SERVIAMUS MUTUAL BENEFIT ASSOCIATION INC.
4th Floor, Diocesan Centrum Bldg., Lluch St. Poblacion, Iligan City
Telephone: (063) 223-2493, 228-4354 Email:serviamus_mba@yahoo.com

ENTERPRISE RISK MANAGEMENT FRAMEWORK

Rationale

Serviamus MBA's vision/goal is to ensure that risks are properly assessed and managed in a proactive manner.

In pursuing our vision/goal, we will face many strategic risks, operational risks and risks associated with the protection of our people, property and reputation. This document describes the policies by which these risks are to be effectively managed.

ERM Policy

Statement of Board Support

The Serviamus MBA Board of Trustees acknowledges the importance of ERM in our MBA's growth and sustainability and must be embodied in our organizational culture. The Board fully supports this policy and the underlying principles and will review this document annually to ensure its continued application and relevance.

ERM Policy Objective

Our policy is to identify, analyze and respond appropriately to all risks. The risk responses selected are determined by our appetite and tolerances for risk. These will vary over time according to the specific business situation.

Definition of Risk

We define risk as any potential event which could prevent the achievement of an objective. It is measured in terms of impact and likelihood. Risks arise as much from the likelihood that an opportunity will not happen, as it does from the threat or uncertainty that something bad will happen.

Risks can be viewed from three perspectives:

Opportunity -Risk of lost opportunity or something good not happening. We recognize the fundamental relationship between risk and return, that is, the greater the risk, the greater the potential return or loss.

Uncertainty - Risk of not meeting expectations. We need to determine how we can proactively prevent an uncertainty from having a negative impact.

Hazard - Risk of loss or something bad happening. We need to mitigate the degree of damage to critical business assets (people, property, earning capacity and reputation) that would be caused if a hazard occurs.

Risk Appetite and Risk Tolerance

Our business objectives are fundamental factors in determining our appetite for, and tolerance of, risk. The risk appetite and tolerance dictate the nature and level of risks that are acceptable to us. We define risk appetite and risk appetite as:

Risk appetite - *the* amount and types of risk we are willing to accept to achieve our objectives.

Risk tolerance - the level of acceptance of the outcomes of a risk should they occur, and having the right resources and controls in place to absorb or "tolerate" the given risk.

Risk appetites and tolerances will vary according to the balance of opportunity, uncertainty or hazard which differing risks represent.

Risk Management Principles

The following principles provide the foundation for effective risk management of our organization:

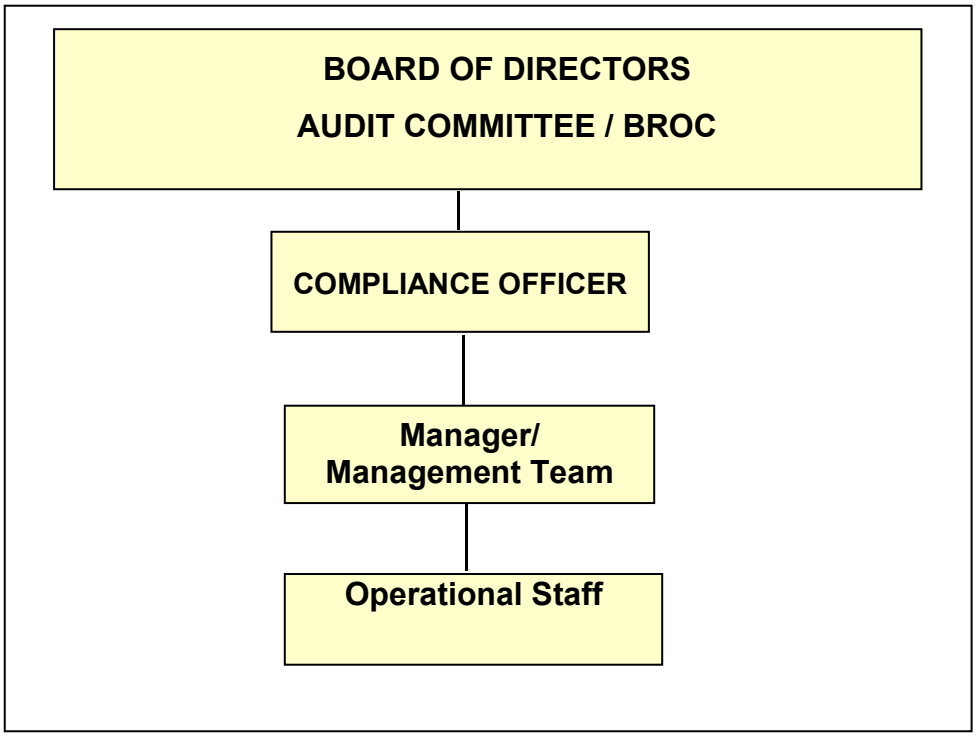
Risk management should create value	Risk management should contribute to the achievement of objectives. It should help improve performance, efficiency of operations, governance, and regulatory compliance.
Risk management should be an integral part of organizational processes	Risk management is not a stand-alone activity. It is a key responsibility of management and integrated in strategy development, planning, implementation and assessment processes. It is neither an additional task to comply with.
Risk management should be part of decision making	Risk management should help decision makers differentiate among alternative courses of action, make informed choices, and prioritize actions to take. It helps management decide how to allocate of scarce resources.
Risk management explicitly addresses uncertainty	Risk management takes into account uncertainty, the nature of that uncertainty, and how it can be addressed.
Risk management should be systematic and structured	Risk management should be a methodical approach. It should contribute to consistent, comparable and reliable results. It should be aligned to the existing organizational systems and structure to make it efficient and effective.
Risk management should be based on the best available information	Risk management should collect and use information from a variety of available sources including historical information, experience, observation, forecasts and expert judgment
Risk management should be "tailor fit" to the organization	Risk management should be aligned with the organization's internal and external environment. It should consider the type and size of the organization,

	its strategy, its systems, and processes among others.
Risk management should take into account human factors.	Risk management should recognize that every organization is different. It will have its own culture, capabilities, perceptions, and intentions of people distinct from other organizations.
Risk management should be transparent and inclusive.	Risk management should involve the participation of key staff at all levels of the organization to ensure that risk management remains relevant and updated.
Risk management should be dynamic, iterative and responsive to change.	Risk management should be a continuous and repetitive process to respond to a changing environment. Existing risks should be monitored and reviewed, and new risks identified as soon as they emerge.
Risk management should be capable of continual improvement and enhancement	Risk management should be able to continually evolve and improve as the organization becomes more knowledgeable and skillful in implementing risk management.

Organizational Arrangement

Risk Management Structure

The Board is responsible for the ERM Framework. The management team under the leadership of the MBA Manager is responsible for implementing the strategy, culture, people, processes, technology and structures which constitute the ERM Framework.



Roles and Responsibilities

The specific roles and responsibilities under our organizational arrangement are as follows:

1.The Board of Trustees

a. Oversees the company's risk management programs, procedures, and controls.
b. Approves the risk management framework.
c. Approves and articulates the risk appetite for the organization; principles and policies recommended by management.
d. Reviews risk reports.
e. Monitor risk indicators for identified significant risks.
f. Support and promote risk management within the association.

2.Audit Committee / BROC

a. Oversees the financial reporting process and the system of internal control.
b. Review reports, opinions and recommendations prepared by the appointed actuary with respect to the adequacy of reserving and reporting practices.
c. Discusses with management, the independent auditor and the appointed actuary matters such as:
    i. key areas of risk for material misstatement of financial statements;
    ii. reasonableness of accounting estimates;
    iii. significant or unusual transactions and;
    iv. contentious matters noted during the audit.

3. Compliance Officer

a. Develop the risk management policy and keep it up to date
b. Document the internal risk policies and structures
c. Co-ordinate the risk management (and internal control) activities
d. Compile risk information and prepare reports for the Board
e. Report on the efficiency and effectiveness of internal controls

4. Manager/ Management Team

a. Develop and implement an effective ERM framework, principles and policies.
b. Continuously improve the ERM framework.
c. Determine the risk for the organization.
d. Establish the risk management structure.
e. Build a risk aware culture.
f. Assign responsibilities for risk ownership, monitoring and reporting.
g. Establish internal and external communication and reporting mechanisms.
h. Takes action, monitors to ensure risks responses are effective and continuous.

i. Present periodic risk report to the Board.

5. Staff/ employees

a. Understand, accept and implement the ERM processes

b. Report inefficient, unnecessary or unworkable controls

c. Report loss events

Risk Management Approach

We have adopted the ORCA approach to ensure the consistent application by all our staff in the execution of our strategy achievement of business objectives and day to day operations.

ORCA represents:

O **Objectives -** Goals/results we aspire to achieve
R **Risks -** Potential events which could prevent the achievement of an objective
C **Control -** Management's response to risks
A **Alignment -** Alignment of our objectives, risks and controls across the organization determined by our appetite and tolerance for risks

1. **Objectives** - ERM starts with a clear understanding of what are we trying to achieve in our business and ensuring that key risks are identified. This includes our mission, vision and business goals/ objectives.

2. **Risks -** Risks are uncertain future events which could influence the achievement of our business objectives and can be viewed from three perspectives:

Opportunity- Risk of lost opportunity or something good not happening.

We recognize the fundamental relationship between risk and return, that is, the greater the risk, the greater the potential return or loss. In this situation, we need to adopt suitable responses to maximize the benefit f such an opportunity within the constraints of its operating environment.

Uncertainty- Risk of not meeting expectations.

We need to determine how we can proactively prevent an uncertainty from having a negative impact. This will mainly be achieved through management of risks relating to operational performance.

Hazard - Risk of loss or something bad happening.

We need to mitigate the degree of damage to critical business assets (people, property, earning capacity and reputation) that would be caused if a hazard occurs.

3. **Control** - Control encompasses all our possible responses to risk, whether viewed as opportunities, uncertainties or hazards. These controls are the responsibilities of all our staff and are designed to provide reasonable assurance regarding the achievement of our business objectives.

   In determining our risk response, we must first assess whether to accept, exploit, mitigate, transfer or avoid the risks. In the case of exploit, mitigate or avoid, controls will need to be put in place.

   There are three main categories of controls:

   Preventive Controls - responses to stop undesirable transactions, events, errors or incidents occurring.

   Detective Controls - responses to promptly reveal undesirable transactions, events, errors or incidents so that appropriate action can be taken.

   Corrective Controls - responses to reduce the consequences or damage arising from materialization of a significant incident.

   Determining the type of control to Use

   In determining the types of controls, to use, the following factors will be considered:

   1. Our business objectives
   2. Our capability and skills
   3. Our appetite and tolerance for the type of risk
   4. The time horizon, matching the duration of the exposure and the length of time required in implementing solutions to manage the risks
   5. Financing i.e., cost effectiveness
   6. Alignment with other initiatives within the MBA and overall business direction

   Factors to ensure the effectiveness of controls

   In ensuring the effectiveness of controls, the following factors will be essential:

   1. Control framework is the responsibility of the Board of Directors
   2. Integrity, ethical values and competencies of staff
   3. Management's philosophy and operating style
   4. Delegation of authority and responsibility
   5. Continuous staff development
   6. Incorporate in existing systems, business processes and reporting as far as possible

4. **Alignment** – alignment must exist between the objectives, risks and controls at all levels of the MBA:
   1. Between strategies, operational objectives and individual job accountabilities
   2. Between the risks being taken and our appetite and tolerance for risk
   3. Between the control and the desired level of investment in implementing such control

ENTERPRISE RISK MANAGEMENT PROCESS OVERVIEW

Our ERM Process is a continuous cycle anchored on the following six steps:

1. Set strategy and objectives
2. Identify risks
3. Assess risks
4. Treat risks
5. Control risks
6. Communicate and monitor risks

Step 1: Set Strategy and Objectives

Defining the strategy and objectives is fundamental before moving to the next step. The strategy will provide the direction in developing operational plans and allocation of resources. Strategic objectives need to be aligned to our acceptable risk appetite to make sure that we are not accepting too much nor too little risk.

Step 2: Identify Risks

The second step in our ERM process is risk identification. The objective is to come up with an inventory of all possible risks that may affect the achievement of objectives and narrow them down to the most significant risks. We will maintain a risk register to keep a list of all possible risks. This risk inventory is reviewed and updated in succeeding risk identification processes taking into account the predicted changes in the internal and external environment.

To identify potential risks, we will use the following techniques:

a. Internal interviews and discussions - individual interviews, questionnaires, facilitated workshops, brainstorming and SWOT analysis.
b. External sources - comparison with other Mi-MBAs, discussion with peers and benchmarks.

Clear risk identification is important because it allows for a more precise assessment of the severity of the risks. It helps identify root causes and the impact of the risk to the objectives of our Mi-MBA. Risks identified will be tabulated in an inventory worksheet as shown below:

Risk Inventory Worksheet

Risk Statement (the event)	Strategic objective affected	Unit objective affected (if applicable)	Risk Owner (responsible person)
The Possibility to failure to meet the agreed policy term & condition(due to failed business) – *Member's Risk*			
The possibility of low interest rate – *Investment Risk*			
The possibility of negligence of function/resignation – *Personnel Risk*			
The possibility of human and system risk – *MIOS Risk*			
The possibility of implementation of IFRS 17 and new FRF – *Regulatory Changes Risk*			
The possibility of natural disaster that damages physical premises that result to MBA failure to operate – *Operational Risk*			
The possibility of poor customer support experiences and negative publicity about the organization – *Reputational Risk*			
The possibility to failure to submit reports that result to violation and penalties – *Compliance Risk*			
The possibility that partner MFI will not make membership to SMBA mandatory – *Security Risk*			

The risks listed in the inventory worksheet are referred to as inherent risks. Once mitigation

actions are determined, what remains are residual risks.

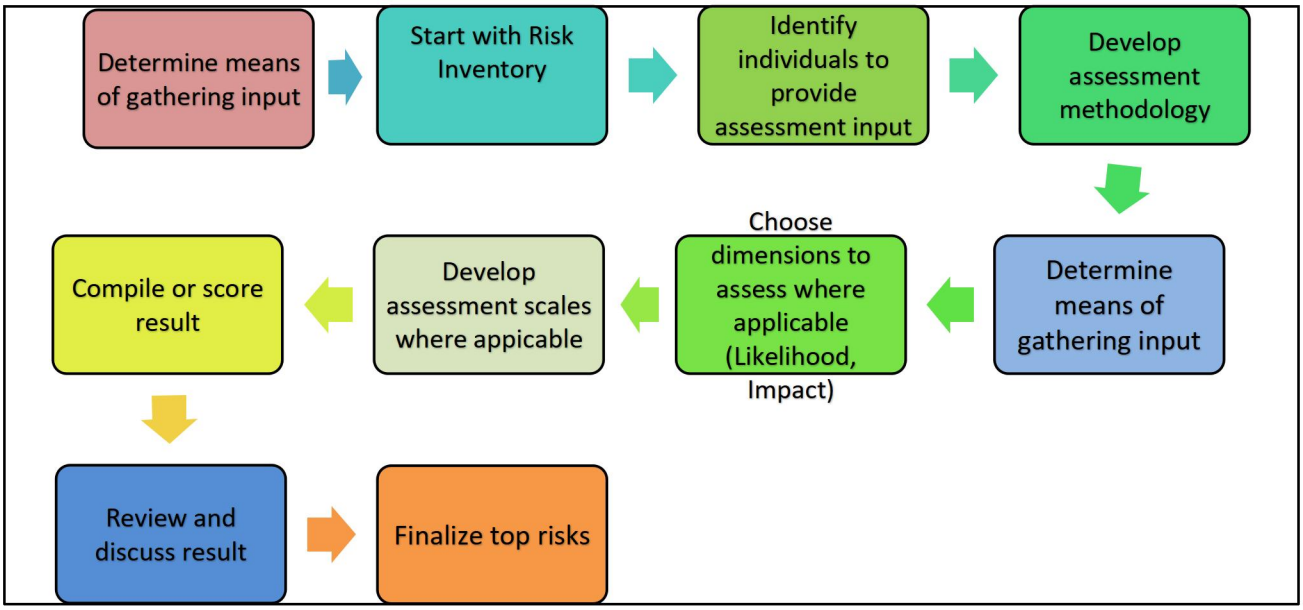
Risk Categories and Definition. We categorize risks based on the table shown below:

Risk Category	Definition	Risks Included
Credit Risks	Risk of financial loss as a result of default or failure of counterparts to meet their obligations.	Reinsurance risks, lending risks and bank deposit risks.
Market risks	Risk of loss from factors related to the financial market that affects the value of assets.	Interest rate deviations, currency fluctuations, devaluation of equity investments, fluctuations in real estate and property investment and inflation.
Operational risks	Risks of loss from inadequate or failed internal systems, processes and procedures	Employee actions such as Fraud
Insurance risks	Risks of loss related to underwriting and claims management that affect insurance operations.	Higher than expected mortality rate; higher than expected health and disability claims; non-renewal of policies; inadequate reserves; catastrophic events.
Liquidity Risks	Risks of the inability to generate sufficient cash resources or liquidate assets fast enough to meet financial obligation as they become due.	
Reputational risks	Risk of loss caused by a decline in the organization's reputation (character, quality or integrity).	Deterioration of image and relationship with clients, partner agent, regulators or with the community where it operates.

Step 3: Risk Assessment/ Analysis

The next step is to systematically evaluate, rank and prioritize risks. The objective of risk assessment is to come up with the "top" risks we face. The risk assessment process will ideally involve all of the Mi-MBA staff, since majority only have less than 10 personnel. The figure below shows the steps we follow in assessing and prioritizing the top risks.

Figure 7: Steps in Assessing Risks



Risk Assessment Method

Our preferred risk assessment method is the Forced Ranking Method. We deem this method as the simplest and most practical for our use given our constraints related to time, money, people, skills and management,

Under the forced ranking method, the following steps are undertaken:

1. **Choose top 10 risks**. Each individual provides input in the risk assessment process and are asked to choose (from their viewpoint) the top 10 risks from the risk inventory. Risks are ranked with 10 as the most important and 1 as the least important.

2. **Tabulate the frequency distribution of responses**. The frequency of responses from all participants are tabulated for each risk according to ranking. The 1st among the top risks is assigned 10 points, the 2nd is assigned 9, the 3rd 8th down to the 10th risk being assigned 1 point.

3. **Calculate scores.** The total risk score is calculated by multiplying the frequency of responses by the assigned points and adding up all the scores.

Evaluating the Risk

Once the top risks are prioritized, a decision is made whether a risk is acceptable or not. A risk is considered as acceptable when the risk is sufficiently low that treatment will not be cost effective or the risk treatment is not available.

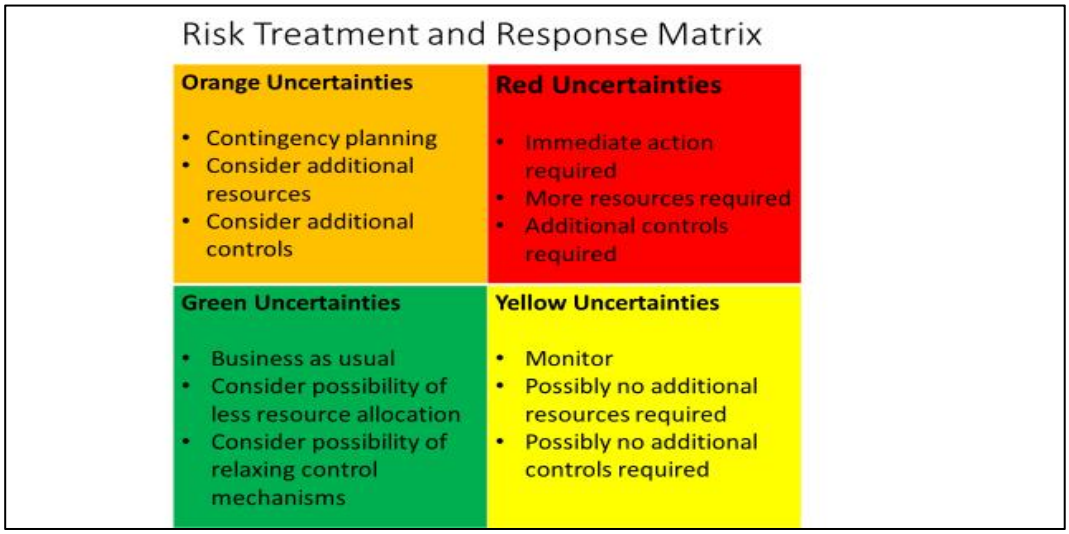
If management determines the risk to be acceptable, the risk may be tolerated with no further action for treatment beyond the control measures already existing. Acceptable risks should be continuously monitored and periodically reviewed to make sure they remain at a tolerable level.

Step 4: Risk Treatment
If a risk is found to be unacceptable, the next step is to treat the risk. The objective of this step is to find a cost-effective option of treating the risk. Treatment decisions must be in accordance with legal and regulatory requirements. A treatment once implemented, becomes a control or modifies an existing control.

There are 4 general treatment options:

Tolerate. This action is chosen when the risk is acceptable, control is impossible or cost of control exceeds the potential benefit. Contingency plan can be put into place to handle any potential impact.
Transfer. Transferring risks is an option that works well for risks to asset risks by paying a third party to take over the risk (such as reinsurance). This option is not possible for other types of risks such as reputational risks.
Reduce. Options to reduce or mitigate risks can include deploying of additional resources (e.g. people, technology, equipment, etc.), setting up new or revising existing control measures, streamline operations and improving staff capacities.
Avoid. Avoiding risk may be the easiest action to mitigate risk. This can be done by foregoing certain strategies or terminating activities that jeopardize the business. However, avoiding risks also means avoiding potential gains.

The Risk Treatment Matrix below will be used in determining treatment option to use.



Step 5: Risk Control
Once risk treatment/control strategies are identified, the next step is to decide whether the strategies identified will be implemented. These control measures include policy, procedures, practice, process, technology, methods and devices that scale down the severity of the risk.

The proposed control measures will be carefully weighed in terms of their cost and the corresponding benefit to the organization. Should the additional costs exceed the benefits, it may no worthwhile to pursue the action. We must also be careful that a control measure does not divert critical resources away from more important activities of the Mi-MBA.

Once a decision to implement control mechanisms is taken, we will put into place a risk management plan. The plan will include the key activities, performance indicators to measure

the completion and effectiveness of risk treatment activities and results.

Step 6: Monitor and communicate risks

The monitoring of the risks and the risk response plans is a continuous process. The main objectives of this step are to:

1. Determine whether the ERM process is working. Monitoring of the ERM process on a regularly basis is essential to find out the status of implementation and effectiveness of ERM. Any deviations must be reported for corrective actions to be taken as early as possible. Lesson learnt must be fed back and improvements made to the ERM framework and process.

2. Find out whether risk treatment strategies adopted are sufficient or need further action. Monitoring on a regularly is essential to assess the adequacy and effectiveness of treatment measures. This will allow management to reassess the risk and decide whether additional control measures are necessary.

3. Assess whether the risk profile has changed. Monitoring must also continuously assess the internal and external environment of the Mi-MBA. This allows for the early identification of new emerging risks, discontinuance of control treatment for downgraded risks and re-distribution of resources based on the revised risk profile.

Reporting. A Risk Assessment Report will be prepared periodically (quarterly/ semi annually) and made for submission to the Board of Trustees and MiMAP (RIMANSI). The content of the report includes the following:

1) A summary of the significant risks;

2) Risks that exceed the acceptable risks level;

3) Risk management decisions taken to bring risks to acceptable levels and the status of implementation to bring risks to acceptable levels;

4) New and emerging risks including their assessment

5) The trend of each risk (whether decreasing, stable, or increasing) and the effectiveness of the methodologies and procedures to manage each risk (whether weak, acceptable or strong) based on the definitions stated below.

Weak:	There are significant gaps in the methods, procedures and controls. The methods, procedures and controls are not fully documented. The methods, procedures and controls effectiveness cannot be assessed.

Acceptable:	The methods, procedures and controls are reasonable and appropriate including cost/benefit considerations. There are possibilities to further improve the methods, procedures and controls. The methods, procedures, and controls may either a) not be fully documented b) not fully implemented or c) not fully followed.
Strong:	The methods, procedures and controls are appropriate to the risk, are documented, and are implemented and fully followed.

6) Additional actions that may be required to improve risk management.