KASAGANA KA MUTUAL BENEFIT ASSOCIATION, INC.

RISK MANAGEMENT MANUAL

I. INTRODUCTION

KASAGANA-KA Mutual Benefit Association, Inc. (KASAGANA-KA MBA or KMBA) is a non-stock not-for-profit organization owned and managed by its members. It provides affordable insurance products and services to urban poor women and their families. Organized in 2006, KMBA is a sister organization of the KASAGANA-KA Development Center, Inc. (KDCI), whose client-beneficiaries and staff constitute KMBA's primary members. KMBA also offers associate membership status to client beneficiaries of its partner microfinance organizations and other organized sectors. As of December 2016, KMBA have more than 44,000 members, composed of the KDCI's client-beneficiaries and over 10,000 associate members.

KMBA traces its creation to KDCI, for which it provides various products and services for the latter's micro insurance program. KMBA's initial fund was sourced from a grant from KDCI, which likewise has since been contributing its community presence and center collection infrastructures to KMBA's field operations. The KDCI grant also enabled KMBA to offer to children of its primary and associate members the Kuya Jun Scholarship Program (named after Severiano C. Marcelo, Jr., first KDCI executive director, who passed away in 2008).

KMBA was registered with the Securities and Exchange Commission (SEC) in June 2006, and was given a license to operate as a mutual benefit association by the Insurance Commission (IC) in April 2007. It is a non-stock non-profit organization owned and managed by its members. It is a member of the Micro-insurance MBA Association of the

Philippines (MIMAP) also known as RIMANSI organization for Asia and the Pacific, Inc., a "resource center that develops and offers risk management solutions to member-owned micro-insurers, especially Mutual Benefit Associations." As a member of this association it receives technical assistance and other support.

II. PURPOSE

This Risk Management Manual aims to design a framework that shall identify potential risks that may endanger the achievement of critical objectives of the organization and establish risk handling strategies to mitigate its adverse impacts, specifically by:

a. Identification of inherent and potential risks of the organization's operations, financial inflow and outflow, governance and external threats;
b. Setting appropriate risk appetite levels and limits for every identified risks;
c. Assessment of severity of risk outcomes and implementation of internal control procedures; and
d. Establish risk management plans to support the achievement of organization's objectives, protect staff and business assets and ensure financial sustainability;

III. RISK APPETITE STATEMENT

The KMBA Board of Trustees, through the Risk Management Committee, shall identify and set the risk appetite of the organization which reflects the amount of risk that the organization is willing and able to take in order to achieve its organizational objectives. The risk appetite of KMBA shall be based on its capability and strict observance of its key resources: Total Assets, Net Income, Liquidity, Compliance and Reputation.

KMBA's risk appetite shall be clearly stated, understandable and properly communicated to the business units, the management, committees and Board of Trustees. It shall be aligned to KMBA's overall risk management strategies, long term and short term goals,

and financial position. The risk appetite shall clearly convey the tolerance or maximum level of risk that the organization is willing to take, specifically identifying its inherent and potential risks, its likelihood and impact to the core of KMBA's operations.

IV. KMBA RISK MANAGEMENT FRAMEWORK

KMBA's risk management framework shall be proportionate to the complexity of its operations and organizational strategies which composed of the following factors:

a. Risk Ethics and Principles

KMBA risk management shall be anchored to its cultural value for the members by observing ethical, prudent and proactive risk management. It shall be guided by the following principles:

1. Good risk governance culture - The business unit, management, committees and the Board of Trustees shall ensure commitment to good risk governance by establishing sufficient lines of defenses with clear roles and responsibilities, duties and accountabilities.
2. Organized risk management objectives - The organization shall have an integrated structure and clear risk management lines to cover all perspectives of operation, finance and governance.
3. Information dissemination - The organization shall promote awareness on organizational risks and the management's initiative to combat and prevent its possible adverse effects.
4. Transformation to digitalization - The organization shall embrace opportunities of technological advancement by using modern and applicable software which could strengthen its risk management strategies.

5. Transparent and accurate risk data - Generate useful, relevant and accurate risk data in order to properly assess risk, ascertain appropriate risk management decisions and introduce effective controls and action plans.

b. Key Risk Metrics

KMBA shall establish the following indicators of its key risks, implement risk monitoring initiatives, identify risk reporting for breaches and action plans to manage the risks:

1. Key Risk indicator - is the set of metrics which specifically identify inherent risks of the organization and shall be monitored using the following factors:

    - Level of Exposure
    - Effectiveness of Internal Controls
    - Risk management effectiveness

2. Risk Threshold Report - is the monitoring tool which presents the level of organizational exposure to the inherent risks and interprets the risk appetite of the organization based on the available periodical risk data.

    The risk monitoring report is where the appetite, limit and tolerance to specific risks is identified vis-a-vis actual financial and operational performance of the organization.

3. Risk Appetite - refers to the threshold which interprets the standard risk that the management is willing to assume. No action plans are required if inherent risk is within this threshold.

4. Risk Limit - refers to the threshold where deviations from the standard procedures remain tolerable. Internal controls at this level are required to be reassessed and exceeding this threshold shall trigger a management action.

5. Risk Tolerance - refers to the maximum amount of risk that the organization is willing to take. Internal controls at this level are required to be reassessed and exceeding this threshold shall trigger a Board action as it exposes the organization to possible financial or operational loss.

c. Internal Controls

KMBA shall establish internal controls on its business processes which will provide assurance that the financial and operational procedures are being performed in an efficient and reliable manner. The internal controls shall be compliant to laws, regulations, relative standards and procedures that shall safeguard the organization from possible losses, reputational damage and harm to members.

The internal controls shall be an attribute in achieving the organization objectives by meeting the following standards:

1. That the controls are effective and efficient
2. That the controls are reliable, timely and complete
3. That the controls are compliant to laws and regulations
4. That the controls strictly adhere to internal policies
5. That the controls forms part of the systematic procedures of the organization

V. RISK EXPOSURES

KMBA's material risk exposures revolves on the following risk types:

a. Credit Risk

These are the risk of financial loss due to member's failure to meet the terms and conditions of its policy and its failure to perform as agreed therein. KMBA aims to have a well-balanced portfolio, thus it shall assure that its receivable balances from MFI-partners are in tract and exposures to any impairment to such would be not so significant.

Member credit risk is managed by analyzing the credit risk for each new member before standard payment and appropriate delivery terms and conditions are offered. Outstanding receivables are regularly monitored. The credit quality of the organization's financial assets that are neither past due nor impaired is considered to be good quality and expected to be collectible without any credit losses.

Credit risk from balances with banks is managed by ensuring that deposit arrangements are with reputable and financially sound counterparties.

The credit quality of the association's financial assets is evaluated using internal credit rating. Financial assets are considered as high grade if the counterparties are not expected to default in settling their obligations, thus, credit risk exposure is minimal. These counterparties include banks, related parties and members who pay on or before the due date. KMBA's bases in grading its financial assets are as follows:

- High grade. These are receivables which have a high probability of collection (the counterparty has the apparent ability to satisfy its obligation and the security on the receivables are readily enforceable).

- Standard. These are receivables where collection is probable due to the reputation and the financial ability of the counterparty to pay, but which have been outstanding for a certain period of time.

- Substandard. Receivables that can be collected provided KASAGANA-Ka MBA makes persistent effort to collect them

b. Liquidity Risk

Liquidity risk is the inability of the organization to meet its capital requirements due to threats in its financial position.

c. Operational Risk

The risk of loss resulting from inadequate or failed internal processes, people, and systems form external events but excluding strategic and reputational risks.

- Internal Processes is the risk arising from inadequacy or inappropriateness of established policies, standards and procedures resulting in failure of communication among business units, poor documentation handling, inadequate safety and security controls, and ineffective contingency plans.

- People or personnel related risks involve the breach of internal policies, standards and procedures, and delegated authorities of the management, committees and BoT. It also involves a personnel's negligence due to

oversight of function or due lack of experience and expertise, including internal criminal acts such as fraudulent activities.

- System risks are represented by inadequate hardware and software systems, obsolescence in technology adaptation, lack of server maintenance, and other related system defects or failures.

- External Events are uncontrollable risks but preventative which is triggered by external criminal activities, mis-performance of partners and affiliates, man-made and natural disasters, and regulatory risks.

d. Information Technology Risk

IT risks are subsumed by operational risks, or the adverse outcome for any information technology reliance such as system downtimes, software hacking, software failures, human and system errors and other malicious system attacks.

e. Compliance Risk

Compliance risk arises from violations or non-conformity to laws, rules and regulations, circulars, and prescribed practices of the Insurance Commission and other regulatory bodies that may expose KMBA to fines and penal-ties by these regulatory bodies. This includes legal risks or the exposure to fine and penalties, punitive damages, private settlements

VI. RISK STRUCTURE AND GOVERNANCE

The safety and soundness of the organization rely on the effectiveness of internal control and oversight function of the KMBA's trustees, officers and management team. This includes close integration within the operations, sound corporate governance policies,

processes and structures that shall support risk-related decision-making. Hence, these individuals must ensure ongoing effectiveness of risk management through adaptation of strategic and rigorous planning, and a strong and sustained commitment to the organization's principles and purpose.

KMBA shall establish an up-to-date risk management structure and governance. The structure aims to strengthen KMBA's risk management culture through good corporate governance exercised by both the Management and the Board of Trustees. These bodies shall ensure effectiveness of risk management strategies, processes and communication framework that is spearheaded by the Chief Risk Officer (CRO) of the organization, and which are reviewed and approved by the Risk Management Committee.

a. The Board of Trustee (BoT)

The highest governance body of the organization and shall be ultimately responsible for the governance of the organization. It shall ensure that the appropriate level and quality of capital is maintained and shall be in charge of the overall management culture. Specifically:

- Reviews effectiveness of the association's internal controls
- Provides policy, oversight and review of risk management
- Support and promote risk management within the Association
- Consider the risks associated on its decision-making process
- Appointment of members of the Risk Management Committee
- Ensure that risks associated in operations are identified and effectively managed by Risk Management Committee

b. The Risk Management Committee (RMC)

As a board-level committee, the Risk Management Committee shall be in charge of the management of both financial and non-financial risks of the organization, continuously monitor these risks and ensure that internal controls are in place. RMC shall promote a risk management culture across the organization by nurturing the business units with sufficient knowledge on preventing and foreseeing risk events. It shall assist BoT in fulfilling its duties by overseeing the risk management framework, address breaches and introduce strategies to manage the risks. RMC shall be responsible for the approval of the appointment of the Chief Risk Officer (CRO), setting its responsibilities and monitoring of its performance. Specifically:

- Monitors and considers the internal control environment which focuses on operational risks, internal and external audits and credit assurance with assistance of the Audit Committee and Internal Audit
- Ensure regular review of the risk management activities logged on the service risk register as part of wider association's performance
- Ensure that risk management within its areas of responsibility is implemented in line with the Risk Management Strategy
- Conduct annual reporting to Trustees on any perceived new and emerging risks or, failures of existing control measures
- Continuously improving risk management policy, strategy and supporting framework subject to the Board's Approval

c. **Other Board Level Committee**

1. **Corporate Governance Committee (CGC)**

   The CGC shall be responsible in providing continuing education and performance evaluation of BoT. Outcome of the evaluation shall identify the risks on corporate governance which the CGC shall report to RMC.

2. **Audit Committee**

   The AC shall evaluate and assess the effectiveness of the internal control system of the organization and assist RMC in its oversight function on the management of risks.

3. **Related Party Transactions Committee**

   RPT Committee shall be in charge of all the corporate dealings of the organization with strict observance of highest form of integrity. It shall be responsible in reviewing and vetting the organization's related party transactions and DOSRI.

d. **Lines of Defense**

1. **First Line of Defense**

   Business Units (BUs), including the supporting units, shall perform the first line of defense being the business risk owner. As the first line, the BUs shall identify and manage its risks as it delivers support to KMBA's products and services. Primarily, it is responsible to:

   - Identify and manage risks that is inherent to their business processes, products and services
   - assessment and enhancement of system controls to ensure that risk mitigation strategies are effective.

- Monitoring of member's risk profiles in a timely manner
- Ensure adherence to risk threshold established for the appetite of the organization
- Ensure consistency of internal controls to organization's internal policies and standards, laws and regulations.
- Ensure adequacy in terms of personnel, policies and processes

2. **Second Line of Defense**

The second line of defense is performed by the Chief Risk Officer, Compliance Officer and General Manager. Their responsibilities are as follows:

Chief Risk Officer

- Deploying and designing overall risk management framework across the organization
- Reports to the Risk Management Committee periodical reports on risk thresholds, current losses, risk assessment and business continuity, and provide recommendation and strategies thereof
- Monitors the BUs strict adherence to the established risk management framework
- Compiles all the risks across all business units and communicate the same to the management for proper action
- Develop risk management related policies and standards

Compliance Officer

- In charge of the overall compliance of the organization to laws, rules and regulations

- Interpret the issuances of government bodies, disseminate the same to business units and ensure compliance to any mandated actions and submission of any reportorial requirement
- Performs compliance testing for purposes of assessing risks related to laws and regulations.

General Manager

- Drives culture of risk management and signs off on annual risk attestation
- Responsible for ensuring that appropriate risk management, policies and controls are in place, sufficiently robust to ensure that these key risk are properly identified, assessed, monitored and mitigated
- Ensure the Board that the principal risks are appropriately managed and the operations are within the association's risk appetite
- Ensure personnel in their business units comply with the risk management policy and foster a culture where risks can be identified and escalated
- Report any perceived new and/or emerging risks or failure of control measures to the Risk Management Committee
- Communicates risk management arrangements to personnel

3. Third Line of Defense

The Internal Audit of the organization shall act as the third line of defense. Its responsibilities are the following:

- Provide an annual independent and objective assessment and testing of efficacy risk management control processes and business compliance

- Validation of the overall risk management framework
- Provide assurance of effectiveness of risk management methodologies and design
- Undertake both regular and ad hoc reviews of risk management controls and procedures of which are reported to the Audit Committee
- Report findings that may be perceived as new and/or emerging risks or failed control measures to the General Manager.
- Provide advice, guidance and recommendation on risk and control management for the development in the organization's risk culture

4. Executive Oversight

The Risk Management Committee, Audit Committee and Board of Trustees is responsible for overseeing KMBA's risk management strategies. It sets the tone from the top management, establishes the risk appetite of the organization to each risk and sets up strategies in preventing potential losses, specifically:

- Approval of risk management methodologies, internal policies and tools needed for the framework
- Any decision-making initiatives based on the up to date risk information - accept, mitigate, transfer or avoid.
- Evaluate activities of business units, operations and financial capacity of the organization

VII. RISK MANAGEMENT METHODS AND TOOLS

In the conduct of Risk Management, there are three considerations that shall be taken into the account;

- That it shall form part of the management
- That it is embedded in the culture and practices; and
- That it is tailored to the business process of the organization.

Risks that exist from one organization may not exist in another organization. The rationale behind this is because each entity has different business processes and sustainability. Thus, in order to provide a proper and efficient recommendation in mitigating risks, the strategies that will be taken shall be tailored based on the business process of the organization.

The Risk Management Process Cycle

Establishing the Context

Context identifies the scope of the risk management activities. It sets the criteria against which the risks will be assessed according to the environment by which the association seeks to achieve its objectives. Basically, context is categorized into two – the Internal Context and the External Context. Internal context are those key areas within the scope of control of the association and the External Context are those key areas beyond its control, specifically:

a. **Internal Context**
   - Governance, Organizational Structure, Roles and Accountabilities
   - Policies, objectives and strategies

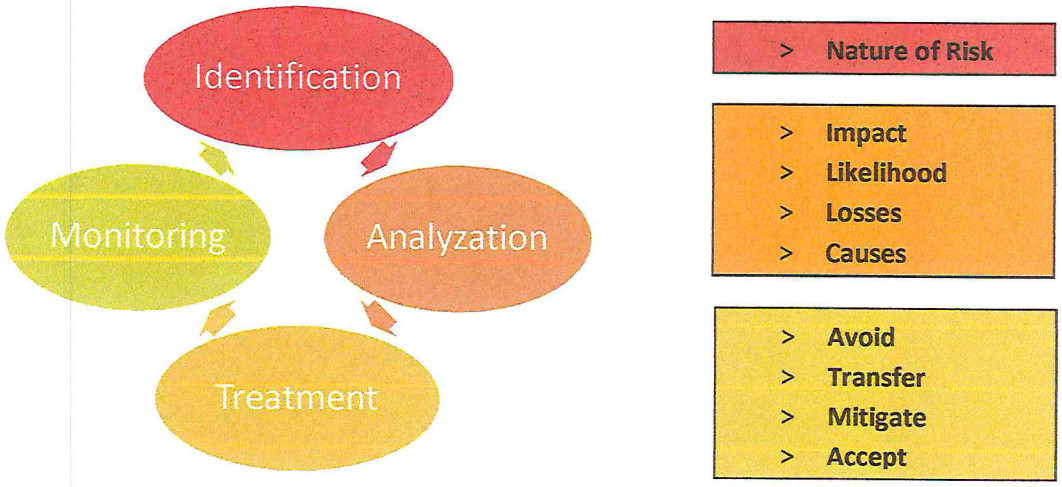
- Capabilities, resources and knowledge
- Information Systems, Flows, Decision-Making Processes (formal and informal)
- Relationships with the internal stakeholders
- Organizational Structure
- Standards, guidelines and models adopted
- Form and extent of contractual relationships

b. External Context

- Social and cultural, political, legal, regulatory, financial, economic, technological, natural and competitive environment (national, local or regional)
- Key drivers and trend that has impact on objectives of the organization
- Relationships with, perceptions and values of external stakeholders

Managing risks is an important aspect of corporate governance for it may lead to serious financial loss or reputational impact. Hence, KMBA shall establish a systematic process cycle which will identify, assess and respond to risks for purposes of minimizing the probability of adverse consequences in achieving its objectives. The risk management process cycle shall reflect to the continous changes on the organization's environment shall be interpreted as follows:

RISK MANAGEMENT PROCESS CYCLE



Identification of Risk

The process of identifying risk exposures of the organization and the nature of the possible consequences it has for organizational objectives.

Analyzation of Risk

This is where several risk monitoring tools are used to identify the risks' impact, likelihood, losses and causes.

- Impact is the level of which the risk will affect the results of financial position of the organization and will require delivery of effective strategies to prevent any potential financial or non-financial loss.
- Likelihood is the probability of the occurrence of risk that could trigger weakness in the established internal control system.
- Losses is the direct financial loss resulting from an event.
- Causes is the factor that changes overtime and brings about the occurrence of the risk event.

Risk Treatment

This is the step where appropriate treatment measures were applied and implemented to threshold breaches, requiring intervention of the management, RMC and BoT. Selection of risks, designing and refining of strategies and risk prioritization takes place in this step.

- Risk Transfer is the measure of transferring the impact of the risk to a third party.
- Risk Avoidance is the measure that would prevent the identified risks from materializing by not further engaging to activities related to the risk event
- Risk Mitigation is the measure that would minimize the negative impact of the identified risks
- Risk Acceptance is the measure where no further action is required because the risk effect can be managed by the organization.

Risk Monitoring

Monitoring of risk involves the treatment measures implemented by the organization, changes in the organization's risk profile and effectiveness of risk management tools and mechanisms.

VIII. RISK MANAGEMENT AWARENESS

a. Communication System

The organization shall have an open communication on risk issues and risk strategies across the organization. It shall adopt a communication system which raises awareness and enables a timely information dissemination and risk education to business units.

b. Mandatory Trainings

Mandatory Training on Risk Management shall be organized annually for personnel, officers and BoT's to ensure their awareness on updated risk management policies and standards, including their roles, duties and responsibilities.

c. Other Training Participation

The organization shall participate in other opportunities of educational development from external professionals and/or academe to improve the organization's risk strategies. This is through participation of the personnel, officers and BoT's in external training and seminars that could innovate the organization's risk handling and internal control systems.

IX. EXCEPTION HANDLING

Any deviation in the policies and standards related to the management of risks of the organization shall adhere to the following requirements:

a. A proposal on exception handling shall be submitted by the requester and where the justification shall be reasonable enough to deviate from the standards and procedures, supported by risk assessment and proposed risk mitigants.
b. The proposal shall be approved by the Chief Risk Officer and Risk Management Committee.