 7
1. Duties and Responsibilities 7
E. Authorized Risk-Takers (ARTs)/ Frontliners 8
1. Duties and Responsibilities 8
2. Specific Duties and Responsibilities 8
Chapter 3 10
RISK MANAGEMENT FRAMEWORK 10
RISK MANAGEMENT STRUCTURE 11
RISK MANAGEMENT FLOW CHART 12
Chapter 4 13
RISK ASSESSMENT, PLAN AND IMPLEMENTATION 13
I. RISK CATEGORIES 13
II. IDENTIFICATION OF RISK 13
A. Market Risk 13
B. Regulatory Risk 13
C. Operational Risk 13
D. Reputation Risk 15
E. Governance 16
F. Planning and Resource Allocation 16
G. Major Initiatives 16
H. Accounting and Reporting 17
III. IMPLEMENTING RISK POLICIES 17

A. Procedures 17
B. Controls for Higher Risk Situations 17
C. Measures 18
D. Record Keeping Management and Requirements 18
E. Methodologies and Monitoring 18
F. Ongoing Monitoring 19
G. Risk Monitoring 19
H. Reporting 19
I. Suspicious Transaction Report (STR) Framework and Confidentiality of Reporting 20
J. Training and Awareness 20
K. Compliance to Regulatory Requirements and Authorities to check compliance 20
L. Enforcement Action 21
ANNEX A 22
RISK CONTROL SELF-ASSESSMENT 22

FIDELITY LIFE MUTUAL BENEFIT ASSOCIATION, INC.
RISK MANAGEMENT MANUAL

Chapter 1

OBJECTIVE

I. Objective

The objective of this Manual is to serve as a basis and reference for consistent risk management that is applicable to all employees of the **Fidelity Life Mutual Benefit Association, Inc. (FLMBAI)**. It aims to create a culture of risk-awareness, not risk-aversion based on the prudential framework required by the Insurance Commission (IC) and the Anti Money Laundering Council System (AMLC), and to provide guidance on Risk-Based Approach to combating Money Laundering and Terrorist Financing (MLTF). It provides a general set of risk principles delegated to each department through its reporting and approval procedures.

- Support the development of a common understanding of what the risk based and management approach involves;
- Outline the high-level principles involved in applying the risk-based and management approach;
- Identify characteristics of risks indicating that enhanced mitigation strategies may be warranted;
- Describe good practices in the design and implementation of an effective risk-based and management approach; and
- Foster communications that are conducive to the prevention of any form of risks.

It should be noted that applying a management and risk-based approach is neither mandatory nor prescriptive. A properly applied management and risk-based approach does not necessarily mean a reduced burden, although it should result in a more cost effective use of resources.

A. Risk Management Objectives:

1. Identify, measure and control risks inherent in all activities
2. Disseminate Compliance and Risk Management philosophy and policies
3. Assist risk-taking business units in understanding, measuring compliance and risk.
4. Develop control infrastructure, compliance and risk management.

Chapter 2

RISK MANAGEMENT SCOPE

The **Risk Management Committee (RiskCom)** is formed by the Board of Trustees (BOT) to assist in the fulfillment of the BOT's risk management responsibilities as defined by applicable laws and regulations. The **RiskCom** shall have direct access to, and receive regular reports from the Management. It shall have the power to conduct or authorize inquiry into any matter within the scope of the committee's responsibilities.

The **RiskCom** shall monitor the risk environment and provide direction for the activities to mitigate to an acceptable level the risks that may adversely affect the Company's ability to achieve its goals.

I. Risk Management Roles and Responsibilities

A. Board of Trustees

The **BOT** is ultimately responsible for ensuring compliance with this Guidelines, the respective implementing rules and regulations, and other directives, guidance and issuances from the lC and AMLC.

B. Senior Management

Oversee the day-to-day management to ensure effective implementation of all risk management policies approved by the Board and alignment of activities with the strategic objectives, risk profile and corporate values set by the Board.

Establish a management structure that promotes accountability and transparency and upholds checks and balances.

C. Board of Trustees thru Risk Management Committee

1. Role

The **RiskCom**, together with the **Audit Committee,** shall be primarily responsible for the development and oversight of the risk management programs which include the following:

a. Oversight of management functions and approval of proposals regarding policies, procedures and best practices relative to asset and liability management, credit, market and business operations risks ensuring that:

- All risks are passed or forwarded for assessment.
- Risk controls and management guidelines are strictly observed.
- Immediate corrective actions are taken whenever guidelines are breached or whenever necessary.

b. Be responsible for ensuring compliance to written policies and procedures relating to the management of risks throughout. This shall include:

- Comprehensive risk management approach;

- Detailed structure of limits, guidelines and other parameters used to govern risk-taking units;
- Clear delineation of lines of responsibilities for managing risk;
- Adequate system for measuring risk; and
- Effective internal controls and a comprehensive risk reporting process.

2. Authority

The **RiskCom** shall exercise authority over matters within the scope of its functions and responsibilities as approved by the BOT.

3. Composition

The **RiskCom** shall be composed of at least three (3) members of the Board of Trustees who shall possess a range of expertise as well as adequate knowledge of the FLMBAI risks exposure to be able to develop appropriate strategies for preventing losses and minimizing the impact of losses when they occur.

4. Frequency of Meetings

The **RiskCom** shall hold regular meetings at least quarterly, or as often as it considers necessary and appropriate. A member or the majority of its members may call a special meeting when deemed necessary. A majority of the members will constitute a quorum.

The **RiskCom** shall report to the Board of Trustees matters discussed at each meeting along with the actions taken during said meeting.

5. Duties and Responsibilities

a. Core Duties and Responsibilities

RiskCom shall perform the following core duties and responsibilities but not limited to:

i. Notation of the risk reports as presented by the Authorized Risk Takers (ARTs). The **RiskCom** shall assess the probability of each risk becoming reality and shall estimate its possible effect and cost with priority on those risks that are most likely to occur and are costly when they happen.

ii. Approval of the Risk Management Strategies and Plan. - Risk Improvement Plan (RIP).

b. Specific Duties and Responsibilities

The **RiskCom** shall perform the following specific duties and responsibilities:

i. Promote a risk culture that requires and encourages the highest standards of ethical behavior by risk management overseers and authorized risk takers.

ii. Meet with and request the submission of and evaluate information from the Management and other departments; and perform/approve the necessary actions/proposals as it deems appropriate, regarding the scope of its work, significant findings, together with the actions and responses of management.
iii. Oversee the management of future risks rather than risk in past transactions.
iv. Recognize those risks and institute contingency plans to mitigate said risks.
v. Provide regular periodic reports to the Board of Trustees pertaining to overall risk exposure and actions taken to reduce the risks.
vi. Encourage the professional development and training of all engaged in both risk oversight and risk-taking activities.
vii. Oversee the adequacy of this Manual on an annual basis and recommend any proposed changes to the Board of Trustees for approval.

D. Risk Management and Audit Officers (RMAOs)

Risk Management and Audit Officers **(RMAOs)** are personnel which report administratively and functionally to **RiskCom.** The **RMAO** who shall be the Risk Focal Persons are composed of:

- Compliance Officer
- Alternate Compliance Officer
- Risk and Audit Officer
- and Committee members

1. Duties and Responsibilities

The RMAO shall perform the following core duties and responsibilities:

a. Consolidate **RiskCom** reports submitted by the Authorized Risk Takers (**ARTs**). The RMAO shall:

i. Perform **RiskCom** Secretariat function
ii. Collaborate with the (Authorized Risk Takers) ARTs for the preparation of **RiskCom** report
iii. Consolidate report for **RiskCom,** including
iv. Risk Improvement Plan (RIP)
v. Internal Audit

b. Develop Risk Management Strategies and Plan. The RMAO shall:

i. Develop a written plan defining the strategies and plan for managing and controlling the major risks.
ii. Identify practical strategies to reduce the chance of harm and failure or minimize losses if the risks become real.
iii. Communicate the risk management plan and loss control procedures to affected parties.
iv. Conduct regular discussions on current risk exposure based on regular management reports and direct concerned units or offices on how to reduce these risks.

c. Review and revise the Compliance and Risk Management Plan, as needed. The RMAO shall:

i. Review and evaluate the steps that management has taken to monitor and control risk exposures to ensure its continued relevance, comprehensiveness and effectiveness.
ii. Revisit strategies, look for emerging or changing exposures and stay abreast of developments that might affect the likelihood of harm or loss.
iii. Report regularly to the Board of Trustees the **FLMBAI**'s overall risk exposure, actions taken to reduce the risks, and recommend further action or plans as necessary.

d. In case of an **Outsource Internal Audit** is needed the **RMAOs** shall be in charge of assigning officer to oversee the audit activity and be responsible for managing the outsourced internal audit according to set guidelines and protocols as approved by the BOT.

Outsource Internal Audit shall perform the core duties and responsibilities, including but are not limited to investigating internal and external management risk, evaluating exposure, fraud, performing **audits** on operations, and reporting on findings, and providing recommendations and other tasks as assigned and guided by Company's **RMAOs or senior officers.**

E. Authorized Risk-Takers (ARTs)/ Frontliners

Authorized Risk-Takers (ARTs) refers to all FLMBAI personnel who have been given authority to commit to insurance and inherently expose FLMBAI to market risks. ARTs, which operate within designated units and specified limits are FLMBAI **``front-line"** in risk exposure management (such as Agents, Customer service, Accounting and the others). They are responsible for identifying opportunities for return, taking commensurate risk positions and actively monitoring, evaluating and adjusting those positions.

1. Duties and Responsibilities

In view of considerable discretion inherent in their activities, ARTs have the responsibility to:

- Identify and evaluate exposures.
- Identify and document types of risks.
- Identify and assess the external risks that may affect the business plans and directions.
- Assess the probability of each risk becoming reality and shall estimate its possible effect and cost with priority on those risks that are most likely to occur and are costly when they happen.
- Conduct risk-taking activities within limits at all times.
- Understand risk profile of managed position/portfolio and to scan and determine market opportunities within context of overall LIBI strategy and risk tolerance.
- Submit quarterly (or as needed) risk reports to the **RiskCom** for notation.

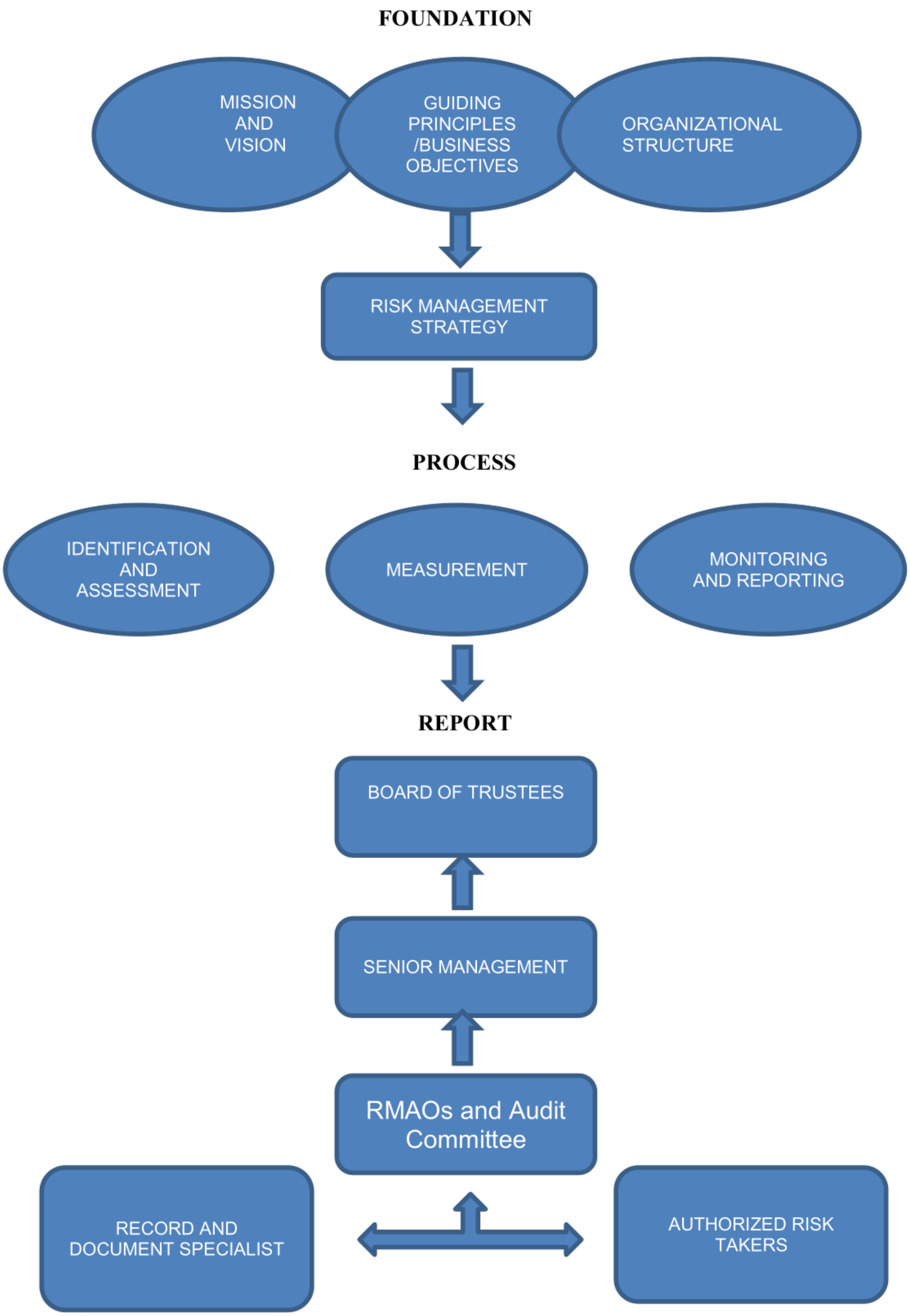
2. Specific Duties and Responsibilities

a. Meet with, request/gather (or compel submission, in proper cases), receive and evaluate information from management and appropriate sources and act or approve proposals, accordingly, on the following items relating to Market and Business Operational Risks.
b. Receive and evaluate information from management and appropriate sources and act or approve proposals, accordingly, on the following:

- Policies and procedures on market and operational risks (e.g., technology, legal, reputation and personal risks;
- Market risk resulting from FLMBAI’s insurance transactions;
- Policies and procedures on operational risk matters e.g. technology, legal, reputation and personnel risks;
- Management reports relating to operational issues and risk;
- Awareness on proper risk culture and how risks should be addresses
- Information relating to compliance with both external and internal regulations regarding market and operational risks.

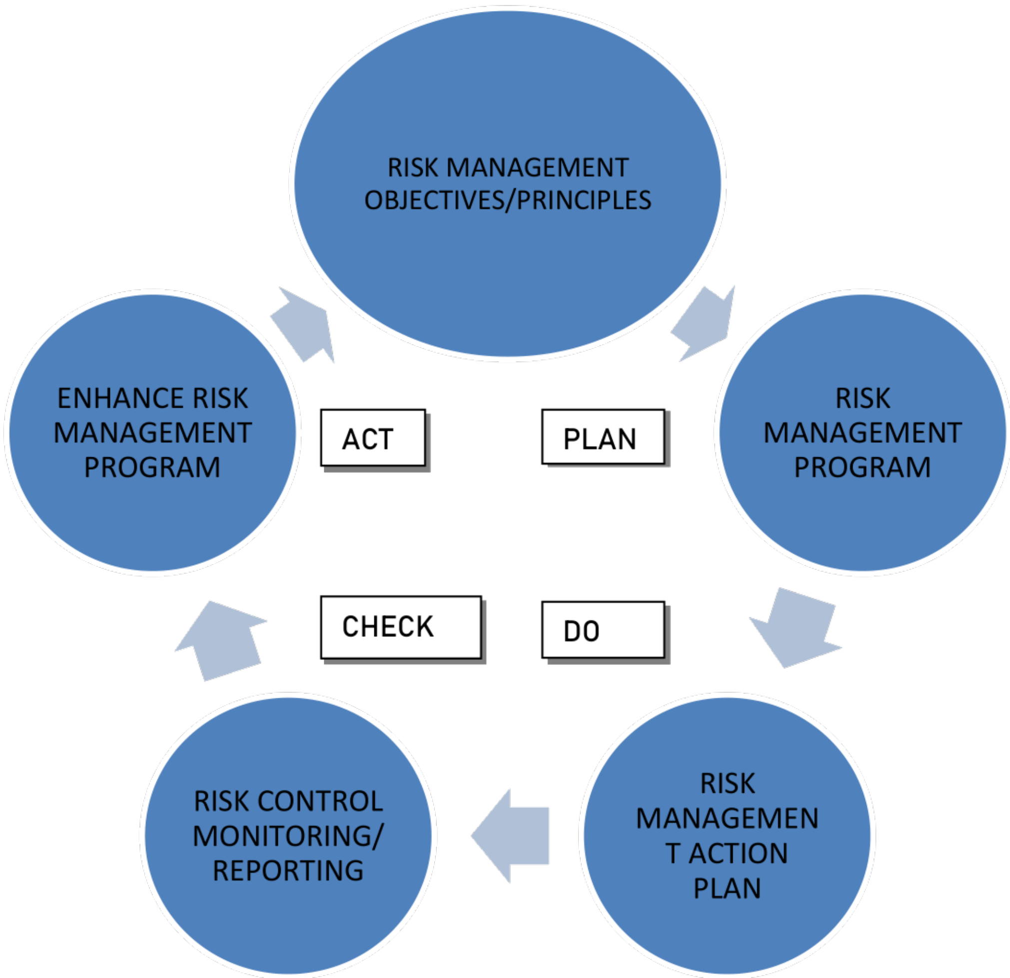
Chapter 3

RISK MANAGEMENT FRAMEWORK



RISK MANAGEMENT STRUCTURE

RISK MANAGEMENT FLOW CHART



Chapter 4

RISK ASSESSMENT, PLAN AND IMPLEMENTATION

I. RISK CATEGORIES

In order to implement a reasonable risk-based approach, FLMBAI identifies appropriate criteria for categorizing risks and assessing risks in each category. Identification of all management risks posed together with an assessment of the level of the risk. This will allow determining and implementing appropriate policies, procedures and controls to mitigate these risks. While a risk assessment should always be undertaken at the inception of a customer relationship, for some customers, a comprehensive risk profile may only become evident over time. As such, it may also have to adjust its view based upon information received from a competent authority.

While there is no universal set of risk categories, there is no one single methodology to apply to assessing the risks and the application of these risk categories is intended to provide a broad strategy for managing all kinds of potential risks.

II. IDENTIFICATION OF RISK

A. Market Risk

It is defined as the risk to earnings or capital arising from changes in the value of traded portfolios of financial instruments. Market risk can be generally defined as risk of loss, immediate or over time, due to adverse fluctuations in price or market value of instruments, products and transactions in FLMBAI's overall portfolio. Market risks are the central focus of risk measurement methodologies and limits, as well as a gauge by which LIBI can determine returns it will require for its activities.

B. Regulatory Risk

It refers to financial loss arising from changes in legal, monetary, tax or other governmental regulations of a country. This risk is interrelated with legal risk and should be covered by legal and tax review.

It is defined as the failure to comply with circulars, memoranda, advisories and other issuances of regulatory bodies as applicable to the insurance industry, may result in loss of business, administrative/criminal penalties/sanctions, and loss to reputation.

C. Operational Risk

It is defined as the current and prospective risk to earnings or capital arising from fraud, error, inadequacy of internal controls and the inability to deliver products or services, maintain a competitive position, and manage information. Risk is inherent in efforts to gain strategic advantage, and in the failure to keep pace with changes in the financial services marketplace. Operational risk is evident in each product and service offered. Operational risk encompasses: product development and delivery, operational processing, systems development, computing systems, complexity of products and services, and the internal environment.

1. Legal Risk – risk of financial loss due to incomplete, incorrect and unenforceable documentation used by FLMBAI to protect and enforce its rights under contracts and

obligations. A legal review shall verify capacity and authority of counterparties and customers to enter into transactions.

Failure to assess the favorableness of the contracts the Company enters into and the failure to comply with and monitor contract terms might lead to financial losses.

FLMBAI uses a Risk Control Self-Assessment (RSCA) as Risk Management tool as shown in Annex A.

2. Communications and Investor Relations

   - Employee Communication
     Failure to understand and respond to the communication needs of different employees may cause discontent in the workforce resulting in operational difficulty.

3. Delivery

   - Product Delivery & Support
     Failure to deliver and support products and services to meet customer expectations might lead to lost business or affect the Company's reputation.

4. People Risk – refers to potential loss due to inadequate training, inexperience or illegal activities of risk-taking personnel. It is likewise interrelated to internal control aspects of operation risk. It highlights the human side of risk-taking, role and adequacy of institutional trading guidelines, codes of conduct, personnel policies and training and development programs in overall Risk Management.

   - Culture
     Inability to create and instill the accepted norms of behavior may inhibit the achievement of desired performance and the accomplishment of corporate goals

   - Recruiting & Retention
     Inability to attract and retain competent employees might lead to organizational dysfunction and low morale.

   - People Development & Performance
     Inability to develop and enhance employee skills and provide a sound employee performance management system may reduce employee motivation and may adversely impact the achievement of desired Performance and conduct.

   - Succession Planning
     Failure to create and implement a feasible continuance plan for key positions and employees might adversely affect the stability of organizational leadership and business continuity.

5. Information Technology

   - IT Management
     Failure to effectively prioritize IT initiatives and administer IT resources may lead to

lost business and hinder the achievement of the goals and objectives.

- <u>IT Confidentiality</u>
  Failure of information systems to adequately protect both IT data and IT infrastructure may lead to or allow unauthorized access, or lead to destruction of information and information systems.

- <u>IT Availability/Continuity</u>
  Failure to ensure uninterrupted operations and immediate recovery from systems and implementation failures may lead to lost business and losses.

- <u>IT Integrity</u>
  Failure of an information system to provide accurate, reliable and timely financial and non-financial information when needed may lead to operational inefficiencies or lost business opportunities.

6. Business Interruption

- <u>Business Continuity Planning</u>
  Failure to undertake the appropriate advanced planning related to critical business functions/processes may result in the inability to recover and maintain business operations in the event of a disruption due to natural events or terror and malicious acts.

D. Reputation Risk

It refers to the current and prospective impact on earnings or capital arising from negative public opinion. This affects the FLMBAI's ability to establish new relationships or services or continue servicing existing relationships. This risk may expose FLMBAI to litigation, financial loss, or a decline in its customer base. Reputation risk exposure is present throughout the organization and requires the responsibility to exercise an abundance of caution in dealing with customers and the community.

E. Governance

1. Board Performance

   Inability of the Board of Trustees to discharge their obligations and duties owed to the Company and its stakeholders in good faith may hinder effective strategy-setting and decision-making.

2. Tone at the Top

   Inability of the Board of Trustees and Senior Management to establish a culture of accountability, integrity, professionalism and competency may result in an unfavorable working environment and lack of integrity in the way the business is conducted.

F. Planning and Resource Allocation

1. Organizational Structure

   Lack of a responsive organizational structure may prevent the achievement of the strategic goals and objectives in an efficient manner.

2. Strategic Planning

   Failure to develop, implement and monitor institutional strategies and direction may threaten the overall viability and growth prospects.

3. Forecasting

   Inability to foresee macroeconomic and market trends, opportunities and threats will threaten the competitiveness in the long run and may result in inappropriate business strategies and missed business opportunities.

G. Major Initiatives

1. Vision & Direction

   Failure to establish, align and communicate a vision and direction for the institution and its major initiatives, including services, products and programs, may hamper the achievement of the objectives and strategies.

2. Planning & Execution

   Failure to plan and execute programs and initiatives effectively may lead to operational inefficiencies, financial losses and project failure.

3. Measuring & Monitoring of Major Initiatives

   Failure to identify appropriate performance metrics and standards to monitor attainment of objectives and targets may prevent the achievement of desired output and performance.

4. Technology Implementation

Failure to adopt and implement the appropriate system and technology to support business processes or major initiatives may lead to costly investments and work inefficiencies, and may compromise product or service delivery.

H. Accounting and Reporting

1. Accounting, Reporting and Disclosure

   Inaccurate recording and reporting of material financial transactions in accordance with existing standards may result in regulatory sanctions for the Bank, and may also lead to misinformed business decisions by Management and other stakeholders.

2. Internal Control

   Failure to establish and maintain adequate internal controls that align with stakeholder and regulatory expectations may result in errors or omissions in financial reporting, control breakdowns or fraud.

III. IMPLEMENTING RISK POLICIES

A. Procedures

1. Authorized Risk Takers (ARTs) and others which perform the transactional level involves specific day-to-day risk-taking activities.
2. ARTs start with the day-to-day Risk Management Process by determining opportunities. Once opportunities are determined, ARTs identify types of risks associated.
3. ARTs quantify and evaluate identified risk limits delegated to them or its potential effect on a position. It also includes assessment of existing system capability to support risk-taking activities.
4. To measure and effectively manage impact of risk, specific tools and techniques, ARTs use Proper tools and techniques as well as strict compliance in policies and procedures are requisites of a coherent risk management system.
5. The culmination of transactional level is when an ARTs take a position. This act would further entail active monitoring, evaluating and if necessary, adjusting position to attain Risk Management twin objectives of pursuing best possible return and managing associated risk.

B. Controls for Higher Risk Situations

Implement appropriate policies, procedures and controls to mitigate the potential money laundering and terrorist financing risks of those customers, products and countries that they determine pose a higher risk. Risk mitigation measures and controls include:

- Identify and monitor higher risk customers and transactions within business lines across the company.

- Increased levels of due diligence and preventive guidelines. The measures should be directed toward strengthening the knowledge of all these measures.

- Increased levels of ongoing controls and frequency of reviews of relationships.

The same measures and controls may often address more than one of the risk criteria identified, and it is not necessarily expected that an insurance company establishes separate controls, providing that identified heightened risks are addressed.

C. Measures

Whenever measures are applied as required by guidelines or by the customer, the concerned staff, officers and the BOT acceptance policies or where the risks are higher the Company should perform applicable measures.

D. Record Keeping Management and Requirements

Complemented by the requirements under the Guidelines on Customer Records, the Company must retain all transaction records in accordance with prevailing tax and other regulations.

Ensure that all information and transaction records are available swiftly to whenever required by the Insurance Commission, AMLC and other local competent authorities in the exercise of their official functions or upon order by a competent authority.

Take measures to ensure that customer records are submitted in the manner, quality and period as would assist the AMLC and its prompt investigations and institution of legal actions, for this purpose. Should implement the guidelines, on records as issued by the IC and AMLC.

E. Methodologies and Monitoring

Since the degree and nature of monitoring depends on the size of the company; FLMBAI applies a method which includes a manual, automated or combination in monitoring the type of activity under scrutiny. In applying a risk-based approach to monitoring, ARTs must recognize that not all transactions, accounts/policies/contracts, or customers will be monitored in the same way. In highly automated operations, appropriate risk-based practices may start with filtering out those risks which need particular monitoring from the large number which are processed by highly-automated methods. The purpose of the process should be to identify whose activities appear to be unusual and which require further analysis to determine if there are grounds for further concern. The degree of monitoring will be based on the perceived risks associated with the customer, the products or services being used by the customer and the location of the customer and the transactions. These monitoring methodologies may change over time based on specific experience or after general experience by the Company as a whole. Monitoring methodologies and processes also need to take into account the overall volume of higher risk situations, resources of the FLMBAI and the information available for use by the Company.

The principal aim of monitoring in a risk-based system is to respond to enterprise-wide issues based on Company analysis of its major risks. Hence, we trust the regulatory authorities will be mindful of and give due weight to the determinations made, provided that these determinations are consistent with legislative or regulatory requirements, and are reasonable and adequately documented.

Subject to applicable legislation, the monitoring under a risk-based approach should allow the creation of monetary or other thresholds to identify transactions based on size or type which will be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a periodic basis to determine adequacy for the risk levels established. Changes to systems and processes should be based on the analysis of the effectiveness and efficiency of prior results, new information that would warrant such changes, and the ability of the Company to effect such a change. The results of the monitoring should always be documented.

F. Ongoing Monitoring

Considering the risk categories, the Company should establish a system that allows the conduct of ongoing monitoring that will enable the management and stakeholders to understand the norms, the account or business.

G. Risk Monitoring

Risk Monitoring is the process of tracking and evaluating the performance and status of **RiskCom** activities. Risk monitoring should be done to determine the following:

- **RiskCom's** strategies or responses crafted have been implemented as planned;
- If the risk action plans are effective in addressing the risks or if new responses should be developed
- If the risk exposure has changed from its prior state and whether risk priorities should be updated
- If new risks have occurred that were not previously identified or residual risks are still existing and require new responses
- If the business assumptions are still valid and if there is a need to revisit and revise the RMPS

The Company shall utilize the **RiskCom Action Plan Monitoring template** as shown below for an effective monitoring of the actual accomplishments of a particular responsible unit.

Risk Driver	Action Plan	Responsibility	Time Frame	Key Results Are	Accomplishments
Identified critical risk driver	Specific action steps to implement the RiskCom Strategies	Primary unit responsible for the action plan, showing designation of the Unit Head	Specific dae or deadline to implement the RiskCom Action Plan	Expected Output from the RiskCom Action Plan	Actual Output of responsible with the implementation of the RiskCom Action Plan

The **RiskCom** consolidate the risk reports and present it to the Senior Management and the Board of Trustees for approval.

H. Reporting

Following the reporting guidelines of AMLC and the Insurance Commission, the Company shall ensure the accuracy, completeness and timeliness of transaction reports, which shall be filed in such form as prescribed and shall be submitted in a secured manner.

I. Suspicious Transaction Report (STR) Framework and Confidentiality of Reporting

Relevant policies, procedures, processes and controls are in place in the FLMBAI s' Code of Conduct and Business Ethic that would enable an employee to report to the Compliance officer any suspicion or knowledge of all risk and/or transaction that is detected or identified;

When reporting Confidential Transactions and Suspicious Transactions to the AMLC, covered persons, their trustees, officers and employees, are prohibited from communicating, directly or indirectly, in any manner or by any means, to any person or entity, or the media, the fact that a covered or suspicious transaction report was made, the contents thereof, or any other information in relation thereto. Any information about such reporting shall not be published or aired, in any manner or form, by the mass media, or through electronic mail, or other similar devices. In case of violation thereof, the concerned trustee, officer and employee of the covered person shall be criminally liable.

J. Training and Awareness

The Company shall develop programs to address all kinds of risks. These programs should include attendance to training and seminars being conducted by IC and other regulatory institutions; and risk management training to employees. FLMBAI is committed to having strong and adequate controls which relies on both training and awareness. This requires a company-wide effort to provide all relevant employees with a minimum level of general information on Insurance laws, IC regulations and internal policies and procedures.

Continuing training may take place at a time and in a manner deemed appropriate in keeping with the Company's overall risk mitigation strategy, and the methodologies may evolve based on specific training experiences of the participants or the general experiences of the Company as a whole.

Applying a risk-based approach to the various methods available for training, allows the Company additional flexibility regarding the frequency, delivery mechanisms and focus of such training. The Company shall review its workforce and agents and available resources and implement the training programs that provide appropriate risk information that is:

- Tailored to the appropriate staff responsibility (*e.g.*, customer contact or operations).
- At the appropriate level of detail (*e.g.*, front-line personnel, complicated products or customer- managed products).
- At a frequency related to the risk level of the business line involved.

Risk training should take into account those internal risks and procedures which require that high risk situations are forwarded to and handled within the organization.

K. Compliance to Regulatory Requirements and Authorities to check compliance

The Insurance Commission has the authority to conduct checks to validate the compliance of the Company with the requirements of the regulatory commission, applicable laws and their respective implementing rules and regulations.

In compliance thereof, the Company shall upon order of the Commission and based on a letter of authority shall immediately make available, give full access and submit to the compliance checker any and all information and documents, including customer identification, account opening and transaction documents, as they may require and allow them to interview the concerned officers and staff during compliance checking.

L. Enforcement Action

ln line with the objective of ensuring that high standards is maintained and in order to protect its safety and soundness of the Company, violation of the Guidelines under this Manual shall constitute a major violation which may be subject to the following sanctions:

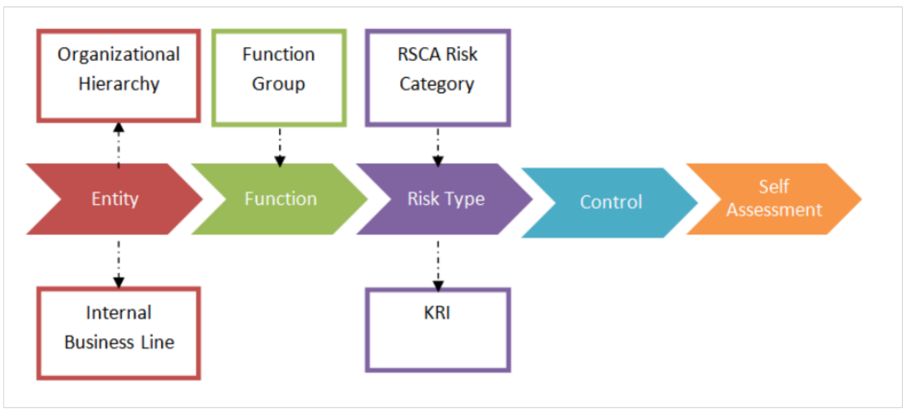
a. Written reprimand;
b. Suspension or removal from the position they are currently holding; or
c. Disqualification from holding any position in the Company.

ANNEX A

RISK CONTROL SELF-ASSESSMENT

Risk Control Self-Assessment (RCSA) is an empowering method/process by which management and staff of all levels collectively identify and evaluate risks and associated controls. It adds value by increasing an operating unit's involvement in designing and maintaining control and risk systems, identifying risk exposures and determining corrective action. The aim of RCSA is to integrate risk management practices and culture into the way staff undertake their jobs, and business units achieve their objectives. It provides a framework and tools for management and employees to:

- Identify and prioritize their business objectives
- Assess and manage high risk areas of business processes
- Self-evaluate the adequacy of controls
- Develop risk treatment action plans
- Ensure that the identification, recognition and evaluation of business objectives and risks are consistent across all levels of the organization



Business units or functions that will be included in the process are those for which a set of objectives or results can be defined. This is important because there must be a common understanding and acceptance of what the group needs to achieve, against which risks and controls can be assessed and evaluated. The workflow is as follows:

RCSA Workflow

RISK MANAGEMENT MANUAL

Prepared By:

Erh Roman H. Enriquez
Quality Assurance Manageger
Alternative Compliance Officer

Reviewed By:

Atty. Rizal Antonio Meru
Compliance Officer

Mr. Rey Vergára
Consultant

Approved By:

Dr. Jose Enrique R. Delas Peñas
President